MEMORIAS

DA

ACADEMIA REAL DAS SCIENCIAS

DE LISBOA.

CLASSE DE SCIENCIAS MATHEMATICAS, PHYSICAS E NATURAES.

Nisi utile est quod facimus stulta est gloria.

NOVA SERIE—TOMO I.—PARTE I.

LISBOA

IMPRENSA NACIONAL.

1854.

PROPRIEDADES GERAES

E

RESOLUÇÃO DIRECTA

DAS

CONGRUENCIAS BINOMIAS

INTRODUCÇÃO AO ESTUDO DA THEORIA DOS NUMEROS

Por **DANIEL AUGUSTO DA SILVA**

LENTE DA ESCÓLA NAVAL

E SOCIO EFFECTIVO DA ACADEMIA REAL DAS SCIENCIAS DE LISBOA

PROPRIEDADES GERAES

E

RESOLUÇÃO DIRECTA

DAS

CONGRUENCIAS BINOMIAS

INTRODUCÇÃO AO ESTUDO DA THEORIA DOS NUMEROS.*

PREFACIO.

1. A theoria dos numeros, considerada por muito tempo mais como uma curiosidade especulativa, do que como um ramo principal e indispensavel das sciencias mathematicas, tende continuamente a desprender-se desse desfavor, para occupar a posição eminente que lhe compete. Cultivada entre os antigos com a mais visivel predilecção, os trabalhos delles, e particularmente a admiravel obra de Diophanto, como que apenas serviam para ostentar a profunda sagacidade desses geometras.

Fermat, no seculo decimo setimo, applicando a sua poderosa intel-

* Esta Memoria foi apresentada na 1.ª Classe da Academia Real das Sciencias de Lisboa em a sessão do dia 24 de Março de 1852. A grave e prolongada enfermidade que o A. tem padecido fez interromper a imp essão durante vinte mezes, desde Junho daquelle anno. Por este imperioso motivo, que subsiste ainda, deixou o A. de fazer a revisão deste prefacio, bem como das ultimas folhas da Memoria, a começar na pag. 117; e pela mesma causa não pôde accrescentar ao capitulo IX, como tencionava, algumas proposições relativas á resolução da congruencia $x^t \equiv c^t$ além das que são contidas no fragmento porque se termina esse capitulo; nem lhe foi possivel desenvolver os assumptos que deviam comprehender-se no capitulo X, de que apenas se publica o resumo.

ligencia a essas difficeis investigações, descobriu muitos theoremas notaveis; mas infelizmente, levado talvez por esse mal entendido espirito de rivalidade scientifica, com que na sua época luctavam entre si os geometras, apresentando uns aos outros, debaixo da fórma de problemas, as descobertas que faziam; Fermat supprimiu a maxima parte das demonstrações dos seus theoremas, as quaes elle affirma ter alcançado; e da veracidade dessa declaração deve considerar-se testemunho bastante a brilhante reputação de integridade que elle obteve na sua longa e assidua carreira na magistratura judicial.

Euler, o genio da lucidez mathematica, applicando-se com o maior ardor ao estudo da theoria dos numeros, chegou a obter importantes resultados, cabendo-lhe a gloria de ter sido o primeiro que demonstrou o theorema que especialmente se designa com o nome de Fermat, e que lhe deu uma notavel e importante generalisação.

As descebertas curiosas com que Lagrange enriqueceu esta sciencia difficil; as excellentes investigações contidas na *Théorie des mombres* de Legendre; as *Disquisitiones Arithmeticæ* de Gauss, a obra mais profunda, mais abundante, e elevadamente original neste genero; as bellas Memorias de Poinsot, e tantos outros escriptos recentes sobre especialidades da arithmetica transcendente, provam o quanto os analistas modernos tem dado consideração ao estudo das propriedades dos numeros.

Finalmente, o ultimo programma da Academia das Sciencias de París, em que apparece proposto pela segunda vez como objecto do premio grande de mathematica a demonstração de um dos theoremas de Fermat, é um solemne documento de nobilitação da theoria dos numeros ratificado com toda a authoridade daquella corporação illustre.

A importancia destes estudos já não póde ser hoje desconhecida. É sabido o quanto lhes devem os outros ramos das sciencias mathematicas. Basta mencionar, como ponderosas contribuições daquella sciencia transcendente, no campo da analyse a resolução algebrica das equações binomias, e em relação á geometria a determinação geral dos numeros primos em relação aos quaes é possivel a divisão *geometrica* em partes iguaes da circumferencia do circulo, admiraveis descobertas que primeiro appareceram na citada obra de Gauss. Poderiamos ainda accrescentar que o bello theorema de Bertrand, relativo ao numero de valores de uma funcção não symetrica de n letras, theorema de tão notavel importancia na theoria da resolução das equações algebricas, não está ainda demonstrado completamente por isso que depende de uma propriedade dos numeros primos, cuja verdade não pôde ainda verificar-se senão empyricamente pelo exame desses numeros, até onde chegam as taboas que delles possuimos.

Em geral póde affirmar-se que ninguem está authorisado a capitular quaesquer theorias mathematicas como destituidas de applicação vantajosa, como um mero recreio de elevadas intelligencias, e como inuteis trabalhos em relação á verdadeira sciencia. Todas as verdades adquiridas são outros tantos elementos de riqueza intellectual accumulada. Cedo ou tarde chegará o dia em que a sciencia concreta terá de ir procurar a este vasto arsenal os instrumentos necessarios para grandiosas descobertas, e que por esse modo passarão de theoremas especulativos para a cathegoria de verdades praticas. Todos os dias se observa que este ou aquelle ramo da physica mathematica, e da mechanica celeste ou industrial suspende repentinamente o seu desenvolvimento para implorar dos ulteriores progressos da analyse pura que lhes prestem o auxilio, sem o qual aquellas importantissimas sciencias não podem progredir.

Em relação, porém, á arithmetica transcendente, a que especialmente nos temos referido, a sua utilidade de applicação conhece-se na asserção de Legendre (obra citada), «*En effet, il n'est pas de théorème sur les nombres qui ne soit pas relatif à la resolution d'une ou de plusieurs équations indéterminées*», e ainda melhor na affirmativa mais amplamente verdadeira de Poinsot (*Réflexions sur les principes fondamentaux de la theorie des nombres*) «*Et cependant, pour peu qu'on y veuille réfléchir, il est aisé de voir que cette arithmétique transcendante est comme le principe et la source de l'algèbre proprement dite. C'est une vérité qu'on pourrait établir par le raisonnement, comme je le mon-*

trerai tout à l'heure, mais qu'on peut aussi prouver en quelque sorte par l'expérience. Car, observez que ce peu qu'on ajoute de temps à autre à l'algèbre vient du peu qu'on découvre par intervalles dans la science des propriétés des nombres.»

É por essas considerações que nós entendemos que é altamente desvantajoso para os futuros progressos das sciencias mathematicas, que a theoria dos numeros continue a ser, como até aqui, quasi inteiramente banida do ensino. Vêr-se-ha no capitulo II desta Memoria, que, mesmo na parte mais elementar da algebra, na resolução das equações indeterminadas do primeiro gráu, o emprego de alguns dos principios fundamentaes da theoria dos numeros conduz immediatamente a obter as formulas geraes e directas daquella resolução, para a qual, nos livros elementares, se costuma apresentar sómente *methodos de calculo numerico*, mais ou menos laboriosos.

2. Como o conhecimento do que se contém em um escripto mathematico, e que faz que este não seja de todo uma contribuição inutil para o progresso da sciencia, é o que póde animar a emprehender a sua leitura; julgámos conveniente indicar desde já mui rapidamente os principaes resultados, que nos parecem novos neste nosso trabalho, em que aliás se acharão tambem muitas demonstrações novas de theoremas conhecidos.

As formulas symbolicas (9, 10) que damos no capitulo I, achar-se-ha que são susceptiveis de variadas applicações. A segunda serve-nos como se verá, para demonstrar, de um modo unico e directo, varios theoremas para que se empregavam demonstrações diversas e indirectas; e pela primeira somos conduzidos a uma expressão elegante da somma dos numeros menores que um numero dado e primos com elle.

A formula (18), que tambem se acha nesse capitulo, comprehende, como caso particular, o theorema de Euler (14).

No capitulo II, além dos desenvolvimentos que damos á solução directa das congruencias lineares a uma incognita, solução que já antes havia sido indicada mui concisamente por Legendre, apresentamos tambem formulas directas para a solução das congruencias lineares a muitas incognitas, e das congruencias simultaneas; e incidentemente completamos a formula de Poinsot, que dá todos os numeros primos com qualquer numero dado, substituindo-a por outra, que fornece qualquer numero correspondente a determinados residuos relativamente aos factores primos de que é formado o numero proposto.

A notação de que constantemente fazemos uso em todas as nossas formulas de resolução, servirá para melhor as fixar na memoria.

Os processos que damos no capitulo IV, para a determinação das raizes primitivas, persuadimo-nos serem mais rapidos e directos do que outros que tem sido propostos: e se não conseguimos ainda que esses methodos sejam sempre isentos de algumas tentativas infructuosas, procede isso talvez da existencia de uma difficuldade insuperavel inherente á indole peculiar daquelles numeros mysteriosos, de uma natureza correlativa, postoque de uma ordem superior á dos numeros primos. Tanto uns como outros, será provavelmente impossivel que jámais venham a ser dados por formulas directas.

O estudo e discussão que fazemos no capitulo V, sobre a formula de Gauss (71), dá-nos não só a formula (73), mas tambem varios theoremas notaveis sobre os residuos (§§ 50 a 56) e o desenvolvimento (79), daquella formula.

No capitulo VI apresentamos formulas directas para a resolução da congruencia $x^D \equiv 1$, relativamente a um modulo potencia de numero primo e transformamos essas formulas de modo a indicar explicitamente as raizes primitivas, e não primitivas daquella congruencia.

No capitulo VII, em que tratamos separadamente a congruencia relativa ao modulo 2^m, accrescentamos varias considerações e formulas ao que se acha no capitulo correspondente da Memoria de Poinsot.

No capitulo VIII achar-se-ha não só varias formulas directas para a resolução de $x^D \equiv 1$ relativa a um modulo multiplo qualquer, mas ainda o theorema que nos dá o numero das suas raizes, e a investigação da existencia de raizes primitivas, e as formulas da sua determinação.

No capitulo IX, em que consideramos geralmente a congruencia $ax^s \equiv b$ para um modulo qualquer, achar-se-ha todas as condições geraes da sua possibilidade; o processo de abaixamento do seu gráu (§§ 122 a 124), e uma extensa investigação, que nos parece inteiramente nova, sobre as propriedades e calculo dos *radicaes modulares* (§§ 125 a 157), theoria que além do interesse que póde offerecer para a resolução daquella congruencia, tem muitos pontos de contacto notaveis com a theoria dos radicaes ordinarios.

....

O pensamento que principalmente nos inspirou na redacção desta Memoria, pensamento que domina tambem em varias das demonstrações novas que apresentamos, foi darmos, quanto nos era possivel, processos e formulas directas para a resolução dos problemas relativos ás congruencias binomias, que são o ponto de partida da theoria dos numeros.

Os methodos indirectos e particularmente os só applicaveis ás questões numericas, são notavelmente inferiores ás formulas geraes e immediatas. É só por meio destas, e não com o auxilio daquelles processos, que póde servir a resolução das congruencias para o descobrimento e demonstração das propriedades dos numeros. Além dessa vantagem fundamental, as formulas geraes tem quasi sempre a importante utilidade pratica, de se prestarem ás applicações com muito maior facilidade, accrescendo ainda que ellas possuem exclusivamente essa belleza intellectual que resulta da absoluta generalisação, qualidade que não só as faz gravar mais profundamente na lembrança, mas que é tambem o caracter que continuamente tendem a adquirir todos os ramos das sciencias mathematicas, e que é o ultimo *desideratum* da sua perfectibilidade.

1.

NOÇÕES PRELIMINARES.

3. A fim de dar a este nosso trabalho uma certa unidade scientifica, de modo que possa servir como introducção ao completo estudo sobre a theoria dos numeros, pareceu-nos conveniente começar por varias considerações preliminares ácêrca de algumas noções e principios, que não é uso serem tratados nos livros elementares.

Todas as letras que empregarmos designam numeros inteiros. Pelas letras I, i, i', i'', i_n, ι, etc. exprimiremos unicamente os numeros impares. Em vez de escrever as equações indeterminadas ao modo ordinario, vg.

$$ax + by = c,$$

empregaremos quasi sempre uma notação analoga á de Gauss, isto é, escreveremos

(1) $$ax \equiv c \,\mathrm{M}\, b, \quad \text{ou} \quad by \equiv c \,\mathrm{M}\, a,$$

expressões mais simples que as daquelle geometra

$$ax \equiv c \text{ (mod. } b); \quad by \equiv c \text{ (mod. } a).$$

As formulas (1) denominam-se *congruencias*, e vg. a primeira dellas exprime que c é o resto da divisão de ax por b; a este divisor dá-se o nome de *modulo*. Nessa divisão emprega-se a palavra *resto*, ou *residuo* n'um sentido mais amplo que na arithmetica, pois que o consideramos como podendo ser negativo, ou maior que o divisor. O modulo considera-se sempre como positivo. A congruencia

$$ax \equiv c \,\mathrm{M}\, b$$

diz pois unicamente que $ax - c$ é divisivel por b, e lê-se *ax congruo com c para o modulo b*. Nessa congruencia é *c o residuo de ax para o modulo b*, ou tambem *ax o residuo de c para o mesmo modulo*. Donde se vê que um numero qualquer $\pm A$ póde ter infinitos residuos para o modulo p; chama-se *residuo minimo* o menor numero positivo r, tal que $\pm A - r$ seja divisivel por p.

Quando se escrevem differentes congruencias relativas ao mesmo modulo, basta exprimir este na primeira dellas.

A notação das congruencias tem a grande vantagem de poderem essas expressões ser tratadas como equações, porque effectivamente gosam de propriedades inteiramente analogas ás destas. Póde dizer-se até, que as congruencias são uma especie de equações, em que de algum modo se considera o modulo como zero. Com effeito é facil de ver, que da congruencia

$$A \equiv B \,\mathrm{M}\, p \tag{2}$$

deduz-se

$$A \pm mp \equiv B \pm m'p\,; \quad pA \equiv pB \equiv 0,$$

e immediatamente se reconhece a analogia destas conclusões com o que aconteceria, se a primeira congruencia se convertesse n'uma equação, e se supposessemos $p = 0$.

4. Ver-se-ha tambem a inteira similhança das seguintes propriedades com o que correspondentemente se verifica nas equações, e que são mui faceis de demonstrar, convertendo qualquer congruencia como (2) na equação equivalente

$$A = B + mp.$$

1.º Podem juntar-se, ou tirar-se quantidades iguaes a ambos os membros de uma congruencia, ou passar um termo de um para outro membro, mudando de signal.

2.º A somma de todos os primeiros membros de varias congruencias referidas ao modulo p, é congrua para o mesmo modulo com a somma de todos os segundos membros.

3.º Uma congruencia subsiste multiplicando ambos os membros pelo mesmo numero, ou dividindo-os por um numero que seja primo com o modulo.

4.º Se o divisor não é primo com o modulo, dividindo ambos os membros por aquelle divisor, teremos uma nova congruencia, cujo modulo será o quociente do primeiro dividido pelo maximo divisor entre este, e o dito divisor.

5.º Podem multiplicar-se ordenadamente os membros de varias congruencias relativas ao mesmo modulo, que o será tambem da congruencia resultante,

6.º Podem elevar-se, sem alteração do modulo, ambos os membros de uma congruencia a uma potencia qualquer inteira e positiva.

7.º Os numeros congruos para um modulo qualquer tem iguaes residuos minimos; e se forem *incongruos*, os residuos minimos serão differentes.

8.º Das duas congruencias

$$Aa \equiv Bb \,\mathrm{M}\, p, \quad a \equiv b,$$

concluiremos tambem, dividindo ordenadamente os seus membros,

$$A \equiv B,$$

com tanto porém, que um dos numeros a, b, e por conseguinte ambos, sejam primos com p. Com effeito, se a ultima congruencia é inexacta, será

$$A \equiv B + r,$$

sendo numericamente $r < p$. Desta e da segunda das propostas tira-se

$$Aa \equiv Bb + rb,$$

e pela primeira

$$rb \equiv 0:$$

ora sendo b primo com p, seria r divisivel por p, o que é impossivel, porquanto numericamente $r < p$: logo necessariamente se verificará o theorema enunciado.

5. Além das analogias precedentes entre as equações e as congruencias, a notação de Gauss, de que usamos, tem ainda a vantagem de representar os problemas relativos á analyse indeterminada, segundo a natureza que elles teem as mais das vezes; pois que frequentemente se pede nesses problemas, quaes devem ser os valores de certas incognitas, para que uma dada funcção dellas se torne divisivel por um modulo qualquer, sem nos importar conhecer o quociente, que effectivamente se não exprime nas congruencias. Chama-se raiz das congruencias (1), ou mais geralmente da congruencia do gráu m

$$(3) \qquad a x^m + b x^{m-1} + c x^{m-2} + \ldots + u \equiv 0 \text{ M } p$$

qualquer valor de x, que lhe satisfaz. Como é facil de reconhecer, se houver uma raiz $x_{\prime}$ de (3), dessa poder-se-ha deduzir uma infinidade de outros numeros dotados da mesma propriedade, isto é, podemos juntar a $x_{\prime}$ *qualquer multiplo do zero relativo* p. Chamam-se porém propriamente raizes de (3) os numeros positivos e menores que p, que lhe satisfazem.

Na congruencia (3) devem suppor-se todos os coefficientes não divisiveis por p; aliás poderiamos supprimir os termos correspondentes, e a congruencia resultante teria as mesmas raizes da proposta. Podem tambem considerar-se congruencias, em que appareça explicitamente mais de uma indeterminada. O gráu destas congruencias determina-se como nas equações.

6. A congruencia (3), em que suppomos p primo absoluto, e primo com a, não póde ter mais de m raizes. Este theorema importante, que é devido a Lagrange, póde provar-se por qualquer dos methodos, que servem para a demonstração da analoga propriedade, que se verifica nas equações. Podemos tambem proceder da seguinte maneira: seja α uma das raizes de (3), será

$$a \alpha^m + b \alpha^{m-1} + c \alpha^{m-2} + \ldots + u \equiv 0,$$

que subtrahida de (3) dará

$$a(x^m - \alpha^m) + b(x^{m-1} - \alpha^{m-1}) + c(x^{m-2} - \alpha^{m-2}) + \ldots + t(x - \alpha) \equiv 0,$$

que evidentemente se transforma em

$$(4) \qquad (x - \alpha)(a x^{m-1} + b' x^{m-2} + c' x^{m-3} + \ldots + t') \equiv 0.$$

As raizes de (3) são as de (4), e reciprocamente: e todas as raizes de (4) são todos os numeros menores que p, que por este modulo tornam divisivel qualquer dos dois factores do primeiro membro de (4). Ora para o factor $x-\alpha$ só ha uma raiz $<p$, que satisfaça a essa condição; e para o outro factor haverá tantas quantas são as raizes da congruencia

$$ax^{m-1}+b'x^{m-2}+\ldots+t\equiv 0\,;$$

logo se designarmos geralmente por ψn o maior numero de raizes que póde ter a congruencia

$$ax^{n}+qx^{n-1}+rx^{n-2}+\ldots\equiv 0,$$

teremos

$$\begin{aligned}\psi m=1+\psi(m-1)=2+\psi(m-2)=3+\psi(m-3)=\ldots\\ =m-1+\psi 1=m+\psi 0.\end{aligned}$$

Ora $\psi 0$ corresponde visivelmente á congruencia

$$a\equiv 0,$$

que é absurda na hypothese adoptada de não ser a divisivel por p; logo $\psi 0=0$, e por conseguinte

$$\psi m=m.$$

7. Um dos theoremas de uso mais frequente na theoria dos numeros, é a formula que, para qualquer grandeza de N, dá o numero, que designaremos por φN, de numeros não maiores que N e primos com elle. Se $N=1$, $\varphi N=1$; e se $N>1$, os numeros primos com N, que consideramos, são todos menores que N.

Suppondo pois que os factores primos diversos de N são A, B, C, etc., isto é, sendo

$$N=A^{\alpha}B^{\beta}C^{\gamma}\text{ etc.},$$

o theorema indicado é

$$\text{(5)}\qquad \varphi N=A^{\alpha-1}B^{\beta-1}C^{\gamma-1}\ldots(A-1)(B-1)(C-1)\ldots.$$

Para demonstrar esta formula empregaremos uma notação, que pode vantajosamente servir em outros casos. Supponhamos que n'uma serie S qualquer de numeros (que consideramos *reunidos*, e não *sommados*, pois que mesmo alguns delles podem ser negativos, sem que dahi resulte *reducção* alguma) se pede quaes são aquelles que gosam de certa propriedade a; designaremos por S_a a *reunião* desses numeros; similhantemente serão S_b, $S_{b,c}$, $S_{a,b,c}$, etc. a reunião dos termos de S dotados da propriedade b, ou dotados simultaneamente das propriedades b, c, etc.; e será vg. S_{b_c} a reunião dos termos de S_b dotados da propriedade c. É facil de ver que será vg.

$$S_{a_b} = S_{a,b}; \quad S_{a_{b_c}} = S_{a,b_c} = S_{a,b,c}; \text{ etc.}$$

Do mesmo modo representaremos por ${}^aS$, ${}^{a,b}S$, ${}^{{}^b a}S$ a reunião dos termos de S privados da propriedade a, ou das duas a, b, ou a reunião dos termos de ${}^aS$ privados da propriedade b etc.

Se a reunião S^{I} fôr obtida pela suppressão dos termos das reuniões S^{II}, S^{III}, etc. os quaes compõem as reuniões S^{IV}, S^{V}, etc., isto é, sendo

$$S^{\mathrm{I}} = S^{\mathrm{II}} + S^{\mathrm{III}} + \ldots - S^{\mathrm{IV}} - S^{\mathrm{V}} \ldots \tag{6}$$

é claro, que será vg.

$$S_a^{\mathrm{I}} = S_a^{\mathrm{II}} + S_a^{\mathrm{III}} \ldots - S_a^{\mathrm{IV}} - S_a^{\mathrm{V}} \ldots$$

Suppostas estas noções teremos

$${}^aS = S - S_a = S\,[1 - {}_a], \tag{7}$$

entendendo-se pela ultima notação symbolica, que a letra a na multiplicação passa para indice.

De (7) conclue-se

$$\left\{\begin{aligned} {}^{b,a}S &= {}^{{}^b a}S = S\,[1 - {}_a]\,[1 - {}_b] \\ {}^{c,b,a}S &= {}^{{}^c b,a}S = S\,[1 - {}_a]\,[1 - {}_b]\,[1 - {}_c] \end{aligned}\right. \tag{8}$$

isto é, em geral

$${}^{c,b,a}S = S\,[1 - {}_a]\,[1 - {}_b]\,[1 - {}_c] \cdots \tag{9}$$

entendendo-se sempre que os productos dos numeros a, b, c, etc. passam a indices compostos das series respectivas, e que qualquer indice composto $a_{b_{c\dots}}$ equivale a um indice simples a, b, c.... A formula (9) não só nos dará a *reunião* de todos os termos de que se compõe ${}^{\dots c,b,a}S$, mas tambem nos fornece immediatamente a sua *somma*, uma vez que no segundo membro realisemos a somma algebrica de todos os valores S_a, S_b, etc., que entram naquelle desenvolvimento.

A mesma formula dá-nos tambem immediatamente o numero dos numeros contidos em ${}^{\dots c,b,a}S$; por quanto se designarmos esse numero por $\psi\,{}^{\dots c,b,a}S$, e se a caracteristica ψ tiver uma significação analoga, applicada ás series additivas e subtractivas do segundo membro de (9), é claro que teremos

$$(10)\qquad \psi\,{}^{\dots c,b,a}S = \psi S\,[1-{}_a]\,[1-{}_b]\,[1-{}_c]\dots$$

Esta formula contem, como um caso muito particular a demonstração da equação (5). Com effeito, se a serie S fôr a dos numeros naturaes $1, 2, 3, \dots N = A^\alpha B^\beta C^\gamma \dots$; se a indicar a divisibilidade de um dos numeros dessa serie por A; se b, c, etc. indicarem similhantemente a divisibilidade por B, C, etc., teremos, por serem A, B, C, etc. primos entre si,

$$S_a = S_A;\ S_b = S_B;\ \text{etc.}\ S_{a.b} = S_{AB};\ S_{a.b.c} = S_{ABC};\ \text{etc.}\ {}^{\dots c,b,a}S = {}^{\dots C,B,A}S;$$

e

$$\psi S_a = \frac{N}{A};\ \psi S_b = \frac{N}{B};\ \psi S_{a.b} = \frac{N}{AB};\ \text{etc.}\ \psi\,{}^{\dots c,b,a}S = \varphi N,$$

o que mudará (10) em

$$\varphi N = N\left(1-\frac{1}{A}\right)\left(1-\frac{1}{B}\right)\left(1-\frac{1}{C}\right)\dots$$

$$= A^{\alpha-1}B^{\beta-1}C^{\gamma-1}\dots(A-1)(B-1)(C-1)\dots$$

Se fôr simplesmente $N = A^\alpha$, teremos

$$\varphi N = A^{\alpha-1}(A-1);$$

e se N fôr um numero primo absoluto, será

$$\varphi N = N - 1.$$

8. Da formula (5) é facil de concluir, que se A', B' forem primos entre si, teremos

$$(11) \qquad \varphi N = \varphi A' B' = \varphi A' \times \varphi B',$$

pois que sendo C, D, etc. os factores primos de A', e E, F, etc. os de B', os quaes serão primos com os primeiros, será

$$A' = C^\alpha D^\beta \ldots;\ B' = E^\gamma F^\delta \ldots;$$

$$\varphi N = \varphi A' B' = \varphi C^\alpha D^\beta \ldots E^\gamma F^\delta \ldots$$

$$= C^{\alpha - 1} D^{\beta - 1} \ldots E^{\gamma - 1} F^{\delta - 1} \ldots (C-1)(D-1)\ldots(E-1)(F-1)\ldots$$

$$= \varphi C^\alpha D^\beta \ldots \times \varphi E^\gamma F^\delta \ldots = \varphi A' \times \varphi B'.$$

De (11) deduz-se, sendo A', B', C', etc. primos entre si,

$$(12) \qquad \varphi A' B' C' \ldots = \varphi A' \varphi B' C' \ldots = \varphi A' \varphi B' \varphi C' \ldots$$

9. A formula (5) foi descoberta por Euler (*Novi Comment. Ac. Sc. Imp. Petrop.* T. VIII) que a demonstrou por um modo summamente engenhoso e geral. Posteriormente (*Acta Ac. Sc. Imp. Petrop.* 1780, pars II) publicou duas outras demonstrações da mesma formula, que de certo não tem o merito da primeira. Em uma dellas emprega-se uma longa e minuciosa inducção, que pela sua crescente difficuldade deixa bastante obscuridade no espirito; a outra, como Euler confessa, foi-lhe suggerida pelo exame das operações indicadas que dão a funcção φN. Esta demonstração, aliás extremamente simples, é, como bem observa Poinsot (memoria acima citada), inteiramente destituida de rigor. Este ultimo geometra reformou o que nessa demonstração havia de inconsistente; mas deve advertir-se que a inducção, de que usa Poinsot, requer, para ser indefinidamente continuada, uma grande contensão de espirito, o que faz que a sua apparente facilidade não se prova pela pouca extensão com que esse raciocinio foi redigido.

Gauss (obra citada) depois de demonstrar, como é facil, a verdade da formula (5) para quando N é potencia de um numero primo, passa a fundar o caso geral na demonstração da formula (12). O seu processo, postoque extremamente engenhoso, é innegavelmente menos simples que o de Poinsot.

Legendre *(Théorie des nombres 3.e edit.)* aproveitando tambem, para a demonstração, a forma do valor do φN, depois de feitas as operações respectivas, empregou uma inducção bastante laboriosa, que para convencer completamente, é necessario ainda que o leitor suppra alguns desenvolvimentos, que explicitamente se não encontram no texto.

O Sñr. F. S. Margiochi nas suas *Instituições mathematicas*, que brevemente verão a luz publica, contemplando a fórma geral daquelle desenvolvimento, procurou demonstrar que ella equivale a um processo successivo para achar os numeros menores que N, e primos com elle; mas a inducção de que faz uso esse distincto analysta está mui longe de ser evidente.

A demonstração que demos, que julgamos não ser mais longa que a de Poinsot, principalmente se a restringirmos ás condições particulares do theorema, para que especialmente a empregámos, tem sobre aquella, nos parece, a vantagem de não exigir a grande contensão de espirito indispensavel a uma enumeração, em que continuamente crescem os elementos, que se devem ter presentes ao entendimento.

10. As formulas (9,10), que teem ainda a vantagem de exprimir theoremas muito mais geraes que o de Euler, podem servir commodamente para a demonstração de formulas importantes e curiosas, sempre que seja possivel determinar cada um dos symbolos S_x, ou ψS_x de maneira, que a reunião delles possa reduzir-se a uma formula facil de calcular.

Por exemplo, a equação symbolica (9) dar-nos-ha, por meio de uma expressão elegante, a somma de todos os numeros não maiores que N, e primos com elle.

Para o conseguir, considerando o segundo membro de (9) como uma somma algebrica de todas as expressões symbolicas, que nelle entram, determinemos o valor de qualquer dellas.

É facil de ver que teremos

$$S_1 = 1 + 2 + 3 + \ldots + N = \frac{N}{2}(N+1);$$

$$S_a = S_A = A + 2A + 3A + \ldots + A^{\alpha} B^{\beta} C^{\gamma} \ldots$$

$$=\frac{A+A^{a}\ B^{\beta}\ C^{\gamma}\ldots}{2}\times A^{a-1}B^{\beta}C^{\gamma}\ldots=\frac{N}{2}\left(\frac{N}{A}+1\right);$$

e similhantemente

$$S_b=\frac{N}{2}\left(\frac{N}{B}+1\right);\ \text{etc.}\ S_{a,b}=\frac{N}{2}\left(\frac{N}{AB}+1\right);\ \text{etc. etc.}$$

Para obter o valor procurado, devemos reunir as duas sommas, que resultam da addição dos primeiros termos e da addição dos segundos termos dos binomios, que representam os valores dos symbolos, que entram no segundo membro de (9). Para termos a primeira destas sommas, basta em (9) substituir S por N; a, b, c, etc. por $\frac{1}{A}$, $\frac{1}{B}$, $\frac{1}{C}$, etc., e multiplicar o resultado por $\frac{N}{2}$, isto é, teremos

$$\frac{N}{2}\cdot N\left(1-\frac{1}{A}\right)\left(1-\frac{1}{B}\right)\left(1-\frac{1}{C}\right)\ldots=\frac{N}{2}\varphi N.$$

Os segundos termos dos binomios substituidos em (9) dão o mesmo resultado, que se obteria suppondo

$$S_1=S_a=S_b=\ldots=S_{a,b}=S_{a,c}=\ldots=\frac{N}{2},$$

isto é, acharemos

$$\frac{N}{2}(1-1)(1-1)(1-1)\ldots=0;$$

logo se designarmos por ΣN a somma de todos os numeros não maiores que N, e primos com elle, será

$$\Sigma N=\frac{N}{2}\varphi N. \tag{13}$$

Se N for um numero primo, como então $\varphi N=N-1$, teremos

$$\Sigma N=\frac{N(N-1)}{2},$$

como aliás era evidente, pois que

$$\Sigma N = 1 + 2 + 3 + \ldots + (N - 1).$$

Para $N = 1$, e para $N = 2$, será

$$\Sigma N = 1;$$

este resultado não será porêm comprehendido na formula (13) para $N = 1$.

Se N tem um factor impar > 1, pela fórma de φN se reconhece que esta funcção é divisivel por 2, e por conseguinte (13) demonstra que ΣN é multiplo de N.

Chegaremos similhantemente á mesma conclusão, se for $N = 2^{\alpha}$, sendo $\alpha > 1$.

Logo ΣN é sempre multiplo de N, excepto os casos unicos de ser $N = 1$, ou $N = 2$.

11. Passaremos agora a demonstrar outro theorema, cuja applicação é frequentissima na theoria dos numeros. Seja a um numero qualquer, e p um modulo primo com a; será sempre

$$(14) \qquad a^{\phi p} \equiv \mathrm{M}\, p,$$

formula que, quando p for numero primo, se reduz a

$$(15) \qquad a^{p-1} \equiv 1\ \mathrm{M}\, p.$$

O theorema (15) tem o nome de Fermat seu inventor, que o publicou sem demonstração (*Fermatii Opera Math.* 1679 *pag.* 163). Euler tendo por algum tempo procurado infructuosamente essa demonstração (*Comm. Acad. Petrop.* T. VI. *pag.* 106) conseguiu finalmente obtel-a (*Comm. Acad. Petrop.* T. VIII.) por meio de uma simples e rigorosa inducção. Posteriormente o mesmo analysta publicou outra demonstração fundada em principios mais elementares. A demonstração de Gauss (obra citada § LI.) é notavel pela sua simplicidade, e por demonstrar um theorema muito mais geral que o de Fermat. Tem ainda sido publicadas varias outras demonstrações da formula (15), bem como da sua generalisação (14), que é devida a Euler, que primeiro a demonstrou (*Nova Acta Petrop.* T. VIII. *pag.* 75).

Apresentaremos a demonstração da formula (14) dada por Poinsot (memoria citada pag. 32), por nos parecer a mais simples e elementar de todas as que tem sido publicadas.

Seja

(16) $$1, \alpha, \beta, \gamma, \delta, \ldots (p-1)$$

a serie dos φp numeros menores que p, e primos com elle; multiplicando-os todos por um qualquer delles, diverso de 1, acharemos

(17) $$a, a\alpha, a\beta, a\gamma, a\delta, \ldots a(p-1);$$

cada um destes numeros é visivelmente primo com p; demais se os dividirmos successivamente por p, os φp residuos achados, que são tambem primos com p, serão todos diversos, pois que se vg. $a\alpha$, $a\gamma$ dessem o mesmo residuo, $a(\alpha-\gamma)$ seria divisivel por p, e como com este é primo a, seria $\alpha-\gamma<p$ divisivel por p, o que é impossivel; logo aquelles residuos são exactamente os φp numeros (16). Podemos pois formar φp congruencias, todas relativas ao modulo p, em que sejam primeiros membros os numeros (17), e segundos membros os numeros (16), postoque estes possam apparecer n'uma ordem differente dos primeiros. Multiplicando ordenadamente essas congruencias, acharemos

$$1.\alpha.\beta.\gamma\ldots(p-1)\,a^{\varphi p} \equiv 1.\alpha.\beta.\gamma\ldots(p-1)\,\mathrm{M}p,$$

donde se conclue, por ser p primo com os numeros (16),

$$a^{\varphi p} \equiv 1.$$

Não só a demonstração que damos suppõe a primo com p, mas effectivamente se reconhece que (14) não póde subsistir, uma vez que a, p tenham um divisor commum, o qual não póde dividir o segundo membro 1.

12. De (14) conclue-se

$$a^{m\varphi p} \equiv 1;$$

logo se for

$$n = m\varphi p + r, \text{ e } a^n \equiv 1 \equiv a^{m\varphi p}.a^r \equiv a^{m\varphi p},$$

será (§ 4, 3.º)

$$a^r \equiv 1.$$

13. Suppondo ser $n < \varphi p$ o menor valor de x que satisfaz á congruencia

$$a^x \equiv 1,$$

é forçoso que seja n divisor de φp. Com effeito, se podesse ser

$$\varphi p = qn + r,$$

sendo $r < n$, e diverso de zero, teriamos

$$a^{nq} \equiv 1;\ 1 \equiv a^{\varphi p} \equiv a^{nq} \cdot a^r \equiv a^r,$$

isto é, haveria um valor $x = r < n$, que satisfaria a

$$a^x \equiv 1,$$

contra a hypothese.

Vê-se pois tambem, que sendo n o menor expoente de a, que faz

$$a^n \equiv 1;$$

se tivermos

$$m = qn + r, \text{ sendo } r < n,$$

será

$$a^m = a^{qn} \cdot a^r \equiv a^r.$$

Logo se for $a^m \equiv 1$, será necessariamente $r = 0$, $m = qn$.

14. Tendo pois n a significação acima dada, diz-se que a é *raiz primitiva* da congruencia

$$x^n \equiv 1.$$

Se p é numero primo, qualquer raiz primitiva da congruencia

$$x^{p-1} \equiv 1$$

diz-se tambem *raiz primitiva* do numero p.

Adiante demonstraremos a existencia, e as propriedades destas especies de raizes.

15. Sendo a^n a menor potencia de a, que produz o residuo 1 para o modulo p, vê-se que os termos da serie

$$a,\ a^2,\ a^3,\ a^4,\ \ldots\ a^n$$

darão, para o mesmo modulo, n residuos diversos; pois que se vg. tivessemos a^α, a^β com o mesmo residuo, seria

$$a^\alpha \equiv a^\beta;$$

e suppondo $\alpha > \beta$,

$$a^{\alpha-\beta} \equiv 1,$$

o que é impossivel, pois $\alpha - \beta < n$.

A serie indefinida das potencias de a

$$a,\ a^2,\ a^3,\ a^4, \ldots$$

reproduzirá por tanto, de n em n termos, e pela mesma ordem, os n residuos que correspondem aos n primeiros termos.

Se a for raiz primitiva de p, será $n = p - 1$.

16. Ao theorema de Euler pode dar-se, como vamos mostrar, uma notavel generalisação.

Com effeito, seja um numero qualquer $p = abcd\ldots$, sendo os factores a, b, c, etc. primos entre si, e n o seu numero; teremos sempre

$$a^{\frac{\varphi p}{\varphi a}} + b^{\frac{\varphi p}{\varphi b}} + c^{\frac{\varphi p}{\varphi c}} + \ldots \equiv n - 1 \text{ M} p; \tag{18}$$

porquanto sendo a divisor de

$$a^{\frac{\varphi p}{\varphi a}},\quad b^{\frac{\varphi p}{\varphi b}} - 1 = b^{\varphi a \varphi c \ldots} - 1,\quad c^{\frac{\varphi p}{\varphi c}} - 1,\ \text{etc.},$$

a congruencia precedente é satisfeita, substituindo o modulo p por a; e como se dirá o mesmo em relação aos modulos b, c, etc., e pois que esses factores são primos entre si, a dita congruencia é verdadeira tambem para o modulo $p = abc\ldots$

Se for $p = ab$, (18) reduz-se a

$$a^{\varphi b} + b^{\varphi a} \equiv 1 \text{ M} ab,$$

que comprehende o theorema de Euler

$$a^{\varphi b} \equiv 1 \text{ M} b.$$

II.

RESOLUÇÃO DAS CONGRUENCIAS LINEARES.

17. A congruencia

$$(19) \qquad ax \equiv c \text{ M } b$$

é indeterminada, isto é, satisfaz a ella qualquer valor de x, quando a, c são ambos divisiveis por b.

Será impossivel, se, tendo a, b um divisor qualquer, este não dividir c.

Se for d o maior divisor commum de a, c, e se tivermos $d = d' d''$, sendo d' o maior divisor commum entre d, e b, da congruencia (19) conclue-se

$$\frac{a}{d} x \equiv \frac{c}{d} \text{ M } \frac{b}{d'}.$$

Para resolver pois geralmente a congruencia (19), podemos suppor que a, c são primos entre si, e do mesmo modo a, b.

A resolução da congruencia (19), ou da equação equivalente

$$ax + by = c\,,$$

em que x, y devem ser numeros inteiros, foi primeiro achada por Bachet de Meziriac *(Problèmes plaisans et délectables 2.^e edit.)*. Deve-se a Lagrange *(Additions à l'algèbre d'Euler)* o ter reparado a injustiça com que os geometras esqueceram aquelle serviço.

Euler, ignorando sem duvida a descoberta de Bachet, publicou *(Comm. Acad. Petrop.* T. VII.*)* um processo, que exigindo as mesmas operações que o de Bachet, apresenta-se porêm de um modo muito mais natural. É o methodo das *indeterminadas*, que se encontra em quasi todos os tractados elementares de Algebra.

Lagrange *(Hist. de l'Acad. de Berlin* 1767 *pag.* 175*)* reflectindo, que as operações do methodo de Euler são exactamente as precisas para determinar as differentes *reduzidas* da fracção $\frac{a}{b}$, ou $\frac{b}{a}$, achou que a penultima reduzida $\frac{x'}{y'}$ de $\frac{b}{a}$, dava uma solução da equação

$$ax - by = \pm 1\,,$$

donde se conclue facilmente a solução geral de

$$ax - by = \pm c.$$

Poinsot publicou (obra citada) duas soluções novas da congruencia

$$ax \equiv 1 \text{ M } b\,,$$

as quaes desembaraçadas da elegante representação geometrica, que o author lhes deu, reduzem-se ao seguinte processo pratico. Pelo primeiro methodo substituem-se successivamente na congruencia precedente todos os numeros 1, 2, 3, etc. menores que b, até achar um que satisfaça. Este processo, considerado como operação arithmetica, não tem pois importancia alguma pratica: é apenas uma successiva verificação. O segundo processo, encarado sob o ponto de vista arithmetico, tem decidida utilidade pratica, se lhe tirarmos a forma de ensaio successivo, que o author lhe dá, para o converter, como abaixo faremos, em uma formula directa (*).

(*) Isto, bem como o que se segue relativamente ás formulas directas de resolução das congruencias lineares, tinha sido escripto antes de vermos na 3.ª edição de Legen-

Por esse processo devem formar-se as potencias successivas a, a^2, a^3, etc., tendo o cuidado de substituir a cada uma o seu residuo minimo para o modulo b, até que se chegue a uma potencia

$$a^m \equiv 1 \text{ M } b,$$

e então visivelmente será

$$x = a^{m-1}.$$

O numero m, que indica o numero de operações que se devem effeituar, nunca poderá ser maior que o numero que indica o numero de numeros menores que b, e primos com elle; mas este processo, que tambem é uma simples verificação successiva, não tem vantagem pratica em relação ao precedente quando for $m = \varphi b$.

18. Passemos agora a resolver directamente a congruencia

$$ax \equiv c \text{ M } b, \tag{20}$$

em que supponios a positivo, e a, b primos entre si.

Se houver duas soluções x', x'', isto é, se tivermos

$$ax' \equiv c;\ ax'' \equiv c;$$

deduziremos

$$a\ (x'' - x') \equiv 0;$$

logo $x'' - x'$ é divisivel por b, e por conseguinte a formula geral de todas as soluções de (20) será

$$x = x' + zb,$$

sendo z um numero qualquer. Vê-se por tanto que todas as raizes de (20) são congruas para o modulo b, e reciprocamente todos os numeros congruos com uma raiz qualquer x' são tambem raizes. E como as quantidades congruas se podem considerar equivalentes, podemos dizer que a congruencia (20) tem uma só raiz, ou escrever

$$x \equiv x' \text{ M } b,$$

---

dre pag. 199 (publicação que, convem notar, é muito anterior á memoria de Poinsot) uma formula directa de resolução, que coincide com a nossa (21). Feita esta declaração, não julgámos necessario alterar a nossa primitiva redacção, onde se contem os desenvolvimentos precisos para se conhecer a vantagem pratica daquella formula, contra a opinião de Legendre, que aliàs allude a este methodo muito concisa e incidentemente.

proposição que aliás já demonstrámos, porque é comprehendida no que provámos (§ 6).

Resta pois unicamente determinar o valor x'. Como

$$a^{\varphi b} \equiv 1 \text{ , será } ca^{\varphi b} \equiv c \text{ ;}$$

logo fazendo

$$x' = ca^{\varphi b - 1},$$

será

$$ax' \equiv c,$$

e por conseguinte teremos geralmente

$$x = ca^{\varphi b - 1} + zb. \tag{21}$$

19. Consideremos agora a equação do primeiro grau a duas indeterminadas, em que a, b são primos entre si,

$$ax + by = c;$$

para determinar todos os valores inteiros x, y que lhe satisfazem, podemos sempre suppor que a, b são positivos, para o que bastará escrever a equação precedente da seguinte maneira

$$a\,(\pm\, x) + b\,(\pm\, y) = c. \tag{22}$$

Pelo que acima dissemos será

$$\pm\, x = ca^{\varphi b - 1} + zb, \tag{23}$$

e substituindo em (22), acha-se

$$\pm\, y = c\,\frac{1 - a^{\varphi b}}{b} - za, \tag{24}$$

valor em que evidentemente a expressão fraccionaria se reduz a um inteiro.

Se resolvessemos primeiramente (22) em relação a y, teriamos similhantemente

$$(25)\qquad \begin{cases} \pm x = c\,\dfrac{1 - b^{\varphi a}}{a} - z' b, \\ \pm\, y = c\, b^{\varphi a - 1} + z' a. \end{cases}$$

Se quizermos que os valores de $\pm x$, $\pm y$ tenham uma forma similhante, poderemos fazer

$$(26)\qquad \begin{cases} \pm x = c a^{\varphi b - 1} + z b\,; \\ \pm\, y = c b^{\varphi a - 1} + z' a\,; \end{cases}$$

para que estes dois valores satisfaçam á equação (22) devemos ter

$$c\,(a^{\varphi b} + b^{\varphi a}) + (z + z')\, ab = c,$$

donde

$$z + z' = -c\,\frac{a^{\varphi b} + b^{\varphi a} - 1}{ab}\,;$$

em que a fracção do segundo membro terá sempre um valor inteiro (§ 16).

Se fizermos

$$c\,\frac{a^{\varphi b} + b^{\varphi a} - 1}{ab} = N,$$

podemos suppor

$$z = -\tfrac{1}{2} N + u\,;$$

logo

$$z' = -\tfrac{1}{2} N - u\,;$$

devendo entender-se que se for N impar, será $u = \frac{i}{2}$, sendo i tambem impar. Substituindo estes valores em (26) e reduzindo, acharemos

$$\pm x = c\,.\,\frac{a^{\varphi b} - b^{\varphi a} + 1}{2a} + ub\,;$$

$$\pm y = c\,.\,\frac{b^{\varphi a} - a^{\varphi b} + 1}{2b} - ua.$$

20. As formulas (23, 24) que nos dão a resolução da equação (22), devem transformar-se do seguinte modo para vantagem da applicação numerica.

Designemos por $[a^{\varphi b-1}]$ o residuo minimo de $a^{\varphi b-1}$ para o modulo b: em logar dessas formulas escreveremos

$$(27)\qquad \begin{cases} \pm x = c\,[a^{\varphi b-1}] + zb\,; \\ \pm y = c\,\dfrac{1 - a\,[a^{\varphi b-1}]}{b} - za. \end{cases}$$

Com effeito reconhece-se primeiramente, que a fracção que entra no valor de $\pm y$ dá um numero inteiro, porquanto não fizemos mais que supprimir no numerador correspondente em (24) um multiplo de b.

Em segundo logar é facil de verificar, que os valores (27), substituidos em (22), tornam identica essa equação.

Quando se tratar simplesmente de resolver a congruencia

$$ax \equiv c \text{ M } b,$$

sendo a positivo, podemos tambem calcular simplesmente o valor geral

$$x \equiv [c]\,[a^{\varphi b-1}];$$

e por isso tambem para resolver a equação (22) podemos calcular o valor geral de

$$\pm x = [c]\,[a^{\varphi b-1}] + zb,$$

e deduzir o de y pela substituição do valor precedente em (22).

Na applicação a qualquer exemplo numerico será mui facil de reconhecer, que o calculo de $[a^{\varphi b-1}]$ é extremamente simples, advertindo que em geral

$$[a^{p+q+r+s\cdots}] = \Big[\,[a^p]\,[a^q]\,[a^r]\,[a^s]\ldots\Big], \text{ e}$$

$$[a^{pqr\cdots}] = \Big[\ldots[\,[a^p]^q\,]^r\ldots\Big].$$

Supponhamos vg. que é proposta a equação

$$31x+19y=181;$$

será

$$x\equiv[181][31]^{17}\ \mathrm{M}\ 19,$$

ou

$$x\equiv10[12]^{17},$$

e teremos

$$[12]^{16+1}\equiv12[144]^8\equiv12[11]^8\equiv12[121]^4\equiv12[7]^4\equiv12[49]^2$$

$$\equiv12[11]^2\equiv12\cdot7\equiv-7\times7\equiv-11\equiv8,$$

logo

$$x\equiv80\equiv4,\ \text{ou}\ x=4+19z,$$

valor que substituido na equação proposta dá

$$y=\frac{181-31x}{19}=9+\frac{10-31x}{19}=3-31z.$$

Se nos fosse dada a equação

$$37x+48y=200,$$

teriamos

$$y\equiv[200][48^{35}]\ \mathrm{M}\ 37\equiv15\,[11^{35}].$$

Ora empregando por simplicidade o signal $=$ em vez de $\equiv$, teremos

$$11^{35}=11^3\cdot11^{32}=11^3\cdot121^{16}=11^3\cdot10^{16}=11^3\cdot100^8$$

$$=11^3\cdot[-11]^8=11^3\cdot11^8,$$

e como se achou

$$11^{32}=11^8,\ \text{será}\ 11^8=11^2;$$

logo

$$11^{35}=11^3\cdot11^2=11\cdot11^4=11\times-11=-10,$$

e por conseguinte

$$y\equiv-150\equiv-2\equiv35,$$

e pela substituição na equação dada teremos o valor correspondente de x.

21. Pelos exemplos precedentes é facil de reconhecer as simplificações, que se effeituam na applicação numerica das nossas formulas, decompondo sempre as potencias a reduzir em productos de potencias 2^a, e introduzindo no calculo os residuos negativos. Vê-se que se tem a executar uma serie de operações todas similhantes; e se o processo do calculo se indica com clareza, frequentemente se observa, que os resultados, que se tem a obter, já se acham explicitamente indicados nas anteriores operações.

Se compararmos este methodo com o de Euler, ou com o de Lagrange, achar-se-ha, sem duvida, que o primeiro é mais simples, sobre tudo attendendo a que a facilidade de execução de um processo arithmetico qualquer, consiste particularmente na analogia e simplicidade das operações que se tem a effeituar, qualidades que seguramente serão reconhecidas no methodo exposto.

Se compararmos este methodo com o processo de Poinsot, ver-se-ha que neste ultimo será necessario em geral effeituar uma serie de operações muitissimo mais longa, pois se tem a calcular os residuos successivos a, a^2, a^3, etc. até chegar a

$$a^m \equiv 1 \, \mathrm{M} \, b,$$

ao passo que nas formulas directas acima transcriptas chega-se mui rapidamente a preencher o valor $m-1=\varphi b-1$.

É verdade que no methodo exposto requer-se, que seja conhecida uma das funcções φb, φa, o que poderia offerecer alguma difficuldade, se a determinação dos factores primos de a, ou de b, não podesse ser feita pelas regras simples que se usam na arithmetica. Então poderiamos recorrer á taboa dos numeros primos, e se a, ou b se não achassem nella, determinariamos os divisores primos de um desses numeros.

Em taes casos innegavelmente seria mais simples empregar o methodo de Euler, ou o de Lagrange. Mas então mesmo sempre será facil fazer depender a resolução de

$$a(\pm x)+b(\pm y)=c$$

da resolução de uma congruencia, para cujo modulo p conheçamos immediatamente o valor φp.

Com effeito, suppondo $a>b$, $a=bq+r$, sendo r positivo e $<b$, teremos

$$\pm y = \mp q x + \frac{c - r(\pm x)}{b},$$

donde

$$c - r(\pm x) = b z.$$

Se φr ainda não é conhecido, procedendo similhantemente acharemos

$$\pm x = -q' z + \frac{c - r' z}{r},$$

$$c - r' z = r z',$$

e assim por diante até achar um resto p, que nos dê facilmente φp. Resolveremos pois a ultima equação pelas nossas formulas, e faremos a substituição successiva nas equações precedentes.

22. Se tivessemos a resolver a congruencia

$$(28) \qquad ax + by + cz + \cdots \equiv k \, \mathrm{M} p,$$

deveremos suppor que não ha divisor algum de p, que o seja tambem de todos os coefficientes do primeiro membro; aliás k tambem seria divisivel por esse numero, uma vez que a congruencia seja possivel; por conseguinte dividindo-a toda, e o modulo, pelo maior divisor commum entre p, e os coefficientes a, b, c, etc., obteremos uma nova congruencia em que se dará a circumstancia, que a principio supposemos.

Nesta hypothese escolha-se um coefficiente a primo com p, deduziremos immediatamente de (28)

$$(29) \qquad x \equiv [a^{\varphi p - 1}](k - by - cz - \text{etc.});$$

de maneira que para quaesquer valores de y, z, etc. teremos os valores inteiros correspondentes de x.

Se porém fosse necessario obter x em funcção das outras incognitas, na hypothese de haver um maximo divisor $d > 1$ entre a e p, começariamos resolvendo a congruencia

$$(30) \qquad by + cz + \cdots \equiv k \, \mathrm{M} d,$$

e achado, por uma formula similhante a (29), o valor geral de uma das incognitas expresso nas outras, (28) mudar-se-hia em

$$\frac{a}{d}x \equiv \frac{k-by-cz-\text{etc.}}{d}\ \mathrm{M}\ \frac{p}{d};$$

e como $\frac{a}{d}$, $\frac{p}{d}$ são primos entre si, obteriamos finalmente

$$x \equiv \left[\left(\frac{a}{d}\right)^{\varphi \frac{p}{a} - 1}\right] \times \frac{k-by-cz-\text{etc.}}{d}.$$

Por meio deste processo poder-se-hia sempre achar em (30) vg. o valor de z expresso em $y, \ldots,$ mesmo quando c, d tivessem divisor commum.

23. Se houvesse muitas congruencias como (28), mas em numero menor que o das incognitas x, y, z, etc., obteriamos pela eliminação

$$(31) \qquad a'x + b'y + c'z + \cdots \equiv m'\,\mathrm{M}\,p,$$

em que teriamos de menos tantas incognitas quantas as congruencias dadas menos uma. De (31) deduziriamos x expresso em y, z, etc., e substituindo esse valor na congruencia precedentemente obtida, em que além de x, y, z, etc. entrasse outra incognita u, teriamos o valor desta, e assim por diante.

24. Supponhamos agora que temos a achar os valores de x, que satisfazem ás congruencias

$$(32) \qquad \left\{\begin{array}{l} ax \equiv \alpha\,\mathrm{M}\,A; \\ bx \equiv \beta\,\mathrm{M}\,B; \\ cx \equiv \gamma\,\mathrm{M}\,C; \\ \ldots\ldots\ldots\ldots \end{array}\right.$$

sendo A, B, C, etc. primos entre si.

Para que ellas sejam possiveis é necessario, que se vg. na primeira a, A tiverem um divisor, esse divída tambem α; e similhantemente nas outras congruencias. Logo em qualquer dellas podemos súppor que o coefficiente do primeiro termo é primo com o modulo.

É tambem facil de ver, que todos os valores de x serão congruos para o modulo composto $N = ABC\ldots$; por quanto sendo x', x'' duas soluções, pela primeira congruencia será $x' - x''$ divisivel por A; e pelas seguintes essa differença terá tambem os divisores B, C, etc.; logo será divisivel por N.

As formulas directas que acima demos para a resolução de qualquer das congruencias (32), conduzir-nos-hão facilmente a estabelecer o valor geral de x, que deve satisfazer ao systema (32). Com effeito teremos

$$(33)\quad x \equiv \alpha\left[\frac{N}{A}\left(a\frac{N}{A}\right)^{\varphi A-1}\right]+\beta\left[\frac{N}{B}\left(b\frac{N}{B}\right)^{\varphi B-1}\right]+\gamma\left[\frac{N}{C}\left(c\frac{N}{C}\right)^{\varphi C-1}\right]+\cdots \mathrm{M}\, N.$$

Para verificar a exactidão da formula (33), vejamos como ella satisfaz vg. á primeira das congruencias (32).

Como os termos do valor de x, que seguem o primeiro, são todos divisiveis por A, para fazer a substituição de x naquella congruencia basta suppor

$$x = \alpha\frac{N}{A}\left(a\frac{N}{A}\right)^{\varphi A-1};$$

será pois em relação ao modulo A

$$ax = \alpha\, a^{\varphi A}\left(\frac{N}{A}\right)^{\varphi A} \equiv \alpha.$$

Similhantemente se prova, que (33) satisfaz ás outras congruencias do grupo (32).

25. Em vez da formula (33) podemos empregar outra, que parecerá mais simples. Tomem-se os numeros q, r, s, etc., taes que

$$(34)\qquad q\frac{N}{A}+r\frac{N}{B}+s\frac{N}{C}+\text{etc.} \equiv 1\ \mathrm{M}\, N,$$

congruencia possivel (§ 22), e será

$$(35)\quad x \equiv \alpha\left[q\frac{N}{A}a^{\varphi A-1}\right]+\beta\left[r\frac{N}{B}b^{\varphi B-1}\right]+\gamma\left[s\frac{N}{C}c^{\varphi C-1}\right]+\text{etc.},$$

pois que vg. para que este valor satisfaça á primeira das congruencias (32), basta verificar

$$(36)\qquad x \equiv \alpha\left[q\frac{N}{A}a^{\varphi A-1}\right];$$

ora sendo

$$a^{\varphi A} \equiv 1 \text{ M } A, \quad \text{e} \quad q\frac{N}{A} \equiv 1,$$

pela condição (34), o valor (36) dá

$$a x \equiv \alpha.$$

Podemos, por simplicidade, fazer $q = r = s =$ etc., isto é, em vez da condição (34), satisfazer a

$$q\left[\frac{N}{A} + \frac{N}{B} + \frac{N}{C} + \text{etc.}\right] \equiv 1 \text{ M } N,$$

congruencia possivel, por ser o coefficiente de q primo com N. A formula (35) muda-se pois em

$$(37) \qquad x \equiv \alpha q\left[\frac{N}{A} a^{\varphi A - 1}\right] + \beta q\left[\frac{N}{B} b^{\varphi B - 1}\right] + \gamma q\left[\frac{N}{C} c^{\varphi C - 1}\right] + \text{etc.}$$

Suppondo $a = b = c = \cdots = 1$, a formula precedente reduz-se a

$$(38) \qquad x \equiv \alpha q \frac{N}{A} + \beta q \frac{N}{B} + \gamma q \frac{N}{C} + \text{etc.}$$

Esta formula é analoga ao processo de Gauss (obra citada § 36) para resolver as congruencias, cujos modulos são todos primos entre si,

$$x \equiv \alpha \text{ M } A, \quad x \equiv \beta \text{ M } B, \quad x \equiv \gamma \text{ M } C, \quad \text{etc.},$$

por quanto esse processo reduz-se a determinar os numeros α', β', γ', etc., taes que

$$\alpha' \equiv 1 \text{ M } A; \quad \beta' \equiv 1 \text{ M } B; \quad \gamma' \equiv 1 \text{ M } C; \quad \text{etc.}$$

$$\alpha' \equiv 0 \text{ M } \frac{N}{A}; \quad \beta' \equiv 0 \text{ M } \frac{N}{B}; \quad \gamma' \equiv 0 \text{ M } C; \quad \text{etc.},$$

e então será

$$x \equiv \alpha\alpha' + \beta\beta' + \gamma\gamma' + \text{etc. M } N.$$

26. As formulas directas (33, 35, 37, 38) de resolução das congruencias (32) tem, particularmente sobre os processos numericos, a vantagem de se prestarem com notavel facilidade para a solução d'uma serie de problemas, em que só devam variar α, β, γ, etc.

A formula (38), reduzindo o segundo membro ao seu residuo minimo para o modulo N, dar-nos-ha vg. todos os numeros menores que esse, e primos com elle; para o que basta substituir todos os systemas α, β, γ, etc., em que estes numeros sejam respectivamente menores que A, B, C, etc., e primos com elles. Com effeito qualquer numero primo com N deve dar para o modulo A um residuo α primo com elle; para B um residuo β primo com elle, etc. A formula dada por Poinsot para representar todos os numeros menores que N, e primos com elle (memoria citada, pag. 43), que equivale a

$$(38') \qquad x \equiv \alpha \frac{N}{A} + \beta \frac{N}{B} + \gamma \frac{N}{C} + \text{etc.}$$

tem, relativamente á nossa, a desvantagem de que para um systema qualquer de residuos α, β, γ, etc. relativos aos modulos A, B, C, etc., essa formula não dá um numero x a que effectivamente correspondam esses residuos.

27. Principalmente quando fôr consideravel o numero das congruencias (32), será para o calculo numerico incontestavelmente mais vantajosa, que as precedentes, a formula que passaremos a deduzir. Multiplicando ordenadamente essas congruencias por $\frac{N}{A}$, $\frac{N}{B}$, $\frac{N}{C}$, etc., e sommando os resultados obtem-se

$$(38'') \quad \left(a\frac{N}{A} + b\frac{N}{B} + c\frac{N}{C} + \text{etc.}\right) x \equiv \alpha \frac{N}{A} + \beta \frac{N}{B} + \gamma \frac{N}{C} + \text{etc. M} N.$$

Ora qualquer valor de x que resolve esta congruencia, que aliás é sempre possivel, satisfaz tambem ao grupo (32); por exemplo, a primeira destas congruencias é satisfeita por esse valor, porque de (38″) conclue-se

$$a\frac{N}{A} x \equiv \alpha \frac{N}{A} \text{M} A,$$

e como $\frac{N}{A}$ é primo com A, teremos

$$ax \equiv \alpha:$$

logo será expressão geral das raizes de (32) o valor de x deduzido de (38''), isto é,

$$x \equiv \left[\left(a\frac{N}{A}+b\frac{N}{B}+c\frac{N}{C}+\text{etc.}\right)^{\varphi N-1}\right]\left(\alpha\frac{N}{A}+\beta\frac{N}{B}+\gamma\frac{N}{C}+\text{etc.}\right) \text{M}\, N.$$

formula que comprehende a (38), quando suppozermos $a=b=c=\cdots=1$.

28. Supponhamos agora que não são primos entre si todos os modulos das congruencias (32). Decomponham-se A, B, C, etc. nos seus divisores primos, isto é, seja vg. $A=m^{\mu}n'p^{\pi}\ldots$; a primeira das congruencias (32) póde ser substituida por

$$(39)\qquad \begin{aligned} ax &\equiv \alpha\ \text{M}\ m^{\mu}\,; \\ ax &\equiv \alpha\ \text{M}\ n'\,; \\ ax &\equiv \alpha\ \text{M}\ p^{\pi}\,; \\ &\ldots\ldots\ldots\ldots \end{aligned}$$

Decomponham-se similhantemente as outras congruencias (32); se nas que resultarem apparecer vg.

$$(40)\qquad bx \equiv \beta\ \text{M}\ m^{\mu'};$$

e fôr $\mu' = > \mu$, deduz-se de (39) e (40) a congruencia de condição

$$(41)\qquad \beta b^{\varphi m^{\mu'}-1} \equiv \alpha a^{\varphi m^{\mu}-1}\ \text{M}\ m^{\mu},$$

a qual se não tiver logar, é impossivel o grupo (32).

Satisfeita (41), bastará em vez de (39, 40) resolver unicamente a ultima. Logo todas as k congruencias, que apparecerem na decomposição de (32), referidas a modulos potencias de m, equivalem áquella dessas congruencias, cujo modulo fôr a maxima potencia de m, e haverá $k-1$ congruencias de condição para que o grupo (32) seja possivel. Similhantemente acontecerá em relação ás outras congruencias componentes referidas a potencias de outro numero primo n, ou p, etc. Todas estas componentes ficarão desse modo reduzidas a um grupo, cujos modulos serão todos primos entre si; e dessas as que procedem da mesma congruencia (32), evidentemente se reduzem a uma só, cujo modulo é o producto dos modulos de todas ellas.

III.

RESOLUÇÃO DA CONGRUENCIA $x^2 \equiv 1$ PARA UM MODULO PRIMO.

29. Para os principios que temos a estabelecer neste capitulo, convem-nos demonstrar a seguinte proposição.

Sendo y, y' primos com p numero qualquer, e α o maior divisor commum entre A, e B, se p dividir $y^\alpha - y'^\alpha$, dividirá tambem os dois binomios $y^A - y'^A$, $y^B - y'^B$; e reciprocamente.

A proposição directa prova-se immediatamente, pois que vg.

$$y^A - y'^A = (y^\alpha - y'^\alpha)(y^{A-\alpha} + y'^\alpha y^{A-2\alpha} + \ldots + y'^{A-\alpha}).$$

Para demonstrar a proposição reciproca, supponhamos $A > B$; acharemos pela divisão

$$y^A - y'^A = y^{A-B}(y^B - y'^B) + y'^B(y^{A-B} - y'^{A-B});$$

logo, se p dividir os binomios $y^A - y'^A$, $y^B - y'^B$, dividirá $y^{A-B} - y'^{A-B}$;

e por conseguinte tambem $y^{A-2B}-y'^{A-2B}, \ldots y^{A-mB}-y'^{A-mB}$, sendo mB o maior multiplo de B contido em A. Vê-se pois que se p divide os dois primeiros binomios, divide $y^r-y'^r$, em que r é o resto $<B$ da divisão de A por B. Similhantemente p será divisor de $y^{r'}-y'^{r'}$, em que r' é o resto da divisão de B por r, e assim por diante: logo finalmente p dividirá $y^\alpha-y'^\alpha$, em que α é o maior divisor commum entre A, e B.

Da proposição demonstrada se conclue, que os dois binomios relativos aos expoentes A, B não podem ser simultaneamente divisiveis por p, uma vez que esses expoentes sejam primos entre si, e y, y' incongruos para o modulo p; por quanto sendo então $\alpha=1$, $y^\alpha-y'^\alpha$ não é divisivel por p.

30. Consideremos agora a congruencia

(42) $$x^{p-1}\equiv 1 \text{ M} p,$$

em que suppomos p primo. As suas $p-1$ raizes propriamente ditas serão (§ 11) os numeros

$$1,\ 2,\ 3,\ \ldots\ p-1.$$

Se porém nos fôr dada a congruencia

$$x^s\equiv 1,$$

as suas raizes achar-se-hão comprehendidas entre aquelles numeros. Digo agora que estas raizes são exactamente as da congruencia

$$x^{p'}\equiv 1,$$

em que p' é o maior divisor commum entre s, e $p-1$.

Com effeito, qualquer raiz a desta faz

$$a^{p'}-1\equiv 0;$$

logo (§ 29)

$$a^s-1\equiv 0;$$

reciprocamente verificando-se esta ultima, como é tambem

$$a^{p-1}-1\equiv 0,$$

conclue-se (§ 29)

$$a^{p'}-1\equiv 0.$$

Em consequencia disto, para indagar as propriedades das raizes de

$$x^s \equiv 1,$$

e para as determinar, substituiremos sempre essa congruencia por outra

$$(43) \qquad x^{p'} \equiv 1,$$

em que p' é divisor de $p-1$.

31. A congruencia (43) tem sempre p' raizes.

Com effeito,

$$x^{p-1}-1=(x^{p'}-1)(x^{p-p'-1}+x^{p-2p'-1}+\ldots+1);$$

ora havendo $p-1$ valores de x menores que p, que tornam o primeiro membro divisivel por p, e como no segundo factor do segundo membro não póde haver mais de $p-p'-1$ valores, que deem essa propriedade ao dito factor (§ 6), segue-se necessariamente que haverá p' valores que tornam $x^{p'}-1$ divisivel por p, isto é, a equação (43) terá p' raizes.

32. Sendo a uma raiz qualquer de (43), satisfarão a essa congruencia todos os termos da serie

$$a,\ a^2,\ a^3,\ a^4,\ a^5,\ \text{etc.}$$

Se a fôr raiz primitiva de (43), os residuos de todas essas potencias até ao gráu p' serão diversos (§ 15), e as p' raizes daquella congruencia serão

$$a,\ a^2,\ a^3,\ a^4,\ \ldots,\ a^{p'} \equiv 1.$$

Sendo ainda a raiz primitiva de (43), se fôr $p'=p-1$, a serie

$$a,\ a^2,\ a^3,\ \ldots\ a^{p-1} \equiv 1,$$

dará os $p-1$ residuos

$$1,\ 2,\ 3,\ \ldots\ p-1,$$

posto que não seguindo a mesma ordem.

Sendo $p'=<p-1$, e a qualquer raiz não primitiva de (43), se fôr n o menor expoente que faz

$$a^n \equiv 1,$$

a serie

$$a,\ a^2,\ a^3\ \ldots\ a^n,$$

conterá n raizes distinctas de (43).

O numero n será sempre divisor de p' (§ 13).

33. Qualquer congruencia (43) tem sempre um numero de raizes primitivas representado por $\varphi p'$.

Esta bella propriedade descoberta por Lambert *(Acta eruditorum*, 1769), foi primeiro demonstrada por Euler *(Comm. nov. Acad. Petrop.*, T. XVIII, pag. 85). Gauss reconhecendo que essa demonstração não era absolutamente rigorosa, publicou (obra citada, §§ 53, 54, 55) duas demonstrações inteiramente isentas de toda a objecção.

A demonstração de Legendre (obra citada, T. II, pag. 16) é analoga á ultima das demonstrações de Euler, de que fallamos (§ 9), e tem o mesmo defeito, que Poinsot reconheceu naquell'outra. Poinsot (memoria citada) deu ainda duas outras demonstrações, a primeira fundada em uma inducção pouco evidente, e outra summamente simples, em que demonstrando previamente a existencia de uma raiz primitiva, conclue d'ahi a existencia de $\varphi p'$ raizes dessa classe, simplificando a demonstração que da ultima proposição deu Gauss *(Disq. Arith.* § 53, 1.º). Serret *(Cours d'Algèbre Supérieure*, pag. 316) demonstrou tambem o mesmo theorema, aproveitando o processo primeiro indicado por Gauss, que faz depender as raizes da congruencia do gráu $p' = q^{\alpha} r^{\beta} s^{\gamma} \ldots$ (sendo $q, r, s, \ldots$ primos entre si) de outras correspondentes aos gráus q^{α}, r^{β}, s^{γ}, etc., processo em que tambem se funda a segunda demonstração de Poinsot.

Apezar da existencia desses numerosos e importantes trabalhos, acreditamos que poderão soffrer a comparação com elles as duas demonstrações, que passamos a expor.

A primeira dellas fornecer-nos-ha uma nova applicação da formula (10).

Qualquer raiz não primitiva de

$$(44) \qquad x^{p'} \equiv 1,$$

em que $p' = q^{\alpha} r^{\beta} s^{\gamma} \ldots$ será raiz de

$$x^{q^{\alpha-\alpha'} r^{\beta-\beta'} s^{\gamma-\gamma'} \ldots} \equiv 1,$$

em que α', β', γ', etc. não serão todos simultaneamente zero. Suppondo pois que vg. α' não é zero, e elevando essa congruencia á potencia $q^{\alpha'-1} r^{\beta'} s^{\gamma'} \ldots$, acharemos

$$x^{q^{\alpha-1} r^{\beta} s^{\gamma} \ldots} \equiv 1,$$

á qual satisfará ainda a raiz supposta não primitiva.

Logo o numero das raizes primitivas de (44) será obtido, tirando do numero p' das suas raizes o numero das que pertencem á congruencia do gráu $\frac{p'}{q}$; tirando das restantes o numero das que pertencem á congruencia do gráu $\frac{p'}{r}$; depois o numero das pertencentes á congruencia do gráu $\frac{p'}{s}$, etc.

Em consequencia disto reconhece-se immediatamente, que o numero das raizes primitivas será dado pela formula (10)

$$(45) \qquad \psi^{\ldots s, r, q} S = \psi S [1 -_q] [1 -_r] [1 -_s] \ldots,$$

na qual vg. o symbolo ψS_q é o numero de raizes de

$$x^{q^{\alpha-1} r^{\beta} s^{\gamma} \ldots} \equiv 1;$$

$\psi S_{q,r}$ sendo o numero das raizes communs a esta congruencia e a

$$x^{q^{\alpha} r^{\beta-1} s^{\gamma} \ldots} \equiv 1,$$

será o numero de raizes da congruencia do gráu $q^{\alpha-1} r^{\beta-1} s^{\gamma} \ldots$, e assim por diante. Teremos pois

$$\psi S = p'; \ \psi S_q = \frac{p'}{q}; \ \psi S_r = \frac{p'}{r}; \text{ etc. } \psi S_{q,r} = \frac{p'}{qr}, \text{ etc. } \psi S_{q,r,s} = \frac{p'}{qrs}, \text{ etc.}$$

logo (45) muda-se em

$$\psi^{\ldots s, r, q} S = p'\left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{r}\right)\left(1 - \frac{1}{s}\right) \ldots,$$

isto é, será $\varphi p'$ o numero das raizes primitivas de (44).

Esta demonstração teria logar ainda, se fosse $p' = q$ numero primo. Então todas as raizes seriam primitivas, á excepção de 1 raiz unica de

$$x \equiv 1,$$

cujo gráu seria o unico divisor de p' menor que este numero.

34. A segunda demonstração terá a vantagem de nos conduzir ao elegante processo de Gauss acima mencionado; processo que deduziremos das seguintes proposições:

Se fôr $p' = AB$, sendo A, B primos entre si, e se representarmos respectivamente por y, y' duas raizes de

$$x^A \equiv 1, \quad x^B \equiv 1, \tag{46}$$

será sempre:

1.º yy' uma raiz de (44); pois que de

$$y^A \equiv 1, \quad y'^B \equiv 1,$$

conclue-se

$$y^{AB} \equiv 1, \quad y'^{AB} \equiv 1, \quad (yy')^{AB} \equiv 1.$$

2.º Todos os productos yy' serão raizes distinctas, tomando para y, y' todas as raizes das duas congruencias (46). Com effeito, suppondo

$$yy' \equiv y_{\prime}\, y_{\prime}',$$

concluiriamos

$$y^B y'^B \equiv y_{\prime}^B, \; y_{\prime}'^B;$$

e como

$$y'^B \equiv 1 \equiv y_{\prime}'^B,$$

seria

$$y^B \equiv y_{\prime}^B, \text{ ou } y^B - y_{\prime}^B \equiv 0;$$

mas é

$$y^A - y_{\prime}^A \equiv 0,$$

e esta congruencia não póde subsistir com a precedente (§ 29), visto que A, B são entre si primos, e y, $y_{\prime}$ incongruos para o modulo p. Logo os $A \times B = p'$ productos yy' dão exactamente todas as p' raizes de (44).

3.º As raizes primitivas de (44) serão dadas por todos os productos yy', cujos factores forem ambos raizes primitivas das congruencias correspondentes. Nesta hypothese, se fosse possivel que yy' não fosse raiz primitiva de

$$x^{AB} \equiv 1,$$

seria necessariamente raiz d'outra congruencia

$$x^m \equiv 1,$$

em que $m < AB$; sendo pois D o maximo divisor commum entre AB, e m, a dita raiz satisfaria a

$$x^D \equiv 1,$$

em que $D = \frac{A}{d} \cdot \frac{B}{d'}$, sendo d, d' divisores de A, e de B, os quaes não poderiam ser simultaneamente iguaes á unidade. Suppondo portanto $d > 1$, yy' satisfaria á congruencia

$$x^{\frac{A}{d}B} \equiv 1,$$

e como

$$y'^{B\frac{A}{d}} \equiv 1,$$

concluir-se-hia

$$(46') \qquad y^{\frac{A}{d}} \equiv 1,$$

contra a hypothese. Reciprocamente, se uma das raizes y, y', vg. a primeira, não fosse raiz primitiva da congruencia correspondente, isto é, se se verificasse a congruencia (46'), seguir-se-hia

$$y^{\frac{A}{d}B} \equiv 1,$$

e como

$$y'^{B \cdot \frac{A}{d}} \equiv 1,$$

achariamos finalmente

$$(yy')^{\frac{A}{d}B} \equiv 1,$$

isto é, yy' não seria raiz primitiva de (44).

Segue-se do que acabamos de expor, que designando pela caracteristica ψ o numero de raizes primitivas, que correspondem a uma congruencia de qualquer gráu divisor de $p-1$, teremos

$$\psi p' = \psi AB = \psi A \times \psi B.$$

De maneira que se forem q, r, s, etc. os factores primos de p', isto é, $p' = q^\alpha r^\beta s \ldots$, será

$$\psi p' = \psi q^\alpha \times \psi (r^\beta s^\gamma \ldots) = \psi q^\alpha \times \psi r^\beta \times \psi (s^\gamma \ldots) = \psi q^\alpha \times \psi r^\beta \times \psi s^\gamma \ldots$$

Ora na congruencia do gráu vg. q^α visivelmente são raizes não primitivas as $q^{\alpha-1}$ raizes da congruencia do gráu $q^{\alpha-1}$; logo

$$\psi q^\alpha = q^\alpha - q^{\alpha-1} = \varphi q^\alpha;\ \ \psi r^\beta = \varphi r^\beta;\ \ \text{etc.}$$

e por conseguinte

$$\psi p' = \varphi q^\alpha \times \varphi r^\beta \times \varphi s^\gamma \ldots = \varphi p'.$$

35. Por um modo inteiramente analogo ao que ultimamente se empregou para achar o numero das raizes primitivas da congruencia do gráu $p' = q^\alpha r^\beta s^\gamma \ldots$, se concluirá, que se representarmos por y, y', y'', etc. um systema de raizes que respectivamente pertençam ás congruencias

$$x^{q^\alpha} \equiv 1;\ \ x^{r^\beta} \equiv 1;\ \ x^{s^\gamma} \equiv 1;\ \ \ldots \tag{47}$$

1.º O producto $yy'y'' \ldots$ será raiz de (44).

2.º Os p' productos $yy'y'' \ldots$ formados por todas as combinações das raizes das congruencias (47) são todos distinctos, isto é, incongruos para o modulo p, e por consequencia representam todos as raizes de (44).

3.º As raizes primitivas de (44) serão dadas por todos os productos $yy'y''$ etc., cujos factores forem todos raizes primitivas das congruencias correspondentes: e por tanto as raizes não primitivas de (44) serão dadas por aquelles productos em que um, ou mais factores forem raizes não primitivas das congruencias correspondentes.

36. O methodo mais simples para determinar as raizes de

$$x^{p'} \equiv 1, \tag{47'}$$

em que se suppõe $p' < p - 1$, e divisor deste ultimo numero, consiste em procurar nas taboas, que dão as raizes primitivas dos numeros primos, uma raiz ρ qualquer de p, e então suppondo $p - 1 = p'p_{,}$, serão raizes da congruencia precedente

$$(48) \qquad [\rho^{p_{,}}],\ [\rho^{2p_{,}}],\ [\rho^{3p_{,}}],\ \ldots\ [\rho^{p'p_{,}}] = 1,$$

que serão todas distinctas, isto é, incongruas para o modulo p (§ 15).

Entre estas raizes serão primitivas da congruencia dada aquellas, em cujo expoente $np_{,}$ fôr n primo com p'; por quanto se nessa hypothese podesse a raiz correspondente ser primitiva da congruencia

$$x^{p''} \equiv 1,$$

em que p'' é divisor de p', teriamos

$$\rho^{np_{,}p''} \equiv 1,$$

donde, por ser ρ raiz primitiva de p, seria (§ 13)

$$np_{,}p'' = z(p-1), \quad \text{ou} \quad np'' = zp';$$

e como n é primo com p', este dividiria p'', o que é impossivel.

Tambem se vê claramente que se n tiver com p' o divisor commum $d > 1$, será $\rho^{np_{,}}$ raiz de

$$x^{\frac{p'}{d}} \equiv 1,$$

isto é, $\rho^{np_{,}}$ não será raiz primitiva da congruencia do gráu p'.

O numero das raizes primitivas dadas pela formula $\rho^{np_{,}}$, em que n é primo com p', é pois $\varphi p'$, como precedentemente tinhamos demonstrado.

Se p' é um numero primo, todas as raizes (48), á excepção da ultima, são raizes primitivas da congruencia (47'), e por conseguinte nesse caso qualquer numero ρ, cuja potencia $p_{,}$ fôr incongrua com 1, dará pelas suas potencias successivas todas as raizes.

Se $p' = p - 1$, as raizes da congruencia (47') são

$$\rho,\ [\rho^2],\ [\rho^3],\ [\rho^4],\ \ldots\ [\rho^{p-1}] = 1,$$

e serão primitivas todas aquellas, cujo expoente fôr primo com $p - 1$.

37. Quando p' fôr primo, em vez de representar as $p'-1$ raizes primitivas de $(47')$ pela progressão

$$(49) \qquad r,\ r^2,\ r^3,\ \ldots\ r^{p'-1},$$

em que r é uma raiz primitiva qualquer dessa congruencia, podemos exprimi-las por uma serie, em que cada termo seja a mesma potencia do termo precedente, isto é, como todos os numeros

$$1,\ 2,\ 3,\ \ldots\ p'-1,$$

são dados pelos residuos relativos ao modulo p' da serie

$$a,\ a^2,\ a^3,\ \ldots\ a^{p'-1},$$

em que a é qualquer raiz primitiva de

$$x^{p'-1} \equiv 1 \text{ M } p',$$

a serie (49) equivalerá a

$$r^{a},\ r^{a^2},\ r^{a^3},\ \ldots\ r^{a^{p'-1}}.$$

38. Se tivermos a resolver a congruencia

$$(50) \qquad x^{p'} \equiv 1,$$

sendo $p' = ABC\ \ldots$, e A, B, C, etc. numeros quaesquer, mas primos entre si, e se conhecermos os numeros r, $r_{,}$, $r_{,,}$, etc., que sejam respectivamente raizes primitivas de

$$x^A \equiv 1;\ x^B \equiv 1;\ x^C \equiv 1;\ \text{etc.};$$

as p' raizes de (50) serão dadas (§§ 34, 35) pelos p' termos de

$$(1+r+r^2+\cdots r^{A-1})(1+r_{,}+r_{,}^2+\cdots r_{,}^{B-1})(1+r_{,,}+r_{,,}^2+\cdots r_{,,}^{C-1})\cdots$$

isto é, sendo ρ raiz primitiva de (50), todos os termos da serie

$$\rho,\ \rho^2,\ \rho^3,\ \ldots\ \rho^{p'}$$

serão dados por todos os divisores do producto $r^A\, r_{,}^B\, r_{,,}^C \ldots$

IV.

DETERMINAÇÃO DIRECTA DAS RAIZES PRIMITIVAS DOS NUMEROS PRIMOS.

39. A resolução indicada (§ 36) suppõe, que se possue uma taboa das raizes primitivas dos numeros primos. Ensinaremos agora o modo de construir essa taboa, isto é, de determinar todas as raizes primitivas de um numero primo qualquer p.

Sendo A, B, C, etc. os factores primos de $p-1$, isto é, suppondo

$$p-1=A^{\alpha}B^{\beta}C^{\gamma}\ldots,$$

poderiamos resolver a questão, excluindo successivamente da serie

$$2,\ 3,\ 4,\ 5,\ \ldots\ p-1$$

todos os numeros, que satisfazem a alguma das congruencias

(51) $$x^{\frac{p-1}{A}}\equiv 1\ \mathrm{M}\,p;\quad x^{\frac{p-1}{B}}\equiv 1;\quad x^{\frac{p-1}{C}}\equiv 1;\ \text{etc.}$$

Logo que achassemos um numero, que não satisfizesse a nenhuma dessas congruencias, seria esse uma raiz primitiva, que, elevada successivamente ás $\varphi(p-1)-1$ potencias competentes, daria todas as outras raizes primitivas.

Este processo seria o mais simples, se encontrassemos uma raiz primitiva, depois de um pequeno numero de exclusões: por quanto as verificações que tem a fazer-se nas congruencias precedentes, effeituam-se com bastante rapidez (§ 20), e os residuos de potencias achados na verificação de uma das congruencias, servem para facilitar o calculo relativo ás outras.

Mas como effectivamente poderia acontecer que verificassemos $p-2-\varphi(p-1)$ dos numeros

$$2,\ 3,\ 4\ \ldots\ p-1,$$

exporemos outro processo, que evitará sempre essa longa serie de tentativas.

Como $p-1$ é sempre um numero par, se forem B, C, D, etc., os seus divisores primos differentes de 2, podemos suppôr

$$p-1=2^{\alpha}B^{\beta}C^{\gamma}D^{\delta}\ldots;$$

as raizes primitivas serão as que não satisfazem a alguma das congruencias

$$(52)\qquad x^{\frac{p-1}{2}}\equiv 1\ \mathrm{M}\,p;\quad x^{\frac{p-1}{B}}\equiv 1;\quad x^{\frac{p-1}{C}}\equiv 1;\quad x^{\frac{p-1}{D}}\equiv 1;\ \text{etc.}$$

Se representarmos por r qualquer raiz primitiva de p, todos os numeros que satisfazem á primeira congruencia serão congruos com uma potencia r^{2n}, isto é, serão *residuos quadraticos;* os numeros que satisfazem á segunda, serão congruos com r^{qB}, isto é, serão *residuos potencias B*, e similhantemente para as congruencias seguintes.

Teremos pois todas as raizes primitivas da seguinte maneira:

1.º Excluindo da serie

$$1,\ 2,\ 3,\ \ldots\ p-1$$

todos os residuos quadraticos, cujo numero é $\frac{p-1}{2}$, que designa o numero de raizes da primeira das congruencias (52).

2.º Dos $\frac{p-1}{2}$ numeros restantes devem excluir-se os que são residuos potencias B; e como estes tem a fórma r^{qB}, em que $q < \frac{p-1}{B}$ é impar, o numero das exclusões será $\frac{p-1}{2B}$, e por conseguinte restarão $(p-1)\left(1-\frac{1}{2}\right)\left(1-\frac{1}{B}\right)$ numeros.

3.º Destes excluir-se-hão os que são residuos potencias C; e como esses tem a fórma r^{sC}, em que $s < \frac{p-1}{C}$, não é divisivel por 2, nem por B; por conseguinte (10) será $\frac{p-1}{C}\left(1-\frac{1}{2}\right)\left(1-\frac{1}{B}\right)$ o numero de valores de s, e o destas ultimas exclusões. Restarão pois $(p-1)\left(1-\frac{1}{2}\right)\left(1-\frac{1}{B}\right)\left(1-\frac{1}{C}\right)$ numeros.

4.º Proseguiremos na exclusão dos residuos de potencias relativas a todos os outros factores primos de $p-1$, e finda essa exclusão, ter-nos-ha restado o numero

$$(p-1)\left(1-\frac{1}{2}\right)\left(1-\frac{1}{B}\right)\left(1-\frac{1}{C}\right)\left(1-\frac{1}{D}\right)\ldots = \varphi(p-1)$$

de numeros não excluidos, que serão as raizes primitivas que procuravamos. Este processo, como se vê, dá-nos tambem outra demonstração do numero das raizes primitivas.

40. Resta-nos indicar o modo mais simples de effeituar estas exclusões successivas.

Para ter os residuos quadraticos, que se devem excluir, basta quadrar os $\frac{p-1}{2}$ numeros

$$1,\ 2,\ 3,\ \ldots\ \frac{p-1}{2};$$

por quanto todos elles dão residuos diversos. Com effeito, representando f, $f+g$ dois desses numeros, será

$$(f+g)^2 - f^2 = g(2f+g),$$

producto que não póde ser divisivel por p, pois

$$g < \frac{p-1}{2} \cdot f + f + g < p:$$

logo $(f+g)^2$, f^2 serão incongruos. A cada termo f da serie precedente corresponderá porém, no seu prolongamento, outro termo $p-f$, que visivelmente dará o mesmo residuo quadratico que f.

Feita pois a exclusão dos residuos quadraticos, supponhamos que ficaram os $\frac{p-1}{2}$ numeros

$$(53) \qquad a, \ b, \ c, \ d, \ \ldots$$

Para destes excluir os residuos potencias B, tome-se entre elles um numero m, que não satisfaça á congruencia

$$(54) \qquad x^{2B} \equiv 1 \ \mathrm{M}p:$$

essa determinação não será difficil, por quanto no caso mais desfavoravel, isto é, supporido que se escolhiam successivamente na serie (53) todos os numeros que são raizes de (54), esses numeros tendo a fórma ρ^i, em que ρ representa uma raiz primitiva dessa congruencia, será B o maior numero de valores que terá i, e por conseguinte o maximo numero de ensaios infructuosos; e em cada um delles só temos a determinar os residuos de potencias B, pois já possuimos todos os residuos quadraticos dos numeros (53). E mesmo só teremos a calcular potencias $B-2$, visto que sendo m um numero da serie

$$2, \ 3, \ \ldots \ p-1,$$

já conhecemos o seu residuo quadratico.

Podiamos tambem escolher m entre os numeros da serie precedente, sem que por isso o calculo fosse mais longo, pois que sendo

$$x^{2B} - 1 = (x^B - 1)(x^B + 1) \equiv 0,$$

e procurando o numero m, cujo residuo potencia B não é 1, nem -1, nunca teriamos a effeituar mais de B tentativas.

Não sendo pois

$$m^{2B} \equiv 1,$$

seja n o minimo numero, que faz

$$m^{2Bn} \equiv 1;$$

tome-se na serie (53) um numero qualquer $a \equiv r^i$, representando ainda r uma raiz primitiva de p; forme-se a serie de residuos

$$(55) \qquad a^B,\ a^B m^{2B},\ a^B m^{4B},\ a^B m^{6B}, \ldots\ a^B m^{2B(n-1)};$$

estes residuos tendo todos a forma r^{iB+2h}, são contidos em (53), ainda que seja $iB+2h > p-1$; e sendo todos potencias B, devem ser excluidos da mesma serie; demais são todos distinctos, pois se fosse

$$a^B m^{2qB} \equiv a^B m^{2sB},$$

sendo $s > q$, concluiriamos

$$m^{2(s-q)B} \equiv 1,$$

o que é impossivel, pois $s - q < n$.

Se fôr n menor que $(p-1)\left(1-\frac{1}{2}\right)\frac{1}{B}$, numero dos residuos potencias B contidos em (53), dos numeros que restam nessa serie, depois de feita a exclusão precedente, tome-se vg. b^B, e forme-se a serie

$$b^B,\ b^B m^{2B},\ b^B m^{4B},\ \ldots\ b^B m^{2B(n-1)},$$

cujos termos são todos incongruos com os de (55); por quanto se fosse

$$b^B m^{2Bq} \equiv a^B m^{2Bs} \equiv a^B m^{2B(s+n)},$$

concluir-se-hia

$$b^B \equiv a^B m^{2B(s+n-q)},$$

e portanto b^B seria um dos residuos já excluidos, contra a hypothese.

O numero adoptado b fará pois excluir outros n termos de (53).

Se $2n < (p-1)\left(1-\frac{1}{2}\right)\frac{1}{B}$, outro numero dos restantes em (53) produzirá n novas exclusões nessa serie. Continuaremos pois similhantemente até serem excluidos de (53) todos os $(p-1)\left(1-\frac{1}{2}\right)\frac{1}{B}$ residuos potencias B. Este processo demonstra-nos pois que o dito numero de residuos é sempre multiplo de n, o que aliás se poderia provar *à priori*.

Teremos pois, em consequencia dessa operação, os $(p-1)\left(1-\frac{1}{2}\right)\left(1-\frac{1}{B}\right)$ numeros

$$(56) \qquad a',\ b',\ c',\ d',\ \ldots,$$

dos quaes devemos excluir os residuos potencias C.

Se m satisfizer á congruencia

$$x^{2BC} \equiv 1,$$

procuraremos em (56) outro numero m', que não tenha essa propriedade.

O numero de ensaios infructuosos nunca excederia $(B-1)\,C$, pois sendo ρ qualquer raiz primitiva da congruencia precedente, em (56) contem-se, quando muito, as raizes ρ^s, em que $s < 2BC$ é primo com 2, e com B.

Achado esse numero m', e sendo n' o menor numero, que faz

$$m'^{2BCn'} \equiv 1,$$

os n' residuos potencias C

$$a'^C,\ a'^C m'^{2BC},\ a'^C m'^{4BC},\ \ldots\ a'^C m'^{2BC(n'-1)},$$

tendo todos a fórma $r^{iC+q\cdot 2BC}$, em que i é primo com 2, e com B, serão contidos na serie (56), ainda que seja $iC+q\cdot 2BC > p-1$: demais são todos incongruos; logo darão nessa serie n' exclusões de potencias C. E se n', que deve ser divisor de

$$(p-1)\left(1-\frac{1}{2}\right)\left(1-\frac{1}{B}\right)\frac{1}{C}$$

numero total dos residuos, que temos a excluir, não fôr igual a esse numero, com outro numero b' restante em (56) formaremos n' novas exclusões, e assim por diante até exhaurir todos os residuos potencias C.

Excluiremos depois similhantemente os residuos potencias D, determinando um numero m'', que não satisfaça a

$$x^{2BCD} \equiv 1,$$

não podendo nunca o numero de ensaios infructuosos exceder a $(B-1)$ $(C-1)$ D.

Por um analogo processo excluiriamos os residuos relativos a potencias designadas pelos outros factores primos de $(p-1)$, com a excepção que abaixo indicaremos (§ 42).

41. O numero de ensaios infructuosos para a determinação dos numeros m, m', m'', etc. ficará muito abaixo dos *maxima*, que acima indicamos, excluindo da verificação não só os numeros productos de factores primos já verificados, mas tambem os numeros, aos quaes juntando um multiplo do modulo, resulta um producto de numeros já verificados. Com effeito, se g satisfaz á congruencia

$$x^{2BC\ldots} \equiv 1,$$

tambem satisfará a ella qualquer potencia desse numero; e satisfazendo igualmente h, o mesmo acontecerá ao producto de quaesquer potencias de g, e h, etc. Omittimos ainda outras simplificações, que occorrerão facilmente a quem possue alguma aptidão para esta especie de calculos.

42. O methodo exposto (§ 40) não seria applicavel á exclusão dos residuos potencias relativas ao ultimo factor de $p-1$, se fosse $\alpha=\beta=\gamma=\delta=\cdots=1$, isto é, se

$$p-1=2BCD\ldots IK;$$

por quanto, depois de excluidas as potencias 2, B, C, ... I, os numeros restantes, bem como todos os excluidos, satisfazem á congruencia

$$x^{2BCD\ldots K} \equiv 1.$$

Nesse caso, bem como em todos os outros, em que não seja facil determinar o numero m, por meio do qual devemos excluir os residuos potencias K, empregaremos o seguinte processo, que é muito mais directo, e em que nunca terão a effeituar-se inuteis tentativas, quando o expoente de K em $p-1$ fôr $\varkappa=1$.

Supponhamos primeiro que é $\varkappa=1$.

Seja

(57) $$a,\ b,\ c,\ d,\ \ldots$$

a serie obtida depois de excluidos todos os residuos potencias de qualquer dos factores de $p-1$, diversos do ultimo K. Tome-se vg. o termo a da serie (57), será

$$a \equiv r^{n K^m},$$

em que n é primo com 2, B, C, ... I, K, e $m = > 0$. Determinem-se, por meio da formula de Poinsot (38'), se tanto fôr necessario, e disponham-se em ordem ascendente, todos os $\varphi \frac{p-1}{K}$ numeros menores que $\frac{p-1}{K}$, e primos com este; eleve-se successivamente a^K a todas as potencias designadas por esses numeros; os $\varphi \frac{p-1}{K}$ residuos obtidos serão exactamente todos os $\varphi \frac{p-1}{K}$ residuos potencias K, contidos em (57). Com effeito:

1.° Qualquer das potencias obtidas por aquelle processo vg. $r^{nqK^{m+1}}$ é residuo potencia K contido em (57), pois que o residuo do expoente nqK^{m+1}, para o modulo $p-1$, não é divisivel senão pelo divisor K de $p-1$.

2.° Não póde haver duas potencias congruas; pois que de

$$r^{nqK^{m+1}} \equiv r^{nq'K^{m+1}},$$

concluir-se-hia

$$nqK^{m+1} \equiv nq'K^{m+1} \,\mathrm{M}\,(p-1),$$

e desta

$$q \equiv q' \,\mathrm{M}\, \frac{p-1}{K},$$

o que é impossivel, visto que q, q' são desiguaes, e menores que $\frac{p-1}{K}$.

Supponhamos agora, que o expoente $\varkappa$ de K é maior que 1. Forme-se a serie ascendente

(58) $$1,\ n,\ n',\ n'',\ \text{etc.}$$

dos numeros primos com 2, B, C, ... K. Tome-se um termo qualquer de (57) vg.

$$a \equiv r^{n, K^m},$$

pertencendo $n_{,}$ á serie (58). Será $r^{n_{,}}$ uma raiz primitiva, e por isso podemos suppor sempre

$$a \equiv r^{K^m}.$$

Eleve-se a á potencia K, acharemos necessariamente um dos tres resultados

$$(59) \qquad a^K \equiv r^{K^{\varkappa - q}}; \quad a^K \equiv r^{K^{\varkappa}}; \quad a^K \equiv r^{K^{\varkappa + \iota}}.$$

Elevando agora a^K successivamente ás potencias (58), os residuos obtidos, até que venha de novo a achar-se um congruo com a^K, serão todos potencias da fórma $r^{n_{,,} K^{q'}}$, e por tanto exclusiveis de (57); e demais serão todos distinctos; pois se

$$r^{n_{,,} K^{q'}} \equiv r^{n_{,,,} K^{q'}},$$

teriamos

$$n_{,,} K^{q'} \equiv n_{,,,} K^{q'} \mathrm{M}(p-1),$$

donde

$$(60) \qquad n_{,,} \equiv n_{,,,} \mathrm{M}\, 2^{\alpha} B^{\beta} C^{\gamma} \ldots K^{\varkappa - q'},$$

ou (não indicando ι exclusivamente um numero impar)

$$(61) \qquad n_{,,} \equiv n_{,,,} \mathrm{M}\, 2^{\alpha} B^{\beta} C^{\gamma} \ldots I^{\iota},$$

conforme fôr $q' < \varkappa$, ou $q' = > \varkappa$. Ora verificando-se a primeira dessas congruencias, e suppondo $n_{,,} > n_{,,,}$, o menor valor possivel de $n_{,,}$ seria

$$n_{,,} = 1 + 2^{\alpha} B^{\beta} C^{\gamma} \ldots K^{\varkappa - q'},$$

e este daria

$$a^{n_{,} K} \equiv a^K \cdot a^{K \cdot 2^{\alpha} B^{\beta} C^{\gamma} \ldots K^{\varkappa - q'}} \equiv a^K;$$

logo a potencia $a^{n_{,,} K}$ não teria sido aproveitada, nem nenhuma das seguintes para as quaes se verificasse (60).

Do mesmo modo se prova que, se tivesse logar (61), achariamos um valor minimo

$$n_{\prime\prime} = 1 + 2^{\alpha} B^{\beta} C^{\gamma} \ldots I^{\iota},$$

que faria

$$a^{n_{\prime\prime} K} \equiv a^{K},$$

e por tanto não teria sido aproveitada esta potencia, bem como as seguintes que satisfazem a (61).

O numero μ dos residuos aproveitados indicará se a^{K} pertence á primeira, ou ás duas ultimas classes (59); e no primeiro caso μ dará o valor de $\varkappa - q$. Com effeito nesse caso, sendo $2^{\alpha} B^{\beta} C^{\gamma} \ldots K^{q} + 1$ o menor valor de $n_{\prime}$, que faz

$$a^{n_{\prime} K} \equiv a^{K},$$

teremos

$$\mu = \varphi 2^{\alpha} B^{\beta} C^{\gamma} \ldots K^{q},$$

isto é,

$$(62) \qquad \mu = K^{q-1} (K - 1) \varphi 2^{\alpha} B^{\beta} C^{\gamma} \ldots I^{\iota}.$$

Se pelo contrario fosse

$$a^{K} \equiv r^{K^{\varkappa}}, \quad \text{ou} \quad a^{K} \equiv r^{K^{\varkappa + s}},$$

o primeiro numero $n_{\prime}$ tal que

$$a^{n_{\prime} K} \equiv a^{K},$$

seria $n_{\prime} = 2^{\alpha} B^{\beta} C^{\gamma} \ldots I^{\iota} + 1$; logo designando por φ_{K} o numero de numeros menores que $2^{\alpha} B^{\beta} C^{\gamma} \ldots I^{\iota}$, e primos com este, e com K, teriamos o numero de potencias K aproveitadas

$$\mu_{\prime} = \varphi_{K} 2^{\alpha} B^{\beta} C^{\gamma} \ldots I^{\iota}.$$

Ora a formula (62) dá o minimo valor de

$$\mu = (K - 1) \varphi 2^{\alpha} B^{\beta} C^{\gamma} \ldots I^{\iota};$$

e como é sempre

$$\varphi 2^{\alpha} B^{\beta} C^{\gamma} \ldots I^{\iota} = > \varphi_K 2^{\alpha} B^{\beta} C^{\gamma} \ldots I^{\iota}, \text{ e } K > 2,$$

será em todos os casos

$$\mu_{,} < \mu.$$

Por conseguinte quando acharmos

$$\mu = > (K-1)\varphi \frac{p-1}{K^{x}},$$

terá a^K a primeira das fórmas (59), e pela formula (62) se determinará q.

Esse calculo poderia effeituar-se pelos logarithmos, que dão

$$q = \frac{L\mu - L((K-1)\varphi 2^{\alpha} B^{\beta} C^{\gamma} \ldots I^{\iota})}{LK} + 1;$$

todavia, mesmo quando forem mui grandes os numeros, que entram em (62), será quasi sempre mais rapido executal-o directamente.

Quando porém acharmos

$$\mu' < (K-1)\varphi \frac{p-1}{K^{x}},$$

pertencerá a^K á segunda, ou á terceira das fórmas (59).

Supponhamos pois em primeiro logar, que é

$$a^K = r^{K^{x}};$$

elevando successivamente a^K a todas as potencias designadas pelos termos da serie ascendente

$$1,\ m,\ m',\ m'',\ \ldots\ m_{,},$$

que são todos primos com 2, B, C, ... I, sendo o ultimo $m_{,}$ immediatamente inferior a

$$2^{\alpha} B^{\beta} C^{\gamma} \ldots I^{\iota},$$

acharemos outros tantos residuos distinctos

$$(63) \qquad r^{K^{\varkappa}},\ r^{mK^{\varkappa}},\ r^{m'K^{\varkappa}},\ \ldots\ r^{m_{,}K^{\varkappa}},$$

que são todas as potencias $K^{\varkappa}$, e todas as potencias $K^{\varkappa+s}$ contidas em (57), e exclusiveis dessa serie. A maior parte dessas potencias já foi calculada para a determinação de μ'.

Se fosse porém

$$a^{K} \equiv r^{K^{\varkappa+s}},$$

seguindo exactamente o processo antecedente achariamos em vez de (63) a serie

$$r^{K^{\varkappa+s}},\ r^{mK^{\varkappa+s}},\ r^{m'K^{\varkappa+s}},\ \ldots\ r^{m_{,}K^{\varkappa+s}},$$

que contém todos os residuos (63), pois que qualquer termo da ultima serie, vg. $r^{m_{,,}K^{\varkappa+s}}$, equivalerá ao termo $r^{m_{,,,}K^{\varkappa}}$ de (63), em que $m_{,,,}$ satisfizer á congruencia

$$m_{,,,}K^{\varkappa} \equiv m_{,,}K^{\varkappa+s}\,\mathrm{M}\,2^{\alpha}B^{\beta}C^{\gamma}\ldots K^{\varkappa},$$

que dá

$$m_{,,,} \equiv m_{,,}K^{s}\,\mathrm{M}\,2^{\alpha}B^{\beta}C^{\gamma}\ldots I'.$$

Logo por um unico processo excluimos sempre de (57) todas as potencias $r^{n_{,}K^{\varkappa}}$, e $r^{n_{,}K^{\varkappa+s}}$ quando acharmos

$$\nu_{,} < (K-1)\varphi\frac{p-1}{K^{\varkappa}}.$$

Feita pois essa exclusão, as potencias K restantes em (57) serão da fórma $r^{n_{,}K^{\varkappa-q}}$, e portanto da fórma $r^{K^{\varkappa-q}}$. Tome-se um dos termos restantes, vg. b, será

$$b^{K} \equiv r^{K^{\varkappa-s}},$$

ou quando muito

$$b^{K} \equiv r^{K^{\varkappa}};$$

no segundo caso, isto é, sendo b^K um numero já excluido, tomaremos outro numero c tal que não seja c^K dos numeros já excluidos. Se quizermos evitar tentativas inuteis, como nos basta conhecer c^K, e é inutil saber a grandeza de c, quando b fôr potencia $K^{\varkappa-1}$, podemos tomar

$$c^K \equiv b \equiv r^{K^{\varkappa-1}};$$

isto é, supporemos em geral, que se acha sempre immediatamente

$$c^K \equiv r^{K^{\varkappa-q}};$$

excluiremos por tanto de (57) todas as potencias $r^{n_, K^{\varkappa-q}}$, elevando c^K successivamente ás potencias (58)

$$1,\ n,\ n',\ n'',\ \text{etc.}$$

até exclusivamente acharmos c^K, o que aconteceria quando fosse

$$n_{\prime\prime} = 1 + 2^\alpha B^\beta C^\gamma \ldots I^\iota K^q.$$

Elevando c^K á potencia K, e depois successivamente o resultado ás potencias 1, n, n', etc. até exclusivamente

$$n_{\prime\prime} = 1 + 2^\alpha B^\beta C^\gamma \ldots I^\iota K^{q-1},$$

excluiremos de (57) todas as potencias $r^{n_, K^{\varkappa-q+1}}$.

Elevando ainda c^{K^2} á potencia K, excluiremos similhantemente de (57) todas as potencias $r^{n_, K^{\varkappa-q+2}}$; e assim successivamente até achar uma das potencias já excluidas

$$r^{n_, K^\varkappa} \equiv c^{K^{q+1}}.$$

Se porém a exclusão das potencias K em (57) não tivesse começado tomando $a^K \equiv r^{n_, K^\varkappa}$, ou $\equiv r^{n_, K^{\varkappa+s}}$, mas sim tomando c^K, quando obtivessemos $r^{n_, K^\varkappa}$, esse termo não estaria ainda excluido: o valor de q já conhecido nos daria o momento em que o dito termo deve apparecer, e por meio delle excluiriamos, como acima dissemos, todas as potencias $r^{n K^{\varkappa}}$, e $r^{n_{,} K^{\varkappa+s}}$.

Feitas as exclusões precedentes, tome-se outro termo d dos restantes em (57), que não dê d^K residuo já excluido, o que, como acima dissemos, se effeituará sem tentativa alguma infructuosa; será

$$d^K \equiv r^{K^{\varkappa-q'}},$$

e $q' > q$; e imitando o processo precedente excluiremos as potencias

$$r^{n_{,} K^{\varkappa-q'}}, \quad r^{n_{,,} K^{\varkappa-q'+1}}, \quad r^{n_{,,,} K^{\varkappa-q'+2}}, \text{ etc.}$$

Excluiremos depois os residuos potencias K desde os da fórma $r^{n_{,} K^{\varkappa-q''}}$ (em que $q'' > q'$) até á fórma $r^{n_{,} K^{\varkappa-q'}}$ exclusivamente; e assim por diante até excluirmos as potencias $r^{n_{,} K}$.

43. O methodo que precedentemente exposemos será tanto mais directo, quanto maior fôr q em

$$a^K \equiv r^{K^{\varkappa-q}}.$$

Esse methodo poderia tambem applicar-se, com algumas modificações, ás exclusões relativas ás potencias correspondentes aos factores de $p-1$ anteriores ao ultimo K; mas tornar-se-hia bastante longo, não sendo

$$\alpha = \beta = \gamma = \cdots = \varkappa = 1.$$

Para determinar as raizes primitivas de qualquer numero p, o mais simples e directo será:

1.º Se $\alpha > 1$; excluidos os residuos quadraticos, qualquer dos numeros restantes não satisfará a nenhuma das congruencias

$$x^{2B} \equiv 1 \,\mathrm{M}\, p; \quad x^{2BC} \equiv 1; \quad x^{2BCD} \equiv 1; \text{ etc.},$$

e por tanto todos elles poderão representar qualquer dos numeros m, m', m'', etc. que é necessario determinar no processo (§ 40). Por conseguinte neste caso não ha tentativa alguma inutil a fazer para a determinação dos ditos numeros.

É claro que se fôr simplesmente $p-1=2^{a}$, todos os residuos não quadraticos são raizes primitivas.

2.º Sendo $\alpha=1$, se fôr maior que 1 algum dos expoentes $\beta, \gamma, \delta, \ldots \varkappa$ dos factores $B, C, D, \ldots K$ de $p-1$, tome-se o menor destes numeros. vg. C, em que $\gamma>1$, e achados os residuos não quadraticos, procure-se o numero m necessario (§ 40) para a exclusão das potencias C. Feita essa exclusão, m póde representar m', m'', etc. para as exclusões relativas ás potencias $B, D, \ldots K$. Para qualquer dos numeros m', m'', etc. póde-se tambem tomar qualquer dos numeros não residuos potencias C.

3.º Sendo $\alpha=\beta=\gamma=\cdots=\varkappa=1$; na serie dos residuos não quadraticos tome-se um termo qualquer a, será

$$a^{B} \equiv r^{iB},$$

em que i será um numero impar.

Se i não fôr divisivel por nenhum dos numeros $C, D, \ldots K$, elevando successivamente a^{B} ás potencias impares

$$1,\ 3,\ 5,\ \ldots,\ \frac{p-1}{B}-1,$$

acharemos $\frac{p-1}{2B}$ residuos que serão todos incongruos, pois se vg.

$$r^{i_{i}iB} \equiv r^{i_{ii}iB},$$

teriamos

$$i_{i}iB \equiv i_{ii}iB\,\mathrm{M}\,(p-1),$$

donde

$$i_{i} \equiv i_{ii}\,\mathrm{M}\,\frac{p-1}{B},$$

o que é impossivel, pois i_{i}, i_{ii} são desiguaes e menores que $\frac{p-1}{B}$. Demais todos aquelles residuos são potencias B impares, mesmo quando

$$i_{i}iB > 2BC\ldots K;$$

logo os residuos achados são todas as $\frac{p-1}{2B}$ potencias B, que tinhamos a excluir da serie dos residuos não quadraticos.

Se porém elevando a^B successivamente ás potencias

$$1,\ 3,\ 5,\ \text{etc.},$$

acharmos um residuo

$$r^{i_1 iB} \equiv a^{i_1 B} \equiv a^B,$$

antes de termos obtido $\frac{p-1}{2B}$ residuos distinctos, será $i_1 - 1$ divisor de $\frac{p-1}{B}$, e fazendo

$$N = \frac{p-1}{B(i_1 - 1)},$$

ver-se-ha que temos excluido da serie dos residuos não quadraticos sómente as potencias NB.

Nos residuos restantes tome-se outro b tal que b^B não seja potencia NB, e elevando b^B successivamente ás potencias

$$1,\ 3,\ 5,\ \text{etc.}$$

(não aproveitando nesta serie os multiplos de N) até acharmos uma potencia

(64) $$r^{i_{11} iB} \equiv b^{i_{11} B} \equiv b^B,$$

os residuos obtidos antes do ultimo serão todos distinctos: e serão todos differentes das potencias já excluidas, se N fôr um numero primo, e mesmo quando N fôr composto, com tanto que não tenha um divisor, que o seja tambem de i em

$$b^B \equiv r'^B.$$

Se nenhuma dessas hypotheses se verificar, antes de chegarmos a obter (64), teremos achado uma potencia $r^{i_1 'B}$ congrua com uma das potencias NB já excluidas, e i será divisivel por N_1 um dos factores de N, primo, ou multiplo, e i_1 pelo outro $\frac{N}{N_1}$. O primeiro residuo que se encontra congruo com uma potencia NB já excluida, será aquelle em que $i = \frac{N}{N_1}$; logo na seguinte formação das potencias de b^B despresaremos os termos multiplos de $i_{\prime}$ na serie 1, 3, 5, etc., e não appareccerão de novo potencias NB. Se fôr $i_{\prime}$ o primeiro expoente que faz

$$b^{i_{\prime}B} \equiv b^B,$$

e suppondo

$$N' = \frac{p-1}{B(i_{\prime}-1)},$$

ver-se-ha, que temos excluido todas as potencias $N'B$.

Se ainda não tivermos excluido todas as potencias B, nos termos restantes da serie dos residuos não quadraticos tomaremos o termo c tal, que c^B não seja potencia NB, ou $N'B$; e formando as potencias 1, 3, 5, etc. de c^B (não aproveitando naquella serie os numeros multiplos de N, ou de N') antes de chegarmos a uma potencia congrua com c^B não teremos achado potencia alguma NB, ou $N'B$, excepto se em

$$c \equiv r^i$$

fôr i divisivel por um divisor de N, ou de N'. Supponhamos pois que antes de reproduzir a potencia c^B se encontrou uma potencia NB; excluiremos como acima dissemos todos os numeros da serie 1, 3, 5, etc., que dão essas potencias; e se continuando acharmos uma primeira potencia $N'B$, excluiremos similhantemente da mesma serie os numeros, que dão potencias dessa ordem.

Por esse modo proseguiremos até excluir todas as potencias B.

Dos residuos restantes tome-se vg. a', e eleve-se a'^C a todas as potencias designadas pelos termos impares e primos com B da serie ascendente

(65) $$1,\ n,\ n',\ n'',\ \text{etc.}$$

Se acharmos $\frac{p-1}{2B}(B-1)\frac{1}{C}$ residuos incongruos, serão esses todas as potencias C, que havia a excluir. Do contrario, a primeira potencia $n_{\prime}$ de a'^C, que reproduz esta quantidade, dar-nos-ha

$$N = \frac{p-1}{(n_{\prime}-1)C},$$

em que N será um dos divisores de $\frac{p-1}{2BC}$, e teremos

$$a'^{C} \equiv r^{n \cdot NC},$$

isto é, teremos excluido todas as potencias NC.

Tomando outra potencia b'^{C} não excluida, e formando successivamente as potencias designadas pelos termos da serie (65), em que supprimiremos os termos divisiveis por N, ou acharemos todas as restantes potencias C, ou teremos excluido sómente as potencias $N'C$; no progresso desse calculo teremos a supprimir na serie (65) os numeros, que dão potencias NC, se antes de acharmos

$$b'^{n_1 C} \equiv b'^{C},$$

tivermos encontrado uma das potencias NC já excluidas. Em tudo o mais imitaremos o processo indicado para a exclusão das potencias B.

Do mesmo modo excluiremos as potencias D, E, etc.

Na exclusão das potencias relativas a qualquer dos factores B, C, D, etc. para saber quando a operação deve terminar, escusamos contar os residuos supprimidos em cada uma das series de potencias que formamos: a exclusão estará concluida, logo que determinando successivamente os numeros N, N', N'', etc. acharmos um delles igual a 1.

Quando houver a excluir sómente as potencias relativas ao ultimo factor K, uma unica serie de potencias dará todas as exclusões (§ 42).

Quando houver a excluir sómente as potencias relativas aos dois ultimos factores I, K de $p-1$, no termo

$$a_{\prime}'^{I} \equiv r^{nI}$$

adoptado para a exclusão das potencias I, n será, ou deixará de ser divisivel por K. Na primeira hypothese, excluidas as potencias IK, qualquer dos numeros restantes em (53), cuja potencia I não tiver sido excluida, dará para a congruencia precedente n primo com $p-1$.

O methodo geralmente exposto acima, experimenta do mesmo modo alguma simplificação, quando restarem apenas os factores H, I, K, etc. Estas e outras simplificações occorrem porém facilmente, quando se desce ás applicações numericas.

No methodo precedente póde ainda ter logar um consideravel numero de ensaios infructuosos, pois que vg. depois de excluidas as potencias 2, B, C, se o termo $a_{,}$, que se toma para a exclusão das potencias D fôr vg.

$$a_{,} \equiv r^{EF},$$

excluiremos sómente as potencias DEF; e depois quando, para proseguir nas exclusões D, tomamos outro termo $b_{,}$, póde ser

$$b_{,} \equiv r^{nEF},$$

e poderá haver ainda um grande numero de termos dessa fórma.

Para evitar essas incertezas, proceder-se-ha do seguinte modo. Excluidas as potencias DEF, conhecer-se-ha que o termo $a_{,}$ tem a fórma indicada, e por conseguinte por meio delle excluimos todas as potencias EF, elevando $a_{,}$ a todos os expoentes, que não dão potencias já excluidas. E quando passarmos ás exclusões E, deve considerar-se que o processo começou já pela exclusão das potencias EF. Similhantemente se evitarão todas as outras tentativas inuteis, que presuppõe em geral o methodo exposto.

Para operar com facilidade e sem repetição todas as exclusões que temos a effeituar, convem começar por escrever a serie ascendente dos numeros impares

$$1,\ 3,\ 5,\ \ldots\ \frac{p-1}{2B},$$

notando explicitamente os que são divisiveis por algum, ou por alguns dos numeros B, C, D, etc., o que se effeitua, sem calculo algum, pela simples contagem dos termos.

Será tambem conveniente indicar junto a cada um dos residuos excluidos a especie de potencia, que elle é.

14. O methodo para a determinação das raizes primitivas dos numeros primos foi em vão procurado por Euler (*Novi Comm. Acad. Petrop.* T. XVIII.).

Nem Gauss, nem Legendre, que redigiram tratados completos sobre a theoria dos numeros, indicaram processo algum directo para essa determinação.

Foi Poinsot o primeiro que apresentou (memoria citada, pag. 73) um modo systematico para effeituar o calculo das raizes primitivas.

O principio em que elle funda esse calculo, é o mesmo de que partimos nos methodos antecedentemente expostos. Poinsot, depois de achados os residuos não quadraticos, eleva-os todos á potencia B; os residuos distinctos assim obtidos dão-lhe todas as potencias B, que se devem excluir da serie dos residuos não quadraticos. Os residuos restantes elevados todos á potencia C, dão a exclusão das potencias dessa ordem; proseguindo-se desse modo até excluir as potencias relativas a todos os factores primos de $p-1$.

Dessa maneira tem sempre a effeituar-se o maximo numero de operações repetidas: por exemplo, quando se faz a exclusão das potencias B, formam-se $\frac{p-1}{2}$ potencias desse gráu, quando o numero dellas que ha a excluir é apenas $\frac{p-1}{2B}$.

Para evitar esse inconveniente, Poinsot, em relação ao exemplo numerico que apresenta para a determinação das raizes primitivas de 31, diz, depois de ter achado os 15 residuos não quadraticos, e passando á exclusão dos residuos cubicos:

« Mais, comme on ne doit trouver que cinq cubes différents, on peut éviter les opérations inutiles, en rangeant d'abord les quinze non résidus dans l'ordre où ils suivraient une même raison géométrique. Qu'on prenne, par exemple, la raison 2, et les quinze non résidus pourront s'ordonner de cette manière:

$$3,\ 6,\ 12,\ 24,\ 17 \mid 15,\ 30,\ 29,\ 27,\ 23 \mid 13,\ 26,\ 21,\ 11,\ 22,$$

où ces non-résidus se trouvent distribués en trois groupes de cinq termes en progression géométrique, et dont les cubes sont:

$$27,\ 30,\ 23,\ 29,\ 15 \mid 27,\ 30,\ 23,\ 29,\ 15 \mid 27,\ 30,\ 23,\ 29,\ 15,$$

c'est à dire les mêmes pour chaque groupe.

Il suffit donc de former les cinq cubes des nombres contenus dans un quelconque des trois groupes. »

Em presença do que precedentemente havemos exposto, será facil fazer a discussão e apreciação desta regra.

No exemplo escolhido dá ella o mesmo resultado, que o processo que indicámos (§ 40). Com effeito, sendo a um residuo não quadratico, para que os cinco numeros

$$a,\ ad,\ ad^2,\ ad^3,\ ad^4 \tag{66}$$

sejam todos residuos não quadraticos é indispensavel, que seja d residuo quadratico, pois sendo $a \equiv r^t$, se fosse tambem $d \equiv r^{t'}$, os termos de (66) em que d tem expoente impar seriam residuos quadraticos. Depois, para que os mesmos termos sejam incongruos, é necessario que d seja raiz primitiva de uma congruencia

$$x^m \equiv 1,$$

em que $m > 1$; e como $d \equiv r^{2q}$ não póde ser raiz primitiva de

$$x^{30} \equiv 1, \text{ ou de } x^{10} \equiv 1, \text{ ou de } x^6 \equiv 1,$$

será necessariamente raiz primitiva de

$$x^3 \equiv 1, \text{ ou de } x^{15} \equiv 1;$$

no segundo caso os 15 não residuos distribuiam-se n'uma só progressão; e no primeiro distribuir-se-hão em tres progressões. Adoptando a ultima hypothese, e elevando ao cubo os termos de uma dellas (66), teremos, fazendo $d = d_{\prime}^{2}$,

$$a^3,\ a^3 d_{\prime}^{6},\ a^3 d_{\prime}^{12},\ a^3 d_{\prime}^{18},\ a^3 d_{\prime}^{24},$$

resultado que, por serem incongrúos estes termos, coincide com a nossa serie (55), em que se supponha $n = 5$.

Vê-se pois que não é necessario verificar a distribuição dos 15 não residuos nas tres progressões indicadas por Poinsot; basta achar um residuo quadratico d, que dê os cinco residuos não quadraticos (66).

Poinsot não indica porém, nem como se devem distribuir os residuos quadraticos para evitar a inutil repetição de exclusões em relação aos diversos factores primos que póde ter $p-1$, nem tão pouco dá o methodo para achar o numero d, que lhe serviu para a primeira distribuição, no exemplo que elle escolheu; por quanto ainda que nesse caso não houvesse difficuldade em reconhecer que se póde fazer $d = 2$, não acontecerá o mesmo, se forem muito grandes d, e o numero das potencias $\frac{p-1}{2B}$ a excluir, pois que os numeros ad, ad^2, ad^3, etc., quando excedem o modulo p, dão residuos em que não é facil distinguir aquella geração successiva.

Como se viu (§ 40), nem mesmo é sempre necessario, que se forme um primeiro grupo de $\frac{p-1}{2B}$ termos. Nesse processo, bem como em todos os outros que apresentámos, não só houve sempre em vista evitar o mais possivel toda a especie de inutil tentativa, mas tambem procurámos, que em vez de se ter a formar potencias analogas de numeros successivos, se effeituassem potencias ascendentes do mesmo numero, o que é muito mais vantajoso para o calculo numerico.

Muito antes da publicação da memoria de Poinsot (Janeiro de 1845) tinha Ivory (1824) inserido no 4.º volume do supplemento da *Encyclopedia Britannica* um methodo, que elle parece considerar como directo (*), para a determinação das raizes primitivas.

Esse methodo funda-se nas seguintes proposições. Sendo

$$p = 2^{\alpha} B^{\beta} C^{\gamma} D^{\delta} \ldots,$$

qualquer raiz primitiva de p satisfará á primeira das congruencias

$$(66') \quad x^{\frac{p-1}{2}} + 1 \equiv 0; \; x^{\frac{p-1}{2B}} + 1 \equiv 0; \; x^{\frac{p-1}{2C}} + 1 \equiv 0; \; x^{\frac{p-1}{2D}} + 1 \equiv 0; \text{ etc.},$$

e não satisfará a nenhuma das seguintes; e pelo contrario qualquer raiz não primitiva satisfará a alguma, ou algumas dessas congruencias, á excepção da primeira. Estes theoremas que o auctor não demonstra, provam-se com muita facilidade em presença do que temos exposto.

Supposto isso, obtidos os residuos não quadraticos, devem estes ensaiar-se successivamente até achar um delles, que não seja raiz da segunda, ou de alguma das seguintes entre as congruencias precedentes. Esse numero será uma raiz primitiva, que nos dará, pela elevação ás potencias competentes, todas as outras raizes primitivas.

Este processo, como se vê, não é um methodo directo, mas sim uma tentativa, que poderá repetir-se, antes de achar uma raiz primitiva, tantas vezes quantos são os residuos não quadraticos, que não são raizes primitivas.

É notavel que assim como Ivory observou, que os residuos quadraticos não satisfazem á primeira congruencia (66′), não reparasse tambem, que entre os residuos não quadraticos os que não são potencias B não satisfazem á segunda congruencia (66′); e deduzidos esses, não satisfarão á terceira congruencia (66′) os numeros restantes que não forem potencias C; e assim por diante: o que conduziria immediatamente ao methodo

(*) The existence of such numbers (the primitive roots) in everg case is therefore demonstrated; but no direct method of finding them has yet been published with which we are acquainted.

We gladly seize the present occasion of lying down a rule for finding the primitive roots of a prime number. — (Volume citado, pag. 698.)

de Poinsot, methodo que, comparado com o do distincto geometra inglez, merece mais, posto que não absolutamente, o nome de directo.

Sentimos não poder alludir aos trabalhos de Cauchy ácêrca das raizes primitivas (*Exercices de Mathém.* T. IV, 1829): não conseguimos encontrar em Lisboa esta collecção. É porém natural de acreditar, que esse illustre analysta não apresentasse um methodo directo, ou geralmente rapido, para a determinação das raizes primitivas, não só em vista do silencio de Poinsot a tal respeito, sendo a sua memoria publicada em 1845, mas até porque unicamente o methodo deste foi reproduzido por Serret (*Cours d'Algèbre Supérieure*, 1849), que todavia supprimiu inteiramente a simplificação a que acima alludimos, não obstante tratar tambem, como exemplo numerico, da determinação das raizes primitivas de 31.

A falta de um processo directo para achar as raizes primitivas tem sido o motivo por que as taboas daquelles numeros até agora publicadas são excessivamente restrictas, o que é notavelmente desvantajoso attento o grande uso que tem essas raizes na theoria dos numeros.

Por essa consideração nos persuadimos, que os methodos que apresentamos poderão de algum modo merecer a attenção dos geometras.

V.

CONSIDERAÇÕES GERAES SOBRE AS CONGRUENCIAS SUPERLINEARES DE MODULO MULTIPLO.

15. Passaremos agora a occupar-nos da congruencia

$$x^s \equiv 1 \text{ M } p, \tag{67}$$

em p é um numero multiplo qualquer, que podemos exprimir geralmente por $A^\alpha B^\beta C^\gamma$ etc., sendo A, B, C, etc. numeros primos diversos da unidade.

Tendo o modulo p um só divisor primo, isto é, sendo

$$x^s \equiv 1 \text{ M } A^\alpha, \tag{68}$$

Gauss (*Disquis. Arith.* § LXXXVIII) faz depender a determinação de uma raiz dessa congruencia da determinação correspondente á congruencia

$$x^s \equiv 1 \text{ M } A^{\alpha-1};$$

donde se infere, que sabendo nós determinar qualquer das raizes de

$$(69) \qquad x^s \equiv 1 \, M \, A,$$

teremos successivamente raizes congruas com essa para o modulo A, e que satisfazem ás congruencias dos modulos A^2, A^3, ... A^α.

E como o mesmo geometra indicou as formulas simples, que adiante apresentaremos, pelas quaes as raizes de (68) se dispartem em grupos compostos cada um de igual numero de raizes differentes e todas congruas, para o modulo A, com uma das raizes de (69), ficam desse modo determinadas todas as raizes de (68).

Este processo bastante longo e indirecto foi reproduzido por Legendre (*Théorie des n.*, 3 ͤ ed., T. II, pag. 21), e depois por Poinsot (*Refléx. sur les pr. fond. de la th. des n.*, chap. IV. art. VI).

Similhantemente quando o modulo é vg. $A^\alpha B^\beta C^\gamma$, Gauss tinha indicado que a resolução da congruencia binomia podia fazer-se depender da resolução de congruencias, que teriam respectivamente os modulos A^α, B^β, C^γ; e Legendre desenvolvendo essa indicação, mostrou como para cada raiz $a + zA^\alpha$ da congruencia relativa ao modulo A^α se podia successivamente determinar z de modo a satisfazer aquella raiz ás congruencias relativas a B^β, C^γ, e por conseguinte á congruencia proposta. Este mesmo processo foi depois seguido por Poinsot.

Como abaixo se verá, substituimos a esses methodos indirectos e de successiva resolução numerica, formulas geraes e directas, tanto para quando o modulo é potencia de um só numero primo, como quando é producto de potencias de varios numeros primos.

46. Podemos desde já reconhecer com facilidade, que todas as raizes da congruencia (67), em que p é um numero multiplo, são exactamente todas as raizes de

$$(70) \qquad x^D \equiv 1 \, M \, p,$$

em que D é o maior divisor commum entre s, e φp. A demonstração é perfeitamente analoga á que empregámos (§ 30), advertindo que qualquer raiz de (67) deve ser um numero primo com p, e que todos esses numeros são todas as raizes de

$$x^{\varphi p} \equiv 1 \, M \, p.$$

Em consequencia supporemos sempre quando houver a resolver qualquer congruencia binomia como (67), que o seu gráu é um divisor de φp

17. Para o que seguidamente temos a expor ser-nos-ha indispensavel demonstrar a formula

$$(71) \qquad (a+yp^q)^{sp^t} = a^{sp^t} + Yp^{q+t},$$

em que p é um numero primo > 2; a, y, Y, s numeros primos com p, cada um dos numeros q, s, $=> 1$; e $t => 0$.

Por simplicidade façamos $sp^t = m$; o primeiro membro de (71) desenvolvido dá

$$(a+yp^q)^m = a^m + m\,a^{m-1}(yp^q) + m\frac{m-1}{2}a^{m-2}(yp^q)^2 + \cdots$$

$$\cdots + m\frac{m-1}{2}\cdot\frac{m-2}{3}\;\cdots\;\frac{m-x+1}{x}a^{m-x}(yp^q)^x\;\cdots;$$

reconhecendo-se immediatamente, que a mais alta potencia de p que divide o segundo termo é p^{q+t}: provaremos agora que os termos seguintes são divisiveis por potencias de p superiores a essa, donde se conclue que o desenvolvimento tem a fórma (71).

Com effeito, considerando o termo geral acima escripto, vê-se que o seu coefficiente numerico tem a fórma $\frac{m}{x}A$, sendo A um inteiro, que representa um dos coefficientes do desenvolvimento de um binomio elevado á potencia $m-1$; aquelle termo tem pois a fórma

$$\frac{m}{x}Bp^{qx},$$

sendo B um inteiro. O valor de x representa-se do modo mais geral fazendo $x = rp^z$, onde r primo com p, e $=> 1$, $z => 0$, acontecendo que apenas no segundo termo do desenvolvimento poderá ser simultaneamente

$$r = 1, \quad z = 0.$$

Por ser r primo com p, deverá ser $\frac{sB}{r} = N$ numero inteiro; logo o termo geral reduz-se a

$$Np^{t-z+qrp^z}.$$

Se fôr $z = 0$, o expoente de p reduz-se a

$$t + qr > t + q$$

para todos os termos seguintes ao segundo, pois será nelles $r > 1$.

Não sendo porém $z = 0$, teremos

$$p^z = 1 + z\,lp + \frac{z^2}{2}\,l^2 p + \text{etc.} > 1 + z; \tag{72}$$

por quanto sendo $p > 2$, é $lp > 1$; e como q, bem como $r = > 1$, conclue-se de (72)

$$qrp^z > q + zq = > q + z;$$

logo

$$t - z + qrp^z > t + q,$$

o que completa a demonstração, que tinhamos a apresentar.

A formula (71) é devida a Gauss (obra citada, § LXXXVI), que a demonstrou indirectamente, suppondo successivamente $t = 1$, $t = 2$, etc. Poinsot imitando esse methodo, simplificou-o consideravelmente, empregando a formula do binomio, de que Gauss prescindíra, talvez para dar á sua demonstração uma fórma mais elementar. Ambas estas demonstrações tem o defeito de não serem directas. É notavel ainda que esses distinctos geometras se persuadissem que a demonstração immediata offereceria alguma difficuldade (*). Parece-nos porém que a demonstração directa que apresentámos nem é mais longa, nem mais difficil, que a de Poinsot, e é consideravelmente mais simples que a de Gauss.

18. A formula (71) soffre uma excepção quando fôr $p = 2$, e $q = 1$, sendo porém verdadeira ainda para $p = 2$, e $q > 1$. Com effeito, nesta

---

(*) Demonstratio hujus theorematis ex evolutione potestatis binomii peti posset, si ostenderetur omnes terminos post secundum per $p^{\mu+\nu+1}$ (p^{t+q+1} segundo a nossa notação) divisibiles esse. Sed quoniam consideratio denominatorum coefficientium in aliquot ambages deducit, methodum sequentem præferimus. — (GAUSS, *Disquisit. Arithmet.*, § LXXXVI.)

La démonstration immédiate de ce théorème, qui parait facile au prémier coup d'œil, présente néanmoins beaucoup de difficultés, à cause de l'exposant composé sp^r (sp^t segundo a nossa notação) d'où naissent les coefficients du binôme. Mais voici un moyen très simple de sortir de cet embarras, etc. — (POINSOT, *Considér. sur les princip. fondam. de la théor. des n.*, chap. IV, § 30.)

ultima hypothese a demonstração precedente experimentaria apenas a seguinte modificação. Teriamos

$$p^z = 1 + z\,l\,p + \frac{z^2}{2} l^2 p + \text{etc.} > 1 + \frac{1}{2} z;$$

e como $q => 2$, seria

$$r q p^z > q + z, \quad \text{donde} \quad t - z + r q p^z > t + q.$$

Sendo porém $p = 2$, $q = 1$, teriamos, para $s = t = 1$,

$$(a + py)^2 = a^2 + 4y(a + y);$$

e como a, e y são impares, suppondo ser 2^u a maxima potencia de 2 divisora de $a + y$, seria

$$(a + py)^2 = a^2 + Y p^{2+u},$$

sendo Y impar; e por conseguinte, pelo que acabámos de demonstrar, elevando ambos os membros da equação precedente á potencia sp^{t-1}, obteriamos

$$(73) \qquad (a + py)^{sp^t} = a^{sp^t} + Y' \cdot p^{1+u+t},$$

sendo Y' impar.

49. Se em (71) supposermos y divisivel por uma potencia qualquer de p, essa formula subsiste, entendendo-se que a mesma potencia, e não outra superior, dividirá necessariamente Y.

50. Se em (71) supposermos $q = 0$, não subsiste a demonstração que demos dessa formula. A investigação das modificações que então soffre a dita formula não será destituida de interesse, por nos conduzir a algumas propriedades notaveis dos residuos, de alguma das quaes teremos a fazer uso no capitulo seguinte.

Para evitar repetições, usaremos da letra P para designar qualquer numero primo com o modulo p.

Empregaremos tambem a notação $\frac{A\,\mathrm{M}\,p}{B}$, analoga á de Gauss $\frac{A}{B}$ (mod. p), e pela qual designaremos qualquer dos valores da fracção $\frac{A}{B}$, a cujo numerador se suppõe accrescentado um multiplo do modulo (sendo este primo ou multiplo) que converte a fracção em um inteiro. Assim

$$z \equiv \frac{A\,\mathrm{M}p}{B}$$

representa um valor achado pela resolução da congruencia

(74) $$Bz \equiv A\mathrm{M}p,$$

do mesmo modo que

$$z = \frac{A}{B}$$

representa o valor dado pela resolução da equação

$$Bz = A.$$

A fracção $\frac{A\,\mathrm{M}p}{B}$, que poderemos tambem designar por $\frac{A}{B}$, quando dahi não resultar confusão, gosa de propriedades analogas ás das fracções ordinarias. Podem multiplicar-se ambos os termos por um numero qualquer, ou dividir-se por elle: neste ultimo caso devem fazer-se as restricções indicadas (§ 4, 3.º e 4.º). A fracção z, sendo A, B primos entre si, é dada, como sabemos, pela congruencia

$$z \equiv AB^{\varphi p - 1}.$$

De (74) infere-se que só poderá ser $z \equiv 1$, quando fôr

$$B \equiv A,$$

e que z será primo com p, se com este o fôr tambem A.

Suppostas estas noções, tomemos os numeros a, y primos com o numero primo $p > 2$; e seja tambem $a + y$ primo com p; se s fôr primo com $p - 1$, teremos sempre

(74′) $$(a+y)^{sp^t} = a^{sp^t} + P;$$

pois que se pelo contrario fosse

$$(a+y)^{sp^t} \equiv a^{sp^t},$$

teriamos

$$\left(\frac{a+y}{a}\right)^{sp^t} \equiv 1,$$

o que é impossivel, por quanto $z = \frac{a+y}{a} > 1$, e primo com p, não póde ser simultaneamente raiz das congruencias

$$x^{sp^t} \equiv 1, \quad x^{p-1} \equiv 1,$$

mas sómente o será da ultima, sendo sp^t, $p-1$ primos entre si.

51. Supponhamos agora, que se toma para s qualquer dos divisores d, d', d'', etc. de $p-1$, será

$$(75) \qquad (a+y)^d = a^d + Pp^u, \text{ ou } (a+y)^d = a^d + P;$$

e para todos os divisores d, d', etc. a que corresponder a primeira equação, será sempre u constante, isto é, terá o valor que corresponde ao divisor maximo $p-1$: com effeito, a primeira equação elevada á potencia $\frac{p-1}{d}$ dá (71)

$$(a+y)^{p-1} = a^{p-1} + Pp^u.$$

Se fôr d o minimo dos divisores de $p-1$, que dá a primeira das equações (75), será $z = \frac{a+y}{a}$ raiz primitiva de

$$x^d \equiv 1;$$

logo se qualquer outro divisor d' der

$$(a+y)^{d'} = a^{d'} + Pp^u, \text{ donde } z^{d'} \equiv 1,$$

será $d' = md$. E será sempre $d = p-1$, se fôr z raiz primitiva de p.

52. Sendo pois d o gráu da congruencia de que z é raiz primitiva, se s, não divisivel por p, não fôr primo com $p-1$, teremos

$$(76)\qquad (a+y)^s = a^s + P p^u, \quad \text{ou} \quad (a+y)^s = a^s + P,$$

conforme s fôr, ou não fôr divisivel por d; na primeira hypothese terá u a mesma grandeza que em

$$(77)\qquad (a+y)^{p-1} = a^{p-1} + P p^u.$$

53. Suppondo por conseguinte que é D o maior divisor commum entre s, e $p-1$, verificar-se-ha a primeira, ou a segunda das equações (76), conforme fôr, ou não fôr z raiz da congruencia

$$x^D \equiv 1;$$

na primeira hypothese o valor de u será dado por qualquer das equações

$$z^D = 1 + P p^u; \quad z^d = 1 + P p^u; \quad z^{p-1} = 1 + P p^u.$$

54. Do que ultimamente havemos dito, e da formula (71) se conclue, que será geralmente

$$(78)\qquad (a+y)^{sp^t} = a^{sp^t} + P p^{u+t}, \quad \text{ou} \quad (a+y)^{sp^t} = a^{sp^t} + P,$$

conforme qualquer divisor commum entre s, e $p-1$, e por conseguinte o maximo D entre elles, der, ou não der

$$z^D \equiv 1.$$

55. Vê-se tambem, que como um numero qualquer $a < p$, e > 1, e primo com p, é necessariamente raiz primitiva de uma congruencia

$$x^d \equiv 1, \text{ isto é, } x^d = 1 + P p^u,$$

em que d dividirá $p-1$; teremos sempre, se s não fôr divisivel por p,

$$a^s = 1 + P p^u, \quad \text{ou} \quad a^s = 1 + P,$$

conforme s fôr, ou deixar de ser divisivel por d.

Se em vez do expoente s tomarmos sp^t será, para cada uma dessas hypotheses.

$$a^{sp^t} = 1 + Pp^{t+u}, \quad \text{ou} \quad a^{sp^t} = 1 + P.$$

56. Se $a+y$ fosse divisivel por p, sendo ainda a primo com p, é facil de ver que, para quaesquer valores de s, t, p, seria

$$(a+y)^{sp^t} = a^{sp^t} + P.$$

Logo se suppozermos $p = 2$, e forem a, y impares, será sempre

$$(i+I)^{i\cdot 2^t} = i^{i\cdot 2^t} + I'.$$

57. Na formula de Gauss

$$(a+yp^q)^{sp^t} = a^{sp^t} + Yp^{q+t}$$

entra apenas explicitamente o primeiro termo do desenvolvimento do primeiro membro. Em relação aos dois primeiros termos desse desenvolvimento podemos tambem estabelecer a formula seguinte, para $p > 2$, sendo $q > 0$,

$$(79) \qquad (a+yp^q)^{sp^t} = a^{sp^t} + sp^t a^{sp^t - 1} yp^q + Yp^{q+t+1},$$

(em que, mesmo para y primo com p, poderá ser Y divisivel por esse numero) cuja demonstração deduziremos dos mesmos principios com que provámos (71). Como vimos (§ 47) qualquer termo do desenvolvimento do primeiro membro de (79) representa-se por

$$Np^{t-z+qrp^z};$$

para os termos em que fôr $z = 0$, aquelle expoente reduz-se a $t + qr$; e como em todos os termos, posteriores ao segundo, em que fôr $z = 0$, será $r = > 2$, o dito expoente

$$t + qr = > t + 2q = > t + q + 1.$$

Nos termos em que não fôr $z=0$, será

$$p^z = 1 + z\,lp + \frac{z^2}{2}\,l^2p + \text{etc.} = 1 + z\left(lp + \frac{z}{2}\,l^2p + \text{etc.}\right)$$

$$=> 1 + z\left(lp + \frac{1}{2}\,l^2p + \text{etc.}\right) = 1 + z(p-1) => 1 + 2z:$$

logo o expoente

$$t - z + qrp^z => t - z + qr + 2qrz => t - z + q + 2z => t + q + 1;$$

e por conseguinte todos os termos do desenvolvimento posteriores ao segundo serão divisiveis por p^{q+t+1}, como exprime a formula (79).

Quando nessa formula y fôr primo com p, Y será sempre divisivel por p, excepto no caso unico em que fôr $q=1$; o que se demonstra facilmente em vista do que acabamos de expôr. Essa propriedade, bem como a determinação da mais alta potencia de p divisora de Y, ser-nos-hão porém inuteis para a applicação de (79), que temos a fazer no capitulo seguinte.

VI.

RESOLUÇÃO DA CONGRUENCIA $x^D \equiv 1 \text{ M} p^m$.

58. Passaremos agora a determinar as formulas geraes de resolução da congruencia

$$(80) \qquad x^D \equiv 1 \text{ M} p^m,$$

em que suppomos $p > 2$, e primo, e (§ 16) $D = p'p^t$, sendo p' divisor de $p-1$, $t < m$, e por conseguinte D divisor de $\varphi p^m = (p-1)\, p^{m-1}$.

Antes de deduzir essas formulas precisamos demonstrar, que (80) não póde ter mais de D raizes diversas.

Qualquer das raizes de (80) deve necessariamente satisfazer á congruencia

$$(81) \qquad x^D \equiv 1 \text{ M} p;$$

logo designando por a, b, c, d, etc. as p' raizes desta congruencia, menores que p, qualquer raiz A de (80) terá uma das fórmas

$$a + yp,\ b + y'p,\ c + y''p,\ \text{etc.};$$

vejamos qual é o maior numero de raizes, que poderá dar-se em cada uma destas especies. Supponhamos ser A uma raiz qualquer pertencente á fórma $a+yp$. Qualquer outra raiz de (80) incluida na mesma fórma, será expressa geralmente por $A+zp^u$, sendo $u =\!\!> 1$. Como temos

$$(A+zp^u)^D = A^D + Zp^{t+u} \equiv 1 + Zp^{t+u}\ \mathrm{M}\ p^m,$$

para que $A+zp^u$ seja raiz é indispensavel que tenhamos, supponda z primo com p, $t+u =\!\!> m$, ou $u =\!\!> m-t$; por conseguinte a formula geral de todas as raizes da fórma $a+yp$ será $A+zp^{m-t}$, em que z poderá ser divisivel por p. Ora todos os valores da ultima formula, incongruos para o modulo p^m, são os que resultam de se dar a z todos os valores

$$0,\ 1,\ 2,\ 3,\ 4,\ \ldots\ (p^t-1);$$

donde se conclue forçosamente que não póde haver mais de p^t raizes da fórma $a+py$; similhantemente haverá quando muito p^t raizes de cada uma das outras fórmas $b+y'p$, $c+y''p$, etc.; e como o numero de todas estas fórmas é p', vê-se finalmente que o numero de raizes de (80) não póde exceder $p^t p' = D$.

59. Para resolver a congruencia (80), mostraremos como as suas raizes dependem das de

(82) $$x^{p^t} \equiv 1\ \mathrm{M}\ p^{m-t},$$

e como as desta dependem das de

$$x^{p^t} \equiv 1\ \mathrm{M}\ p.$$

Sendo pois 1, a, b, c, etc. as p' raizes desta ultima, digo que serão

(83) $$1,\ a^{p^{m-t-1}},\ b^{p^{m-t-1}},\ c^{p^{m-t-1}},\ \text{etc.}$$

as raizes da precedente.

Com effeito, qualquer dessas quantidades é raiz, porque tomando vg. a segunda, e sendo

$$a^{p^t} = 1 + yp,$$

deduz-se

$$(a^{p^{m-t-1}})^{p'} = (1+yp)^{p^{m-t-1}} = 1 + Yp^{m-t};$$

logo o segundo dos numeros (83) é raiz de (82), e o mesmo acontece aos outros. Como (82) não póde ter mais de p' raizes, se reconhecermos que as p' raizes (83) são todas desiguaes, isto é, incongruas para o modulo p^{m-t}, essas raizes serão todas as de (82).

Ora a formula achada (74′) não só nos demonstra immediatamente, que os numeros (83) são incongruos para o modulo p^{m-t}, mas conduz-nos tambem a uma notavel propriedade desses numeros, isto é, das raizes de (82), e vem a ser, que todas estas são incongruas para o modulo p. Com effeito, suppondo $b > c$, e

$$b = c + s;$$

e sendo os numeros b, c, s primos com p, teremos, pela formula citada,

$$b^{p^{m-t-1}} = (c+s)^{p^{m-t-1}} = c^{p^{m-t-1}} + P,$$

em que será P primo com p.

Verificaremos agora que qualquer das raizes (83) de (82) é tambem raiz de (80); com effeito, visto que achámos

$$(a^{p^{m-t-1}})^{p'} = 1 + Yp^{m-t},$$

será, pela formula (71),

$$(a^{p^{m-t-1}})^{p'p^t} = 1 + Y'p^m;$$

e como as raizes (83) são incongruas para o modulo p, sel-o-hão para o modulo p^m, isto é, serão raizes distinctas de (80).

Ora todas as raizes

$$1,\ a^{p^{m-t-1}},\ b^{p^{m-t-1}},\ c^{p^{m-t-1}},\ \text{etc.}$$

pertencem correspondentemente aos grupos

$$(84)\qquad 1+yp,\ a+y'p,\ b+y''p,\ c+y'''p,\ \text{etc.}$$

a que acima alludimos; por quanto vg. é (15,), para o modulo p,

$$a \equiv a^p \equiv a^{p^2} \equiv a^{p^3} \equiv \ldots \equiv a^{p^{m-t-1}};$$

e pois que designando vg. $a^{p^{m-t-1}}$ por A, a formula $A + zp^{m-t}$ dá, como vimos, p' raizes diversas para (80); e como as raizes contidas em um dos grupos (84) são incongruas, até para o modulo p, com as raizes de outro desses grupos, concluir-se-ha finalmente, que todas as $p'p^t = D$ raizes assim deduzidas dos grupos (84) serão incongruas para o modulo p^m; e como (80) não póde ter mais de D raizes, ficará desse modo demonstrado, que essa congruencia tem effectivamente D raizes.

60. Do que acabámos de demonstrar se infere, que as D raizes de (80) são dadas pela formula

$$x \equiv x_i{}^{p^{m-t-1}} + yp^{m-t} \text{ M } p^m, \tag{85}$$

em que x_i é qualquer das p' raizes de

$$x^{p'} \equiv 1 \text{ M } p,$$

e y um dos numeros 0, 1, 2, 3. ... $(p^t - 1)$.

61. Se na congruencia dada (80) fôr

$$D = p'p^{m-1},$$

teremos $t = m - 1$, e por conseguinte a formula (85) muda-se em

$$x \equiv x_i + yp \text{ M } p^m, \tag{86}$$

na qual y póde ter os p^{m-1} valores 0, 1, 2, ... $(p^{m-1} - 1)$.

E se, além da hypothese precedente, suppozermos $p' = p - 1$, a formula (86) dará visivelmente todos os numeros menores que p^m, e primos com elle, os quaes, como é sabido, são todas as raizes da congruencia

$$x^{(p-1)p^{m-1}} \equiv 1 \text{ M } p^m.$$

Se em (80) suppozermos $D = p'$, será $t = 0$, o que mudará a formula (85) em

$$x \equiv x_i{}^{p^{m-1}} \text{ M } p^m. \tag{87}$$

E se finalmente tivermos $D = p'$, será $p' = 1$, as p' raizes $1.\ a,\ b,\ c$, etc. reduzir-se-hão unicamente á primeira, e teremos

$$x \equiv 1 + y p^{m-\iota} \ \mathrm{M}\, p^m.$$

62. A formula directa (85) tem ainda a vantagem de nos dar explicitamente todas as raizes *não primitivas* de (80), isto é, as raizes que satisfazem a

$$x^{D'} \equiv 1 \ \mathrm{M}\, p^m,$$

sendo D' um submultiplo qualquer de D, e por conseguinte serão raizes *primitivas* todas as que desse modo não ficam representadas.

Em primeiro logar reconheceremos, que não são raizes primitivas todas aquellas em que x_ι não fôr raiz primitiva de

$$x^{p'} \equiv 1 \ \mathrm{M}\, p. \tag{88}$$

Com effeito, sendo x_ι tal que tenhamos

$$x_\iota^{p''} \equiv 1 \ \mathrm{M}\, p,$$

em que é $p'' < p'$, e divisor deste ultimo numero, teremos

$$x_\iota^{p''} = 1 + Zp;\quad x_\iota^{p''p^{m-\iota-1}} = 1 + Zp^{m-\iota}, \tag{89}$$

e por conseguinte a formula (85) dará

$$x^{p''p'} = 1 + Z'p^m, \tag{90}$$

isto é, x satisfará a uma congruencia do gráu $p''p'$ submultiplo de D, e por tanto não será raiz primitiva de (80).

Reciprocamente, de

$$x^{p''p^\iota} = 1 + Z'p^m \equiv 1 \ \mathrm{M}\, p,$$

como

$$x^{p-1} \equiv 1;$$

concluiriamos (§ 30)

$$x^{p''} \equiv 1;$$

e por ser ((85))

$$x^{p''} \equiv x_{\prime}^{p'' p^{m-t-1}} \equiv 1,$$

teriamos

$$x_{\prime}^{p''} \equiv 1.$$

Se fôr pois $D = p'$, isto é, $t = 0$, todas as raizes primitivas de (80) serão as que dá a formula (87), em que se suppõe $x_{\prime}$ raiz primitiva de (88).

Vejamos agora, suppondo $t > 0$, a condição a que deve satisfazer y para que, sendo $x_{\prime}$ raiz primitiva de (88), não seja x raiz primitiva de (80). Neste caso deverá x satisfazer á congruencia

$$x^{p' p^{t-1}} \equiv 1 \text{ M } p^m.$$

Ora de (85) deduz-se nessa hypothese ((79))

$$x^{p' p^{t-1}} \equiv \left(x_{\prime}^{p^{m-t-1}}\right)^{p' p^{t-1}} + p' y p^{m-1} \left(x_{\prime}^{p^{m-t-1}}\right)^{p' p^{t-1} - 1} \equiv 1 \text{ M } p^m.$$

Cumpre pois satisfazer á congruencia

$$x_{\prime}^{p' p^{m-2}} + p' y p^{m-1} \cdot x_{\prime}^{p' p^{m-2} - p^{m-t-1}} \equiv 1 \text{ M } p^m.$$

Como é

$$x_{\prime}^{p'} = 1 + Q p,$$

teremos ((79))

$$x_{\prime}^{p' p^{m-2}} \equiv 1 + Q p^{m-1},$$

o que muda a congruencia precedente em

$$Q + p' y x_{\prime}^{p' p^{m-2} - p^{m-t-1}} \equiv 0 \text{ M } p,$$

que sempre é possivel, visto que p', $x_{\prime}$ são primos com p. Da ultima congruencia deduz-se

$$Q x_{\prime}^{p^{m-t-1}} + p' y x_{\prime}^{p' p^{m-2}} \equiv 0,$$

a qual, attendendo a que geralmente é

$$x_i^{p'} \equiv x_i, \text{ e } x_i^{p'} \equiv 1,$$

reduz-se a

$$Qx_i + p'y \equiv 0,$$

ou

(91) $$p'y \equiv -Qx_i,$$

que dá

(92) $$y = [-Qx_i p'^{\nu-2}] + y'p;$$

conclue se por tanto, que para qualquer valor x_i, raiz primitiva de (88), a formula

(92′) $$x \equiv x_i^{p^{m-t-1}} + ([-Qx_i p'^{\nu-2}] + y'p) p^{m-t} M p^m,$$

dá todos os valores (85), que não são raizes primitivas de (80), quando x_i o fôr de (88).

Todas as raizes não primitivas de (80) são pois comprehendidas em duas formulas; uma (85) em que se suppõe x_i raiz não primitiva de (88); outra (85), em que é x_i raiz primitiva de (88), e y raiz de (91). O numero das raizes dadas pela primeira dessas formulas será o producto do numero de raizes não primitivas de (88) pelo numero de valores que póde ter y em (85), isto é, será

$$(p' - \varphi p') p^t;$$

o numero das raizes dadas pela segunda das ditas formulas será o producto do numero de raizes primitivas de (88) pelo numero de valores, que póde ter y' em (92), isto é, será

$$\varphi p' \times p^{t-1}.$$

Vê-se tambem que todas as raizes primitivas de (80) são dadas pela formula (85), em que se suppõe x_i raiz primitiva de (88), e y não raiz de (91): logo o numero de raizes primitivas de (80) será

$$\varphi p'(p^t - p^{t-1}) = \varphi p' \cdot \varphi p^t = \varphi p' p^t = \varphi D.$$

As tres especies de raizes que temos considerado devem comprehender todas as de (80); e com effeito

$$(p' - \varphi p')p^t + \varphi p' \cdot p^{t-1} + \varphi D = p' p^t - \varphi p'(p^t - p^{t-1}) + \varphi D = D,$$

numero total dessas raizes.

63. Podemos sempre determinar pelo menos uma parte das φD raizes primitivas de (80), sem necessidade de fazer calculo algum para achar valores y, que não satisfaçam a (91); para isso basta que saibamos se Q é, ou não divisivel por p.

Com effeito, na primeira hypothese todo o valor y não divisivel por p não satisfaz a (91). Logo nesse caso (85), em que se supponha $x_{\prime}$ raiz primitiva de (88), e y não divisivel por p, dará

$$\varphi p'(p^t - p^{t-1}) = \varphi D$$

raizes primitivas de (80), que são todas as que esta possue.

Na segunda hypothese, sendo $x_{\prime}$ sujeito á condição indicada, e sendo y divisivel por p, (85) dar-nos-ha

$$\varphi p' \cdot p^{t-1} = \frac{\varphi D}{p-1},$$

raizes primitivas de (80).

64. A demonstração do numero de raizes primitivas de

(93) $$x^{p' p^t} \equiv 1 \,\mathrm{M}\, p^m,$$

póde effeituar-se por um modo inteiramente similhante a qualquer das duas demonstrações (§§ 33, 34).

Imitando a primeira dellas, teriamos similhantemente, supponde $p' = q^{\alpha} r^{\beta} s^{\gamma} \ldots,$

$$\psi^{\ldots s, r, q, p} S = \psi S\left[1 - {}_q\right]\left[1 - {}_r\right]\left[1 - {}_s\right] \ldots \left[1 - {}_p\right],$$

em que

$$\psi S_q = \frac{p' p^t}{q}; \quad \psi S_r = \frac{p' p^t}{r}; \quad \text{etc.} \quad \psi S_{q,r} = \frac{p' p^t}{qr}; \quad \text{etc.} \quad \psi S_p = \frac{p' p^t}{p};$$

$$\psi S_{p,q} = \frac{p' p^t}{pq}; \quad \text{etc.}$$

e por conseguinte

$$\psi^{\ldots r, q, p} S = p'p'\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\left(1-\frac{1}{s}\right)\cdots\left(1-\frac{1}{p}\right)=\varphi(p'p').$$

Imitando a segunda, provaremos que, sendo y, y' duas raizes quaesquer correspondentes ás congruencias

$$(94) \qquad x^{p'} \equiv 1 \text{ M } p^m; \quad x^{p'} \equiv 1;$$

1.º yy' é raiz de (93).

2.º Todos os $p'p'$ productos yy' são incongruos para o modulo p^m, e por conseguinte representam todas as soluções de (93).

3.º Todos os productos yy' cujos factores forem respectivamente raizes primitivas das congruencias (94), serão raizes primitivas de (93), e não serão raizes primitivas desta, os productos em que algum dos factores não fôr raiz primitiva da congruencia correspondente.

4.º A segunda das congruencias (94) tem p'^{-1} raizes não primitivas, porque estas são as raizes de

$$x^{p'-1} \equiv 1;$$

e por isso aquella terá $p' - p'^{-1} = \varphi p'$ raizes primitivas.

5.º Sendo $p' = q^{\alpha} r^{\beta} s^{\gamma} \ldots$, é sempre raiz da primeira das congruencias (94) o producto $zz'z'' \ldots$, cujos factores são respectivamente raizes das congruencias dos gráus q^{α}, r^{β}, $s^{\gamma} \ldots$; todos esses p' productos são incongruos para o modulo p^m, e por isso dão as p' raizes da congruencia do gráu p'. Serão raizes primitivas desta, sómente aquelles productos cujos factores forem todos raizes primitivas das congruencias correspondentes.

6.º Tendo pois as congruencias dos gráus q^{α}, r^{β}, s^{γ}, … respectivamente os seguintes numeros de raizes primitivas φq^{α}, φr^{β}, φs^{γ}, etc. (4.º), o numero de raizes primitivas da congruencia do gráu p' será

$$\varphi q^{\alpha} \times \varphi r^{\beta} \times \varphi s^{\gamma} \ldots = \varphi p',$$

e por conseguinte acharemos finalmente, que o numero de raizes primitivas de (93) é

$$\varphi p' \times \varphi p' = \varphi(p'p').$$

65. Achada uma raiz primitiva r de (93), serão todas as raizes dessa congruencia

$$r,\ r^2,\ r^3,\ \ldots\ r^{p'p'}-1,$$

o que se demonstra por um modo simillhante ao empregado (§ 36). E tambem se reconhecerá de uma maneira analoga á de que então usámos, que serão raizes primitivas todas as potencias r^n, em que n fôr primo com $p'p^t$.

66. Para a applicação numerica da formula (85) convem substituir no primeiro termo do valor de x o seu residuo minimo para o modulo p^{m-t}. Eis-aqui como esse calculo póde effeituar-se sem grande difficuldade. Determine-se rapidamente (§ 20) o residuo minimo x_2 de $x_t{}^p$ para o modulo p^2, será

$$x_t{}^{p^{m-t-1}} \equiv x_2{}^{p^{m-t-2}}\ \mathrm{M}\,p^{m-t};$$

determine-se simillhantemente o residuo minimo x_3 de $x_2{}^p$ para o modulo p^3; depois o residuo x_4 de $x_3{}^p$ para o modulo p^4; e assim successivamente até achar o residuo x_{m-t} de x^p_{m-t-1} para o modulo p^{m-t}; será

$$x_{m-t} \equiv x_t{}^{p^{m-t-1}}\ \mathrm{M}\,p^{m-t}.$$

Omittimos por brevidade varias outras simplificações, que occorrem facilmente ao calculador exercitado, que tiver presentes os principios, que temos exposto.

VII.

RESOLUÇÃO DA CONGRUENCIA $x^D \equiv 1 \text{ M } 2^m$.

67. Se tivermos a resolver a congruencia

$$x^D \equiv 1 \text{ M } 2^m,$$

em que por em quanto seja $m > 2$, devemos suppor (§ 46) D um divisor qualquer 2^t de $\varphi 2^m = 2^{m-1}$.

68. Consideremos em primeiro logar a congruencia

$$x^{2^{m-1}} \equiv 1; \tag{95}$$

são raizes desta todos os numeros impares menores que 2^m, isto é, todos os valores da formula $1 + y \cdot 2$, em que y deverá ser qualquer numero da serie

$$1,\ 2,\ 3,\ \ldots,\ 2^{m-1},$$

reduzindo ao seu residuo minimo 1, a raiz correspondente a $y = 2^{m-1}$.

A congruencia (95) tem pois um numero de raizes designado pelo seu gráu. Podemos representar mais commodamente essas raizes pela formula

(95′) $$x \equiv \pm 1 + y \cdot 2^2,$$

em que y poderá ter os valores

$$1,\ 2,\ 3,\ \ldots\ y^{m-2};$$

por quanto as raizes da fórma $-1 + y \cdot 2^2$ são as que correspondem á fórma $1 + y \cdot 2$, em que se suppõe y impar.

69. A congruencia (95) não tem raizes primitivas, por quanto qualquer valor $\pm 1 + y \cdot 2^2$ satisfaz a

$$x^{2^{m-2}} \equiv 1,$$

visto ser (§ 48)

$$(\pm 1 + y \cdot 2^2)^{2^{m-2}} = 1 + Y \cdot 2^m.$$

Podemos porém á falta dessas raizes primitivas absolutas, que pelas suas potencias successivas dariam todas as raizes de (95), considerar, como faz Poinsot, uma especie de raizes *primitivas imperfeitas*, e taes, que qualquer dellas ρ dará pelas suas potencias

(96) $$\rho,\ \rho^2,\ \rho^3,\ \ldots,\ \rho^{2^{m-2}}$$

2^{m-2} raizes distinctas de (95). Essas raizes primitivas são dadas pela formula $\pm 1 + y \cdot 2^2$, sempre que y fôr impar, por quanto nessa hypothese

$$\rho^{2^{m-2}} = (\pm 1 + i \cdot 2^2)^{2^{m-2}} = 1 + I \cdot 2^m;$$

e outra equação similhante prova que qualquer potencia de ρ, cujo expoente fôr $i' \cdot 2^t$, sendo $t < m - 2$, será incongrua com 1 para o modulo 2^m, donde (§ 15) serão todas as potencias (96) incongruas para esse modulo.

70. Supponhamos agora que se toma

(97) $$r = 1 + i \cdot 2^2;$$

terão essa mesma fórma os termos da serie

$$(98) \qquad r,\ r^2,\ r^3,\ \ldots\ r^{2^{m-2}},$$

cujos expoentes são impares (§ 48); e como o numero delles é 2^{m-3}, a dita serie contém, nos termos de ordem impar, todas as raizes primitivas da classe (97). As raizes (98) serão todas as 2^{m-2} raizes de (95), que tem a fórma $1+y\cdot 2^2$. Por conseguinte qualquer outra raiz primitiva da classe (97)

$$r' = 1 + i'\cdot 2^2$$

dará na serie (98) as mesmas raizes que produziu (97), posto que em ordem differente.

71. Similhantemente sendo

$$(99) \qquad r_{,} = -1 + i_{,}\cdot 2^2,$$

a serie

$$(100) \qquad r_{,},\ r_{,}^2,\ r_{,}^3,\ \ldots\ r_{,}^{2^{m-2}}$$

dará 2^{m-2} raizes distinctas de (95), entre as quaes as correspondentes a expoentes impares tem a fórma $-1+i_{,}'\cdot 2^2$, isto é, são todas as raizes primitivas da segunda classe (99).

72. As raizes (100), cujos expoentes são pares, coincidem com as potencias pares (98). Com effeito, tome-se para formar a serie (98) uma raiz

$$r' = 1 + (2^m - i_{,})\, 2^2;$$

teremos geralmente

$$r'^{2n} = (1 + (2^m - i_{,})\, 2^2)^{2n} \equiv (-1 + i_{,}\cdot 2^2)^{2n} = r_{,}^{2n};$$

isto é, as potencias pares de (98) coincidirão pela mesma ordem com as de (100). Logo se tomarmos para formar (98) a raiz (97), não sendo

$$i + i_{,} = 2^m,$$

coincidirão ainda as potencias pares de (98) e (100), posto que em differente ordem.

73. Do que acabamos de dizer se conclue, que qualquer outra raiz $r_{,}'$, da classe (99) dará todos os termos da serie (100), posto que em ordem diversa; pois que as potencias impares de $r_{,}'$ serão todas as raizes primi-

tivas de segunda classe (99), e as potencias pares coincidirão com as de (98). Vê-se tambem que as potencias de ordem impar de cada uma das series (98, 100) não podem achar-se na outra, pois que cada um desses grupos de potencias impares representa a totalidade das raizes primitivas (97), ou (99), e é sempre impossivel a congruencia

$$1+i\cdot 2^2 \equiv -1+i_{\prime}\cdot 2^2 \text{ M } 2^m.$$

74. Nas duas series (98, 100) acham-se pois todas as 2^{m-3} raizes de (95) da fórma $1+i.2^2$; todas as 2^{m-3} raizes da fórma $-1+i.2^2$, e finalmente todas as 2^{m-3} raizes da fórma $1+y\cdot 2^3$, que são as de ordem par em (98), ou em (100); e por conseguinte para completar a totalidade das 2^{m-1} raizes de (95) faltam 2^{m-3} raizes, que são todas as comprehendidas na formula $-1+y\cdot 2^3$, nenhuma das quaes entra em (98), ou em (100).

Todas as raizes porém da ultima classe, que tiverem a fórma $-1+i.2^{2+\alpha}$, serão dadas pelas $2^{m-3-\alpha}$ potencias daquelle numero, cujos expoentes forem

$$1,\ 3,\ 5,\ \ldots\ (2^{m-2-\alpha}-1),$$

reunião dos numeros impares menores que $2^{m-2-\alpha}$.

75. As raizes das duas fórmas

$$-1+i\cdot 2^2,\quad -1+y\cdot 2^3$$

deduzem-se de todos os valores de r^u

$$1+i\cdot 2^2,\quad 1+y\cdot 2^3$$

pela simples subtracção do numero 2; por conseguinte as 2^{m-1} raizes de (95) serão dadas pelas duas formulas

$$(101)\qquad x\equiv r^u \text{ M } 2^m;\quad x\equiv r^u-2,$$

em que

$$r=1+i\cdot 2^2,$$

é uma raiz primitiva qualquer de primeira classe, e em que se deve dar a u qualquer dos valores

$$1,\ 2,\ 3,\ \ldots\ 2^{m-2}.$$

As raizes primitivas de primeira, e de segunda classe serão dadas respectivamente pela primeira, e pela segunda das formulas (101), sempre que nellas se tomar para u um numero impar.

76. Similhantemente as raizes das duas fórmas

$$1+i\cdot 2^2,\quad -1+y\cdot 2^3$$

deduzem-se de todos os valores de r_i^u

$$-1+i\cdot 2^2,\quad 1+y\cdot 2^3,$$

juntando 2 aos de primeira especie, e tirando 2 aos de segunda, o que equivale a juntar ou tirar 2, conforme em r_i^u fôr u impar, ou par: logo as 2^{m-1} raizes de (95) serão tambem dadas pelas formulas

$$(102)\qquad x\equiv r_i^u;\quad x\equiv r_i^u-2(-1)^u.$$

em que

$$r_i=-1+i\cdot 2^2$$

é uma raiz primitiva qualquer de segunda classe, e u terá qualquer dos 2^{m-2} valores acima escriptos (§ 75).

As raizes primitivas de primeira, e de segunda classe serão dadas respectivamente pela segunda, e pela primeira das formulas (102), sempre que nellas se tomar para u um numero impar.

77. Consideremos agora geralmente a congruencia

$$(103)\qquad x^{2^{m-n}}\equiv 1\ \mathrm{M}\ 2^m,$$

em que $n>1$, e $n<m$.

As suas raizes devem ser numeros impares; ora como qualquer delles se póde representar por $\pm 1+i\cdot 2^\alpha$, em que $\alpha>1$, para que seja

$$1\equiv(\pm 1+i\cdot 2^\alpha)^{2^{m-n}}=1+I\cdot 2^{m-n+\alpha},$$

deve ser pelo menos $\alpha=n$: logo todas as raizes de (103) são dadas pela formula

$$(104)\qquad x\equiv\pm 1+y\cdot 2^n,$$

em que tomaremos para y qualquer dos numeros

$$1,\ 2,\ 3,\ \ldots\ 2^{m-n}.$$

Vê-se por tanto, que o numero das raizes de (103) é sempre o dôbro do seu gráu, exceptuando o caso já considerado, em que $n=1$, pois então o gráu designa o numero das raizes.

78. Qualquer valor x, em que y seja impar, não satisfaz a uma congruencia de gráu inferior a 2^{m-n}; por quanto sendo 2^{m-n-1} o maior submultiplo desse numero, não é

$$x^{2^{m-n-1}} \equiv 1,$$

pois

$$(\pm 1 + i \cdot 2^n)^{2^{m-n-1}} = 1 + I \cdot 2^{m-1}.$$

Apezar do que, a congruencia (103) não tem raizes primitivas senão imperfeitas, isto é, taes que pelas suas potencias successivas dão apenas metade das raizes dessa congruencia. Essas raizes são de duas classes, isto é, teremos

(105) $$r = 1 + i \cdot 2^n,$$

que dará as 2^{m-n} raizes distinctas de (103)

(106) $$r,\ r^2,\ r^3,\ \ldots\ r^{2^{m-n}};$$

ou teremos

(107) $$r_i = -1 + i_i \cdot 2^n,$$

que dará as 2^{m-n} raizes distinctas

(108) $$r_i,\ r_i^2,\ r_i^3,\ \ldots\ r_i^{2^{m-n}},$$

proposições que se demonstram como fizemos (§ 69).

79. Á similhança do que dissemos (§§ 70, 71, 72, 73) se reconhecerá, que as potencias impares da serie (106) dão sempre todas as raizes primitivas de primeira classe, e que as de segunda classe são dadas pelas potencias impares da serie (108); e outrosim se verá, que as potencias

pares das duas series dão as mesmas raizes, pela mesma ou por differente ordem, conforme fôr ou deixar de ser 2^m a somma dos numeros i, i_i que entram em (105, 107). Logo outra raiz de primeira classe r', e outra de segunda classe r_i' darão respectivamente todos os termos das series (106, 108), posto que em ordem differente.

80. As duas series (106, 108) dão pois 2^{m-n-1} raizes da fórma $1+i\cdot 2^n$; outras tantas da fórma $-1+i\cdot 2^n$; e finalmente o mesmo numero de raizes da fórma $1+y\cdot 2^{n+1}$; por conseguinte para completar a totalidade das 2^{m-n+1}, raizes de (103) faltam 2^{m-n-1}, que são todas as comprehendidas na formula $-1+y\cdot 2^{n+1}$, nenhuma das quaes entra em (106), ou em (108).

Todas as raizes porém da ultima classe, que tiverem a fórma $-1+i\cdot 2^{n+a}$ são dadas por todas as potencias impares menores que 2^{m-n-a} de qualquer das ditas raizes.

81. Tambem á similhança do que fizemos (§§ 75, 76) quando $n=1$, se verificará, que representando por r qualquer das raizes primitivas de primeira classe de (103); por r_i qualquer das de segunda classe, todas as raizes dessa congruencia serão dadas pelas formulas

$$(109) \qquad x \equiv r^u, \quad x \equiv r_i^u - 2;$$

ou tambem pelas formulas

$$(110) \qquad x \equiv r_i^u, \quad x \equiv r_i^u - 2(-1)^u,$$

dando a u, tanto em umas como em outras, todos os valores

$$1,\ 2,\ 3,\ \ldots\ 2^{m-n}.$$

As raizes primitivas de primeira classe serão dadas todas, ou pela primeira das formulas (109), ou pela segunda (110), dando a u todos os valores impares: as de segunda classe são dadas, para u impar, ou pela segunda (109), ou pela primeira (110).

82. No que temos exposto supposemos sempre, que na congruencia a resolver

$$(111) \qquad x^p \equiv 1\ M\ 2^m,$$

era D submultiplo do modulo, e $m > 2$. Se porém fôr $m = 2$, a congruencia dada será

$$x^2 \equiv 1 \text{ M } 4, \quad \text{ou} \quad x \equiv 1 \text{ M } 4;$$

a primeira tem as duas raizes 1, 3, das quaes a ultima é uma raiz primitiva absoluta. A segunda tem apenas a raiz 1.

83. Em vista do que dissemos (§§ 18, 68, 77, 82) conclue-se geralmente, que a congruencia (111) tem D raizes quando fôr $D = 1$, ou $D = 2^{m-1}$, e terá $2D$ raizes em todos os outros casos.

Cumpre-nos dizer, que a maior parte dos theoremas demonstrados neste capitulo acham-se na memoria de Poinsot (chap. IV, art. VII).

VIII.

RESOLUÇÃO DA CONGRUENCIA $x^D \equiv 1 \text{ M } A^\alpha B^\beta C^\gamma \ldots$

84. Suppondo o modulo $N = A^\alpha B^\beta C^\gamma \ldots$, sendo A, B, C, etc. primos entre si, e se tivermos a resolver a congruencia

$$(112) \qquad x^D \equiv 1,$$

devemos sempre suppor (§ 46) que D é divisor de φN.

85. A resolução geral de (112) depende da resolução das congruencias seguintes, em que D', D'', D''', etc. são respectivamente os maximos divisores communs entre D, e cada um dos numeros φA^α, φB^β, φC^γ, etc.

$$(113) \qquad x^{D'} \equiv 1 \text{ M } A^\alpha; \quad x^{D''} \equiv 1 \text{ M } B^\beta; \quad x^{D'''} \equiv 1 \text{ M } C^\gamma; \text{ etc.},$$

em virtude das proposições, que passamos a enunciar:

1.° Qualquer raiz x' de (112) é tambem raiz de todas as congruencias (113), pois que sendo vg.

$$x'^D \equiv 1 \text{ M } N \equiv 1 \text{ M } A^\alpha,$$

e por ser necessariamente x' primo com A, teremos

$$x'^{\varphi A^\alpha} \equiv 1;$$

e como D' é o maximo divisor commum entre D, e φA^α, concluir-se-ha

$$x'^{D'} \equiv 1.$$

2.° Reciprocamente qualquer raiz x' commum ás congruencias (113) será raiz de (112), pois que de

$$x'^{D'} \equiv 1 \text{ M } A^\alpha; \quad x'^{D''} \equiv 1 \text{ M } B^\beta; \quad x'^{D'''} \equiv 1 \text{ M } C^\gamma; \text{ etc.}$$

deduz-se, por serem D', D'', D''', etc. divisores de D,

$$x'^{D} \equiv 1 \text{ M } A^\alpha; \quad x'^{D} \equiv 1 \text{ M } B^\beta; \quad x'^{D} \equiv 1 \text{ M } C^\gamma; \text{ etc.};$$

logo

$$x'^{D} \equiv 1 \text{ M } N.$$

86. Em consequencia do que acabamos de demonstrar, não haverá difficuldade em estabelecer a formula geral de resolução de (112). Com effeito, determinem-se os numeros p, q, r, etc. taes que satisfaçam (§ 22) á congruencia

$$(114) \qquad p\frac{N}{A^\alpha} + q\frac{N}{B^\beta} + r\frac{N}{C^\gamma} + \text{etc.} \equiv 1 \text{ M } N;$$

e tomem-se os numeros a, b, c, etc., que sejam respectivamente raizes das congruencias (113); será raiz de (112)

$$(115) \qquad x \equiv a\,p\frac{N}{A^\alpha} + b\,q\frac{N}{B^\beta} + c\,r\frac{N}{C^\gamma} + \text{etc. M } N.$$

Esta formula dará, sem repetição, todas as raizes de (112), substituindo nella todos os systemas a, b, c, etc. de raizes das congruencias (113). Para o reconhecer notaremos:

1.° Todos os valores (115) são raizes de (112). Com effeito, elevando (115) á potencia D, e despresando os multiplos do modulo, acha-se

$$(116) \qquad x^D \equiv \left(a\,p\frac{N}{A^\alpha}\right)^D + \left(b\,q\frac{N}{B^\beta}\right)^D + \left(c\,r\frac{N}{C^\gamma}\right)^D + \text{etc.};$$

e como

$$a^D \equiv 1 \text{ M } A^\alpha;\quad b^D \equiv 1 \text{ M } B^\beta;\quad c^D \equiv 1 \text{ M } C^\gamma;\quad \text{etc.}$$

a congruencia (116) reduz-se a

$$x^D \equiv \left(p\frac{N}{A^\alpha}\right)^D + \left(q\frac{N}{B^\beta}\right)^D + \left(r\frac{N}{C^\gamma}\right)^D + \text{etc. M } N;$$

mas (114) elevada á mesma potencia D produz

$$\left(p\frac{N}{A^\alpha}\right)^D + \left(q\frac{N}{B^\beta}\right)^D + \left(r\frac{N}{C^\gamma}\right)^D + \text{etc.} \equiv 1,$$

logo

$$x^D \equiv 1.$$

2.° Reciprocamente qualquer raiz x de (112) será representada pela formula (115); pois que se forem respectivamente a', b', c', etc. os residuos desse valor x para os modulos A^α, B^β, C^γ, etc. teremos (§ 85, 1.°)

$$x^{D'} \equiv a'^{D'} \equiv 1 \text{ M } A^\alpha;\quad x^{D''} \equiv b'^{D''} \equiv 1 \text{ M } B^\beta;\quad x^{D'''} \equiv c'^{D'''} \equiv 1 \text{ M } C^\gamma;\quad \text{etc.};$$

a', b', c', etc. formarão pois um dos systemas a, b, c, etc. que podem entrar na formula (115).

3.° Todos os valores (115), correspondentes a systemas a, b, c, etc. a', b', c', etc. distinctos, são diversos, isto é, incongruos para o modulo N; pois que designando por x', x'' as duas raizes relativas áquelles systemas, se vg. suppozermos que a, a' são raizes distinctas da primeira das congruencias (113), como

$$x' \equiv ap\frac{N}{A^\alpha} \text{ M } A^\alpha,$$

donde, pela formula (114), será

$$x' \equiv a;$$

e como similhantemente

$$x'' \equiv a',$$

x', x'' serão incongruos para o modulo A^α, e por conseguinte para o modulo N.

87. Pelo exposto se conclue immediatamente o numero de raizes de (112). Com effeito, se nenhum dos factores A, B, C, etc. fôr 2, os numeros das raizes a, b, c, etc. serão respectivamente os gráus D', D'', D''', etc. das congruencias correspondentes (113); se vg. fôr $A=2$, e fôr $D'=1$, ou $D'=2^{\alpha-1}$, será ainda D' o numero das raizes a; esse numero será porém $2D'$, se, sendo $A=2$, fôr $D'>1$, e $D'<2^{\alpha-1}$. Conclue-se por tanto, que o numero das raizes de (112) será sempre $D'D''D'''$ etc., excepto quando fôr $A=2$, e $D'>1$, e $<2^{\alpha-1}$, pois nesses casos o numero das raizes é $2D'D''D'''$ etc.

A nossa formula (115), em relação ao laborioso processo de resolução successiva dado por Legendre, e por Poinsot, não tem pois só a vantagem de ser um methodo geral e directo, mas tambem a de nos conduzir immediatamente a determinar o numero de raizes de (112).

88. O gráu D da congruencia (112), sendo divisor de φN, terá necessariamente a fórma

$$D=A'A^{\alpha'}B'B^{\beta'}C'C^{\gamma'}\ldots,$$

em que A', B', C', etc. serão respectivamente divisores de $A-1$, $B-1$, $C-1$, etc., e α', β', γ', etc. respectivamente menores que α, β, γ, etc. Supponhamos que é d' o maior divisor commum entre $\frac{\varphi A^{\alpha}}{A'A^{\alpha'}}$, e $\frac{D}{A'A^{\alpha'}}$; d'', d''', etc. respectivamente os maximos divisores communs entre $\frac{\varphi B^{\beta}}{B'B^{\beta'}}$, e $\frac{D}{B'B^{\beta'}}$, entre $\frac{\varphi C^{\gamma}}{C'C^{\gamma'}}$, e $\frac{D}{C'C^{\gamma'}}$, etc.; será evidentemente

$$D'=A'A^{\alpha'}d'; \quad D''=B'B^{\beta'}d''; \quad D'''=C'C^{\gamma'}d'''; \text{ etc.}:$$

logo se nenhum dos numeros A, B, C, etc. fôr 2, o numero de raizes de (112) será

$$D'D''D''' \text{ etc.} = Dd'd''d''' \text{ etc.},$$

isto é, esse numero será sempre maior que o gráu D, e um multiplo delle, excepto unicamente se fôr

$$d'=d''=d'''=\text{etc.}=1. \tag{117}$$

Se se verificarem as condições precedentes, é claro que tambem D', D'', D''', etc. serão primos entre si; pois que se não fosse vg. $d'=1$.

esse numero dividiria $\frac{D}{A'A^{\alpha}}$, isto é, não poderia ser simultaneamente primo com $B'B^{\alpha'}$, com $C'C^{\gamma'}$, etc.; logo D' deixaria de ser simultaneamente primo com D'', com D'', etc. Reciprocamente sendo D', D'', D''', etc. primos entre si, verificar-se-hão as equações (117). Conclue-se por tanto que se nenhum dos numeros A, B, C, etc. fôr 2, sendo D', D'', D''', etc. primos entre si, a congruencia (112) terá D raizes; e reciprocamente.

Se um dos numeros A, B, C, etc. fôr 2, e D', D'', D''', etc. forem primos entre si, o numero das raizes de (112) será ainda D, se fôr $D'=1$, ou $D'=2^{\alpha-1}$, e será $2D$ nos outros casos.

Quando os numeros D', D'', D''', etc. não forem todos primos entre si, e fôr $A=2$, o numero das raizes de (112) será $Dd'd''d'''$ etc., ou $2Dd'd''d'''$ etc. conforme se verificar, ou não, uma das equações $D'=1$, $D'=2^{\alpha-1}$.

Se D fôr par, sel-o-hão todos os numeros D', D'', D''', etc., com a unica excepção de que sendo vg. $A^{\alpha}=2$, será $D'=1$.

89. Não sendo 2 nenhum dos numeros A, B, C, etc., se D', D'', D''', etc, não forem primos entre si, a congruencia (112) não póde ter raizes primitivas.

Com effeito, sendo $x_{\prime}$ uma raiz qualquer de (112), e devendo ella satisfazer ás tres congruencias (113), teremos

$$x_{\prime}^{D'}\equiv 1\,\mathrm{M}\,A^{\alpha};\quad x_{\prime}^{D''}\equiv 1\,\mathrm{M}\,B^{\beta};\quad x_{\prime}^{D'''}\equiv 1\,\mathrm{M}\,C^{\gamma};\quad \text{etc.};$$

ora não sendo D', D'', D''', etc. primos entre si, será o menor multiplo delles $\Delta < D'D''D'''$ etc.: logo como das congruencias precedentes se deduz

$$x_{\prime}^{\Delta}\equiv 1\,\mathrm{M}\,A^{\alpha};\quad x_{\prime}^{\Delta}\equiv 1\,\mathrm{M}\,B^{\beta};\quad x_{\prime}^{\Delta}\equiv 1\,\mathrm{M}\,C^{\gamma};\quad \text{etc.};$$

donde

$$x_{\prime}^{\Delta}\equiv 1\,\mathrm{M}\,N,$$

$x_{\prime}$ não será raiz primitiva de (112), pois que apenas poderá dar, pelas suas potencias successivas, Δ raizes de (112).

90. Se porém D', D'', D''', etc. forem primos entre si, não sendo 2 nenhum dos numeros A, B, C, etc., (112) terá sempre φD raizes primitivas.

Com effeito, tomem-se as raizes a, b, c, etc. respectivamente primitivas de cada uma das congruencias (113), serão tambem raizes primitivas dellas

$$a+yA^{\alpha},\quad b+y'B^{\beta},\quad c+y''C^{\gamma},\quad \text{etc.};$$

ora (§ 24) póde sempre dar-se a y, y', y'', etc. valores taes, que tenhamos

$$a + yA^\alpha = b + y'B^\beta;$$

$$a + yA^\alpha = c + y''C^\gamma;$$

$$\cdots\cdots\cdots\cdots$$

visto ser A primo com B, com C, etc.; logo

$$r = a + yA^\alpha,$$

será raiz primitiva de todas as congruencias (113), e por tanto se fôr n o menor expoente que faz simultaneamente

$$r^n \equiv 1 \text{ M } A^\alpha; \quad r^n \equiv 1 \text{ M } B^\beta; \quad r^n \equiv 1 \text{ M } C^\gamma; \quad \text{etc.},$$

n será divisivel por cada um dos numeros D', D'', D''', etc. (§ 13); e como elles são primos entre si, teremos

$$n = D'D''D''' \text{ etc.} = D,$$

isto é, r será raiz primitiva de (112).

Provada a existencia de uma raiz r primitiva de (112), entre as D raizes dessa congruencia

$$r, \; r^2, \; r^3, \; \ldots \; r^D,$$

serão primitivas aquellas cujo expoente fôr primo com D, o que se demonstra como fizemos (§ 36): logo o seu numero é exactamente φD.

91. Evidentemente se reconhece tambem, que haverá φD raizes primitivas em (112), se, sendo vg. $A = 2$, fôr $D' = 1$, e D'', D''', etc. forem primos entre si, e deixará de haver raizes primitivas para $D' > 1$, ou para D'', D''', etc. não primos entre si.

Conclue-se pois que, sendo $D = \varphi N$, ainda que não seja 2 nenhum dos factores A, B, C, etc., (112) não tem raizes primitivas, por quanto $A-1$, $B-1$, $C-1$, etc., e por conseguinte D', D'', D''', etc. tem sempre o divisor commum 2. Haverá porém φD raizes primitivas se fôr $D = \varphi N$, $N = 2A^\alpha$, e $A > 2$.

92. Até aqui havemos supposto, que se a congruencia a resolver fosse

$$x^t \equiv 1 \text{ M } N, \tag{118}$$

devel-a-hiamos substituir por (112), em que D é o maximo divisor commum entre s, e φN. Notaremos agora que os numeros D', D'', D''', etc. são tambem os maximos divisores communs entre s, e φA^α, φB^β, φC^γ, etc.; porque para achar D podiamos vg. procurar o maximo divisor commum D' entre s, e φA^α, depois o maximo divisor commum $D_{,}$ entre $\frac{s}{D'}$, e $\frac{\varphi A^\alpha}{D'}\varphi B^\beta C^\gamma \ldots$, e teriamos

$$D = D' D_{,}:$$

seriam pois $\frac{s}{D'}$, $\frac{\varphi A^\alpha}{D'}$ primos entre si, e por conseguinte $D_{,}$ primo com $\frac{\varphi A^\alpha}{D'}$: logo D' seria tambem o maximo divisor commum entre D, e φA^α. O mesmo se diz em relação a D'', D''', etc.

93. Seja Δ' o maximo divisor commum entre s, e ψN, designando por esta ultima expressão o menor multiplo commum de φA^α, φB^β, etc.: digo que será Δ' igual ao menor multiplo commum Δ de D', D'', etc.

Em primeiro logar qualquer factor primo f commum a s, e a ψN deve entrar em um dos numeros φA^α, φB^β, etc.; logo f entrará em um dos numeros D', D'', etc., e por tanto em Δ; todos os divisores primos de Δ' sel-o-hão pois de Δ. A reciproca desta proposição é tambem verdadeira, por quanto qualquer factor primo f de Δ entra em um dos numeros D', D'', etc., e por isso divide s, e um dos numeros φA^α, φB^β, etc., isto é, divide s, ψN, e o seu maximo divisor commum Δ'. Logo Δ, Δ' tem os mesmos divisores primos.

Seja agora f^m a maior das potencias do numero primo f, que dividem φA^α, φB^β, etc., e supponhamos vg. que f^m corresponde a φA^α; será f^m a maxima potencia divisora de ψN; logo a maxima potencia f^n que entra nos numeros D', D'', etc. corresponderá ao primeiro delles, e será f^n a maxima potencia commum a s, e ψN, isto é, a maxima potencia, que entra em Δ'; mas visivelmente tambem é f^n a maxima potencia que entra em Δ: logo finalmente Δ, Δ' contém os mesmos divisores primos elevados ás mesmas potencias, isto é, $\Delta' = \Delta$.

94. Todas as raizes de (112) satisfazem a (113), e por conseguinte a

$$(118') \qquad x^{\Delta} \equiv 1 \text{ M } N;$$

ora Δ, maximo divisor commum entre s, e ψN, é sempre divisor de D, maximo divisor commum de s, e $\varphi N = \varphi A^{\alpha} \varphi B^{\beta} \ldots$; logo todas as raizes de (118′) satisfazem a (112), e por conseguinte (112) póde ser substituida por (118′), que em muitos casos será de um gráu menor.

Supporemos pois d'ora em diante, que se fez essa reducção, isto é, supporemos em (112), que D é o maximo divisor commum entre s, e ψN, ou o menor multiplo commum de D', D'', D''', etc.

Feita pois essa hypothese, subsistem todos os theoremas demonstrados nos paragraphos antecedentes deste capitulo, porque nelles suppozemos que D era um divisor qualquer de φN, propriedade que compete a qualquer divisor de ψN.

95. Se a congruencia dada fôr

$$x^{\varphi N} \equiv 1,$$

que é satisfeita por todos os numeros primos com N, ver-se-ha pelo que demonstrámos precedentemente, que todos esses numeros são raizes de

$$x^{\psi N} \equiv 1;$$

logo no theorema de Euler

$$a^{\varphi N} \equiv 1$$

póde substituir-se φ por ψ.

Será

$$\varphi N = \psi N,$$

unicamente se N fôr um numero primo, ou potencia delle, ou o dòbro de um numero primo > 2, ou de qualquer potencia delle. Nos outros casos φA^{α}, φB^{β}, etc. terão pelo menos o divisor 2, e será por tanto $\psi N < \varphi N$, e ψN divisor de φN.

Vê-se tambem, que nos theoremas demonstrados (§§ 12, 13) póde substituir-se φ por ψ, e por conseguinte em todas as formulas de resolução das congruencias lineares (capit. II) podemos fazer uma analoga substituição.

96. Nas applicações que se fizerem da formula (115), é claro que os coefficientes de a, b, c, etc. devem reduzir-se ao seu residuo minimo para o modulo N. À mesma formula póde dar-se uma expressão mais simples, fazendo iguaes os numeros p, q, r, etc., á similhança do que fizemos (§ 25), isto é, determinando o numero p, que satisfaz a

$$(118'') \qquad p\left(\frac{N}{A^\alpha}+\frac{N}{B^\beta}+\frac{N}{C^\gamma}+\text{etc.}\right)\equiv 1 \text{ M } N.$$

Tomando pois por p a raiz propriamente dita da congruencia precedente, quer dizer, fazendo

$$p=\left|\left(\frac{N}{A^\alpha}+\frac{N}{B^\beta}+\frac{N}{C^\gamma}+\text{etc.}\right)^{\phi N-1}\right|,$$

mudar-se-ha (115) em

$$(119) \qquad x\equiv p\left(a\frac{N}{A^\alpha}+b\frac{N}{B^\beta}+c\frac{N}{C^\gamma}+\text{etc.}\right)\text{M } N.$$

Esta formula, bem como (115), tem ainda logar se A, B, C, etc. não forem numeros primos absolutos, mas sim primos entre si.

Podemos tambem deduzir de (115) uma formula de resolução immediatamente expressa em a, b, c, etc., A, B, C, etc.; com effeito, fazendo

$$p=\left(\frac{N}{A^\alpha}\right)^{\phi A^\alpha-1};\quad q=\left(\frac{N}{B^\beta}\right)^{\phi B^\beta-1};\quad r=\left(\frac{N}{C^\gamma}\right)^{\phi C^\gamma-1};\quad \text{etc.};$$

a congruencia (114) é satisfeita para os modulos A^α, B^β, C^γ, etc., isto é, para o modulo N; logo (115) mudar-se-ha em

$$(120) \qquad x\equiv a\left(\frac{N}{A^\alpha}\right)^{\phi A^\alpha}+b\left(\frac{N}{B^\beta}\right)^{\phi B^\beta}+c\left(\frac{N}{C^\gamma}\right)^{\phi C^\gamma}+\text{etc. M } N.$$

97. A formula (115), como vimos (§ 86, 3.º), dá para um systema qualquer de raizes a, b, c, etc.

$$x\equiv a \text{ M } A^\alpha;\quad x\equiv b\text{ M } B^\beta;\quad x\equiv c\text{ M } C^\gamma;\quad \text{etc.},$$

isto é, qualquer valor x dado por essa formula tem como residuos respectivamente para os modulos A^α, B^β, C^γ, etc. as raizes a, b, c, etc. que entram no dito valor.

Similhantemente acontece nas formulas (119, 120).

98. Em vez da equação de condição (114)

$$p\frac{N}{A^\alpha}+q\frac{N}{B^\beta}+r\frac{N}{C^\gamma}+\text{etc.}\equiv 1 \text{ M } N$$

poderiamos empregar

$$\left(p\frac{N}{A^\alpha}+q\frac{N}{B^\beta}+r\frac{N}{C^\gamma}+\text{etc.}\right)^n\equiv 1 \text{ M } N,$$

porque é apenas em ser satisfeita esta ultima congruencia, que se funda a demonstração que demos da formula (115). O mesmo se dirá relativamente á condição (118″); logo em (119) podemos fazer $p=1$, não só quando a funcção

$$\frac{N}{A^\alpha}+\frac{N}{B^\beta}+\frac{N}{C^\gamma}+\text{etc.}\equiv 1,$$

mas tambem quando essa funcção fôr uma das raizes da congruencia dada (112).

99. Supponhamos que não é 2 nenhum dos numeros A, B, C, etc.; sejam respectivamente R, R', R'', etc. raizes primitivas das congruencias (113); a formula (120) poderá substituir-se por

$$(121) \qquad x\equiv R^u\left(\frac{N}{A^\alpha}\right)^{\varphi A^\alpha}+R'^{u'}\left(\frac{N}{B^\beta}\right)^{\varphi B^\beta}+R''^{u''}\left(\frac{N}{C^\gamma}\right)^{\varphi C^\gamma}+\text{etc. M } N,$$

em que u, u', u'', etc. poderão ter todos os valores inteiros desde 1 até respectivamente D', D'', D''', etc.

100. Se fôr $A=2$, $D'=1$ a formula precedente reduz-se a

$$(122) \qquad x\equiv\left(\frac{N}{2^\alpha}\right)^{\varphi 2^\alpha}+R'^{u'}\left(\frac{N}{B^\beta}\right)^{\varphi B^\beta}+\text{etc.}$$

Se fôr $A^\alpha = 2^m$, $D' = 2^{m-n}$, sendo $n > 0$, e $n \leq m$, a formula (121) será substituida (§ 81) pelas seguintes

$$(123)\quad \begin{cases} x \equiv r^u \left(\frac{N}{2^m}\right)^{\varphi 2^m} + R'^{u'} \left(\frac{N}{B^\beta}\right)^{\varphi B^\beta} + \text{etc.}; \\ x \equiv (r^u - 2) \left(\frac{N}{2^m}\right)^{\varphi 2^m} + R'^{u'} \left(\frac{N}{B^\beta}\right)^{\varphi B^\beta} + \text{etc.}; \end{cases}$$

ou por

$$(123')\quad \begin{cases} x \equiv r_{\prime}^u \left(\frac{N}{2^m}\right)^{\varphi 2^m} + R'^{u'} \left(\frac{N}{B^\beta}\right)^{\varphi B^\beta} + \text{etc.}; \\ x \equiv (r_{\prime}^u - 2(-1)^u) \left(\frac{N}{2^m}\right)^{\varphi 2^m} + R'^{u'} \left(\frac{N}{B^\beta}\right)^{\varphi B^\beta} + \text{etc.}; \end{cases}$$

em todas as quaes se poderá dar a u todos os valores inteiros desde 1 até 2^{m-n}.

101. Quando (112) tiver raizes primitivas, será uma dellas (§ 90) o numero X, que fôr simultaneamente raiz primitiva de todas as congruencias (113); e se tomarmos os residuos R^u, $R'^{u'}$, $R''^{u''}$, etc. de X para os modulos A^α, B^β, C^γ, etc. esses residuos serão respectivamente raizes primitivas das ditas congruencias, isto é, u, u', u'', etc. serão respectivamente primos com D', D'', D''', etc.; logo as φD raizes primitivas de (112) corresponderão aos

$$\varphi_{\prime} D' \times \varphi_{\prime} D'' \times \varphi_{\prime} D''' \times \text{etc.} = \varphi_{\prime} D$$

systemas de valores de u, u', u'', etc., em que esses numeros são correspondentemente primos com D', D'', D''', etc. Todas as raizes primitivas de (112) serão pois dadas pelas formulas (121, 122), quando nellas se tomar para u, u', u'', etc. valores que tenham a indicada propriedade.

IX.

RESOLUÇÃO DA CONGRUENCIA $ax^s \equiv b \text{ M } N$.

102. Consideremos agora a congruencia binomia geral

$$(124) \qquad ax^s \equiv b \text{ M } N,$$

cujo modulo seja um numero qualquer primo, ou multiplo, e em que s é tambem um numero qualquer.

Em (124) devem a, N ser primos entre si; aliás se tivessem o maximo divisor commum $d > 1$, para que (124) fosse possivel, deveria ser b divisivel por d. Suppondo pois que nesse caso se dividiram a, b, N por d, consideraremos sempre a, N como primos entre si. Tambem podemos suppor sempre a, b primos entre si, pois se tivessem o maximo divisor d, o qual, sendo a, N primos entre si, seria primo com N, deduziriamos

$$\frac{a}{d} x^s \equiv \frac{b}{d}.$$

103. A congruencia (124) reduz-se sempre mui facilmente a ter a

unidade por coefficiente no primeiro membro; basta para isso multiplical-a por $a^{\phi N-1}$, e teremos

$$(125) \qquad x^s \equiv b a^{\phi N-1}.$$

Não só as raizes de (124) são raizes de (125), mas reciprocamente as desta satisfarão áquella, pois de (125) deduz-se (124), multiplicando a primeira por a.

Bastará pois sempre resolver a congruencia

$$(126) \qquad x^s \equiv c.$$

104. Outra reducção se póde ainda effeituar, a saber, podemos sempre suppor, que c, e N são primos entre si. Com effeito, se esses dois numeros tiverem um divisor primo $d > 1$, sendo respectivamente α, β os gráus das maximas potencias de d divisoras dos ditos numeros, será a congruencia proposta

$$(127) \qquad x^s \equiv c d^{\alpha}\ \mathrm{M}\ P d^{\beta},$$

e teremos a considerar os seguintes casos:

1.º Sendo $\alpha = \beta = qs$, o primeiro membro de (127) será divisivel por d^{qs}; logo $x = zd^q$, o que transforma a congruencia dada em

$$z^s \equiv c\,\mathrm{M}\,P.$$

2.º Sendo $\alpha = \beta = qs + s'$, em que $s' > 0$, e $< s$, e em que poderá ser $q = 0$; fazendo, como é necessario, $x = zd^{q+1}$, (127) muda-se em

$$d^{s-s'} \cdot z^s \equiv c\,\mathrm{M}\,P;$$

ora sendo d, e P primos entre si, podem determinar-se u, v taes que

$$c + uP = v d^{s-s'},$$

o que reduz a congruencia precedente a

$$z^s \equiv v.$$

3.° Sendo $\alpha > \beta$, e $\beta = qs$, a hypothese $x = zd^q$ muda (127) em

$$z' \equiv e d^{\alpha - \beta} \mathrm{M} P.$$

4.° Sendo $\alpha > \beta$, e $\beta = qs + s'$, $s' > 0$, e $< s$, a hypothese $x = zd^{q+1}$ muda (127) em

$$(128) \qquad d^{s-s'} \cdot z' \equiv e d^{\alpha - \beta} \mathrm{M} P;$$

e se $s - s' = < \alpha - \beta$, deduz-se logo dessa congruencia

$$z' \equiv e d^{\alpha - \beta - s - s'};$$

mas se fôr $s - s' = \alpha - \beta + \gamma$, podem determinar-se u, v taes que

$$e d^{\alpha - \beta} + u P d^{\alpha - \beta} = v d^{s - s'},$$

ou

$$e + u P = v d^{\gamma},$$

o que reduzirá (128) a

$$z' \equiv v.$$

5.° Sendo $\alpha = qs < \beta$, fazendo $x = zd^q$, a congruencia (127) reduz-se a

$$z' \equiv e \mathrm{M} P d^{\beta - \alpha}.$$

6.° Finalmente, sendo $\alpha = qs + s' < \beta$, em que $s' > 0$, e $< s$, a hypothese $x = zd^{q+1}$ muda (127) em

$$d^{s-s'} \cdot z' \equiv e \mathrm{M} P d^{\beta - \alpha},$$

congruencia impossivel, pois que e não é divisivel por d.

Como as considerações precedentes se applicam a qualquer outro divisor primo d' commum a c, e N, conclue-se que a congruencia (126) se póde sempre reduzir a outra em que esses numeros sejam primos entre si, excepto o caso unico, em que sendo na congruencia dada d^{α}, d^{β} as maximas potencias do numero primo d divisoras de c e de N, fôr $\beta > \alpha$, e este ultimo numero não fôr divisivel por s; quando isso acontecer a congruencia é irresoluvel, por ser impossivel. Como depois veremos, não é este o unico caso de impossibilidade de (126).

Supporemos pois sempre que na congruencia a resolver (126), c é primo com o modulo.

105. Sendo possivel a congruencia (126), e suppondo geralmente o modulo $N = A^\alpha B^\beta C^\gamma \ldots$, designemos por x' qualquer das suas raizes; esse numero deverá necessariamente ser primo com N, pois que N, e c se suppõe primos entre si. Se fôr x'' outra raiz da mesma congruencia, podemos determinar os numeros u, v taes que

$$x'' + uN = vx',$$

ou

$$x'' \equiv vx' \text{ M } N:$$

e como

$$x''^s \equiv c, \quad x'^s \equiv c,$$

será

$$x''^s \equiv v^s x'^s \equiv v^s c \equiv c,$$

donde

(129) $$v^s \equiv 1;$$

logo todas as raizes x', x'', x''', etc. de (126) podem exprimir-se por meio de uma dellas x', isto é, será sempre

$$x \equiv x'v,$$

sendo v qualquer das raizes de (129), as quaes são exactamente todas as raizes de

(130) $$v^D \equiv 1.$$

em que D é o minimo multiplo commum de D', D'', D''', etc. maximos divisores communs entre s e φA^α, φB^β, φC^γ, etc., ou D o maximo divisor commum de s, e φN. Em consequencia, se (126) tem uma raiz x_1, terá tantas raizes distinctas quantas são as da congruencias (130), por quanto se v', v'' fossem duas raizes differentes de (130), não seria

$$x'v' \equiv x'v'';$$

pois sendo x' primo com o modulo, teriamos

$$r' \equiv r'',$$

contra a hypothese.

106. Designaremos pelo symbolo $\sqrt[\prime]{c}\,\mathrm{M}\,N$, ou simplesmente $\sqrt[\prime]{c}$, que denominaremos *radical modular* (assim como ás fracções $\frac{A\,\mathrm{M}\,N}{B}$, ou $\frac{A}{B}$, poderiamos chamar *fracções modulares)* qualquer das raizes de (126).

O radical modular $\sqrt[\prime]{c}$ designa pois qualquer dos numeros inteiros que dá o radical arithmetico $\sqrt[\prime]{c+nN}$, quando o valor de n o torna racional.

Aquella notação proposta por Gauss, faz melhor reconhecer a notavel analogia, que existe entre as propriedades das raizes das congruencias, e das equações binomias, como engenhosamente demonstrou Poinsot *(Mém. sur l'applic. de l'algèb. à la théorie des nomb.)*, fazendo ver, que as formulas que dão a resolução das equações binomias são immediatamente applicaveis á resolução das congruencias binomias. Em virtude pois dessa convenção, será $\sqrt[D]{1}$ qualquer das raizes de

$$x^D \equiv 1,$$

e por conseguinte a proposição enunciada no paragrapho antecedente traduz-se analyticamente na seguinte formula de resolução de (126)

$$x = \sqrt[\prime]{c} \cdot \sqrt[D]{1}. \tag{130'}$$

Designando por ψD o numero de valores de $\sqrt[D]{1}$, qualquer dos valores de $\sqrt[\prime]{c}$ que adoptemos, esse nos dará sempre as ψD raizes de (126).

107. Investiguemos agora quaes são as condições, que tornam possivel uma solução da congruencia (126) em que c é primo com o modulo. Supponhamos em primeiro logar $N = A^\alpha$, sendo $\alpha => 1$, e $A > 2$.

Para que a congruencia

$$x^t \equiv c\,\mathrm{M}\,A^\alpha \tag{131}$$

seja possivel é necessario que, sendo D o maximo divisor commum entre s, e φA^a, e suppondo $\varphi A^a = DD_i$, tenhamos

$$(132) \qquad c^{D_i} \equiv 1;$$

com effeito, qualquer raiz x' de (131) devendo ser prima com A^a, e sendo $= tD$, teremos

$$c^{D_i} \equiv x'^{sD_i} \equiv x'^{tDD_i} \equiv x'^{t\varphi A^a} \equiv 1.$$

A condição (132) não só é necessaria, mas tambem é a sufficiente para que (131) seja resoluvel.

Com effeito, represente r qualquer das raizes primitivas de

$$x^{\varphi A^a} \equiv 1;$$

se formarmos a serie indefinida

$$(133) \qquad r^{tD},\ r^{2tD},\ r^{3tD},\ r^{4tD},\ \text{etc.}$$

o primeiro dos seus termos r^{ntD}, que faz

$$r^{ntD} \equiv 1,$$

será o que corresponde a $n = D_i$, pois que devendo ser

$$ntD \equiv 0 \text{ M } \varphi A^a \equiv 0 \text{ M } DD_i,$$

e sendo t primo com D_i, o minimo valor de n é D_i. Logo os D_i primeiros termos de (133) dão D_i residuos distinctos; ora esses residuos são todas as raizes de

$$(134) \qquad x^{D_i} \equiv 1 \text{ M } A^a,$$

pois

$$(r^{qtD})^{D_i} \equiv r^{qtDD_i} \equiv 1;$$

logo entre aquelles residuos necessariamente se encontrará c, pois suppomos c raiz de (134); por conseguinte se fôr

$$r^{qtD} \equiv c \equiv r^{qs},$$

será r^q raiz de (131).

Quando fôr $\alpha = 1$, isto é, quando tivermos a resolver a congruencia

$$x^{s} \equiv c \text{ M } A,$$

a condição (132) necessaria e sufficiente para a resolubilidade reduz-se a

(135) $$c^{A_{\prime}} \equiv 1,$$

em que $A_{\prime}$ designa o quociente de $A - 1$ por A', sendo esta ultima quantidade o maximo divisor commum entre s, e $A - 1$.

108. A condição (132) póde ser substituida por outra, que na maior parte dos casos será mais simples. Sejam A', $A^{\alpha'}$ os maximos divisores communs entre s, e $A - 1$, e entre s, e $A^{\alpha - 1}$; será, suppondo $A - 1 = A'A_{\prime}$,

$$D = \pm A' A^{\alpha'}; \quad D_{\prime} = A_{\prime} A^{\alpha - \alpha' - 1},$$

e por conseguinte (132) muda-se em

$$c^{A_{\prime} A^{\alpha - \alpha' - 1}} \equiv 1 \text{ M } A^{\alpha};$$

ora, como se viu no capitulo VI, qualquer numero c, que satisfaz á congruencia precedente, satisfaz tambem a

(136) $$c^{A_{\prime}} \equiv 1 \text{ M } A^{\alpha' + 1},$$

e reciprocamente: logo esta condição poderá sempre substituir (132), á qual será identica se $\alpha' = \alpha - 1$.

109. Supponhamos actualmente $A = 2$, isto é, seja proposta a congruencia

(137) $$x^{s \cdot 2^{m-n}} \equiv c \text{ M } 2^{m},$$

em que é inutil suppôr $n = > 0$, pois que então seria $c \equiv 1$.

A condição sufficiente para que (135) seja resoluvel não é já

(138) $$c^{2^{n-1}} \equiv 1,$$

como no caso precedente, ainda que a ultima congruencia deva verificar-se sempre que (137) tiver uma raiz, pois sendo essa necessariamente um numero impar i, teremos

$$c^{2^{n-1}} \equiv (i^{1\cdot 2^{m-n}})^{2^{n-1}} \equiv i^{1\cdot 2^{m-1}} \equiv 1.$$

Em vez de (138) teremos porém como necessaria e sufficiente condição da resolubilidade de (137)

$$(139) \qquad c \equiv 1 + y \cdot 2^{m-n+2},$$

em que y representa um numero qualquer.

Esta condição é necessaria, pois que sendo qualquer raiz de (137)

$$\varrho = \pm 1 + i \cdot 2^{2+\gamma},$$

em que $\gamma = > 0$, será

$$c \equiv \varrho^{1\cdot 2^{m-n}} = 1 + i_1 \cdot 2^{m-n+2+\gamma},$$

valor sempre comprehendido na formula (139).

Reciprocamente tendo logar (139), será sempre resoluvel (137).

Em primeiro logar, se fôr $m = 1$, será $n = 1$, e por tanto $c \equiv 1$, o que torna (137) resoluvel.

Se fôr $m = 2$, será $n = 1$, ou $n = 2$, e nestes dois casos (139) dará $c \equiv 1$, e logo (137) resoluvel.

Se fôr $m > 2$, e $n = < 2$, (139) dará $c \equiv 1$, e por tanto (137) resoluvel.

Supponhamos agora geralmente $m > 2$, $n > 2$, e $n < m$.

Tome-se um numero impar qualquer I representado pela formula

$$I = \pm 1 + i \cdot 2^2;$$

deduz-se dessa hypothese

$$I' = I^{1\cdot 2^{m-n}} = 1 + i' \cdot 2^{m-n+2};$$

e como $I'^{2^{n-2}}$ é a menor potencia de I' congrua com 1 para o modulo 2^m, os 2^{n-2} termos da serie

$$(140) \qquad I', \; I'^2, \; I'^3, \; \ldots \; I'^{2^{n-2}}$$

serão incongruos para o mesmo modulo, e qualquer delles

$$I'^{t} = 1 + y\cdot 2^{m-n+2}.$$

E como todos os valores incongruos que dá o segundo membro da equação precedente são 2^{n-2}, correspondentes aos valores de y

$$1,\ 2,\ 3,\ \ldots\ 2^{n-2},$$

segue-se que todos os residuos da serie (140) são dados por todos os residuos de $1 + y\cdot 2^{m-n+2}$: logo para um valor qualquer (139)

$$c \equiv 1 + y'\cdot 2^{m-n+2},$$

achar-se-ha necessariamente um expoente t tal que

$$I'^{t} \equiv c,$$

isto é,

$$I'^{\,t\cdot 2^{m-n}} \equiv c,$$

e por conseguinte I' sera raiz de (137).

110. Os 2^{n-2} valores de c dados pela condição (139), não são pois todas as raizes da congruencia (138)

$$x^{2^{n-1}} \equiv 1 \text{ M } 2^{m},$$

as quaes são dadas pela formula

(141) $$x \equiv \pm 1 + y\cdot 2^{m-n+1}.$$

A proposição que enunciámos para quando $A > 2$, soffre por conseguinte uma notavel excepção quando $A = 2$; neste caso supondo sempre em (131) $s = tD$, a condição

$$c^{D_{\prime}} \equiv 1 \text{ M } A^{a}$$

é ainda necessaria, mas já não é sufficiente para que a congruencia dada seja resoluvel. Para se dar a possibilidade de resolução é forçoso escolher para c as raizes que satisfazem, não á congruencia

$$x^{D_1} \equiv 1,$$

mas sim á congruencia

$$x^{\frac{1}{2}D_1} \equiv 1,$$

e mesmo entre estas adoptar sómente as que teem a fórma $1 + 4k$.

111. Verificada a possibilidade de haver uma raiz na congruencia

$$x^s \equiv c\,M\,A^\alpha,$$

existirão, como vimos (§§ 105, 106) necessariamente ψD raizes dadas pela formula

$$x \equiv \sqrt[s]{c} \cdot \sqrt[D]{1}.$$

112. Do que precedentemente exposemos é facil concluir as condições de possibilidade da congruencia

$$(142) \qquad x^s \equiv c\,M\,A^\alpha\, B^\beta\, C^\gamma \ldots,$$

em que suppomos primeiro que não é 2 nenhum dos numeros A, B, C, etc.

Qualquer raiz dessa congruencia sel-o-ha necessariamente das congruencias

$$(143) \qquad x^s \equiv c\,M\,A^\alpha; \quad x^s \equiv c\,M\,B^\beta; \quad x^s \equiv c\,M\,C^\gamma; \quad \text{etc.};$$

ora se dermos ainda a D', D'', D''', etc. as significações indicadas (§ 92), sendo A', B', C', etc. os maximos divisores communs entre s, e $A-1$, $B-1$, $C-1$, etc. teremos

$$D' = A'A^{\alpha'}; \quad D'' = B'B^{\beta'}; \quad D''' = C'C^{\gamma'}; \text{ etc.}$$

devendo ser os expoentes α', β', γ', etc. respectivamente menores que α, β, γ, etc.; e suppondo finalmente

$$A - 1 = A'A_1; \quad B - 1 = B'B_1; \quad C - 1 = C'C_1; \text{ etc.}$$

serão (§ 108) as condições necessarias da possibilidade simultanea das congruencias precedentes

$$(144)\qquad c^{A_1} \equiv 1\,\mathrm{M}\,A^{\alpha'+1};\quad c^{B_1} \equiv 1\,\mathrm{M}\,B^{\beta'+1};\quad c^{C_1} \equiv 1\,\mathrm{M}\,C^{\gamma'+1};\ \text{etc.}$$

Representando agora por Δ o minimo multiplo commum de A_1, B_1, C_1, etc., podemos, em vez das condições precedentes necessarias para que (142) seja possivel, adoptar a seguinte

$$(145)\qquad c^{\Delta} \equiv 1\,\mathrm{M}\,A^{\alpha'+1} B^{\beta'+1} C^{\gamma'+1} \ldots$$

113. Reciprocamente, verificadas as condições (144), a congruencia dada será possivel; por quanto dessas condições resulta a possibilidade de resolução de cada uma das congruencias (143); e se a, b, d, etc. forem respectivamente raizes dellas, poder-se-hão determinar z, z', z'', etc. taes que

$$a - zA^{\alpha} = b + z'B^{\beta} = d + z''C^{\gamma} = \cdots = \varphi;$$

logo será φ raiz commum das congruencias (143), e por conseguinte da congruencia dada.

114. As condições sufficientes de resolubilidade (144) podem substituir-se por uma só (145), quando, e só quando A_1, B_1, C_1, etc. forem respectivamente os maximos divisores communs entre Δ, e $\varphi A^{\alpha'+1}$, $\varphi B^{\beta'+1}$, $\varphi C^{\gamma'+1}$, etc.; pois que qualquer numero c que satisfaz á congruencia (145), dando vg.

$$c^{\Delta} \equiv 1\,\mathrm{M}\,A^{\alpha'+1},$$

na hypothese adoptada deduz-se desta (§ 60)

$$c^{A_1} \equiv 1\,\mathrm{M}\,A^{\alpha'+1},$$

e similhantemente se concluem as outras condições (144).

115. A substituição das condições sufficientes (144) por uma só (145) far-se-ha sempre quando forem D', D'', D''', etc. primos entre si; por quanto se podesse vg. ser $A_1 d$, sendo $d > 1$, o maior divisor commum entre Δ e $\varphi A^{\alpha'+1}$, como

$$\varphi A^{\alpha'+1} = (A-1)A^{\alpha} = A' A_1 A^{\alpha} = A_1 D,$$

d dividiria D', e por conseguinte o gráu s da congruencia dada; demais d seria divisor de algum dos numeros $B_{\prime}$, $C_{\prime}$, etc. vg. de $B_{\prime}$, e por conseguinte tambem de φB^{β}; mas sendo D'' o maior divisor commum entre φB^{β}, e s, e tendo estas quantidades o factor commum d, este dividiria D'', isto é, D', D'' teriam o divisor commum d, contra a hypothese.

116. A substituição das condições (144) por uma só (145) far-se-ha tambem sempre, quando D', D'', D''', etc. forem primos com Δ; pois que sendo vg.

$$\varphi A^{\alpha'+1} = A_{\prime} D',$$

e D' primo com Δ, será $A_{\prime}$ o maximo divisor commum entre Δ, e $\varphi A^{\alpha'+1}$.

117. Assim como reduzimos as condições (144), necessarias para a possibilidade da congruencia dada, a uma só (145), podemos tambem substituir qualquer numero dellas, vg. as tres primeiras, por uma só, isto é, em vez dellas adoptar

$$(146) \qquad c^{\Delta'} \equiv 1 \text{ M } A^{\alpha'+1} B^{\beta'+1} C^{\gamma'+1},$$

sendo Δ' o minimo multiplo commum de $A_{\prime}$, $B_{\prime}$, $C_{\prime}$.

Pelo que diz respeito ás condições sufficientes de possibilidade da congruencia dada, a condição (146) equivalerá ás tres primeiras, quando e só quando forem respectivamente $A_{\prime}$, $B_{\prime}$, $C_{\prime}$ os maximos divisores communs entre Δ' e $\varphi A^{\alpha'+1}$, $\varphi B^{\beta'+1}$, $\varphi C^{\gamma'+1}$. E em especial verificar-se-ha essa equivalencia quando forem D', D'', D''' primos entre si, ou quando esses numeros forem primos com Δ'.

118. Supponhamos actualmente que na congruencia dada (142) é vg. $A = 2$. As condições necessarias para a possibilidade de (142) serão (144), á excepção da primeira (que se reduziria a $c \equiv 1$); em vez dessa cumpre tambem satisfazer (§ 109) a

$$(147) \qquad c \equiv 1 + y \cdot 2^2 D' \text{ M } 2^{\alpha}.$$

Para ter agora as condições sufficientes para a possibilidade de (142), bastará reflectir que, sendo resoluvel essa congruencia, sel-o-hão simultaneamente

$$(148) \qquad x^s \equiv c \text{ M } 2^{\alpha}; \quad x^s \equiv c \text{ M } B^{\beta} C^{\gamma} \ldots;$$

e reciprocamente se cada uma destas fôr separadamente resoluvel, será possivel (142); pois que se fôr a raiz da primeira destas, e b da segunda, bastará para ter uma raiz ρ de (142); determinar z, z', que satisfaçam a

$$a + z \cdot 2^{\alpha} = b + z' B^{\beta} C^{\gamma} \ldots = \rho.$$

As condições sufficientes da possibilidade de (142) são pois as de cada uma das congruencias (148); a primeira dellas será possivel verificando-se (147); e a segunda será possivel, quando tiverem logar as condições indicadas (§§ 113, 114, 115, 116, 117).

119. Pelo que demonstrámos (§§ 107, 109, 112) é facil de vêr que para um modulo qualquer $N = A^{\alpha} B^{\beta} C \ldots$, em que poderá ser 2 algum dos seus divisores primos, serão tambem condições necessarias da possibilidade de

$$x^{s} \equiv c \text{ M } N,$$

suppondo respectivamente D', D'', D''', etc. os maiores divisores communs entre s, e φA^{α}, φB^{β}, φC^{γ}, etc. e

$$\varphi A^{\alpha} = D' D_{,}; \quad \varphi B^{\beta} = D'' D_{,,}; \quad \varphi C^{\gamma} = D''' D_{,,,}; \quad \text{etc.}$$

as seguintes

$$(148') \qquad c^{D_{,}} \equiv 1 \text{ M } A^{\alpha}; \quad c^{D_{,,}} \equiv 1 \text{ M } B^{\beta}; \quad c^{D_{,,,}} \equiv 1 \text{ M } C^{\gamma}; \quad \text{etc.},$$

e por conseguinte designando Δ o menor multiplo commum de $D_{,}$, $D_{,,}$, $D_{,,,}$, etc. será condição necessaria para a possibilidade da congruencia dada

$$(148'') \qquad c^{\Delta} \equiv 1 \text{ M } N.$$

As congruencias (148') serão as condições sufficientes de possibilidade, substituindo-se porém (147) á primeira dellas quando $A = 2$. Podiamos tambem á similhança do que fizemos precedentemente reduzir o numero das condições sufficientes (148').

120. Como vimos (§ 105) se a congruencia

$$(149) \qquad x^{s} \equiv c \text{ M } N,$$

em que $N = A^{\alpha} B^{\beta} C^{\gamma} \ldots$, tem uma raiz, terá tantas quantas são as de

$$(150) \qquad x^{D} \equiv 1,$$

em que D é o maximo divisor commum entre s, e ϕN.

Sendo pois ρ uma das raizes de (149), e sendo a resolução completa dessa congruencia dada (§§ 105, 106) por

$$x \equiv \rho \sqrt[D]{1} \equiv \sqrt[s]{c} \sqrt[D]{1},$$

(149) terá um numero de raizes (§ 87) designado por

$$(150') \qquad \psi s = D' D'' D''' \ldots,$$

se não fôr 2 nenhum dos numeros A, B, C, etc.

Porém se vg. $A = 2$, teremos

$$(150'') \qquad \psi s = D' D'' D''' \ldots,$$

unicamente se fôr $D' = 1$, ou $D' = 2^{\alpha - 1}$; e será

$$(150''') \qquad \psi s = 2 D' D'' D''' \ldots,$$

em todos os outros casos.

121. Gauss (obra citada § LXIV) demonstrou a condição necessaria e sufficiente de possibilidade de

$$(151) \qquad x^{s} \equiv c,$$

para um modulo primo.

No caso particular de $s = 2$, e para um modulo potencia de um numero primo A (tacitamente supposto > 2) achou Legendre (obra citada T. I, pag. 251) uma formula que dá sempre uma raiz de (151), conhecido um numero que lhe satisfaz para o modulo A; e por conseguinte demonstra, nessas hypotheses, que (151) é resoluvel para o modulo A^{α}, quando o fôr para o modulo A; ora para que esta ultima circumstancia se verifique deve ser pela condição de Gauss

$$c^{\frac{A-1}{2}} - 1 \,\mathrm{M}\, A,$$

o que combina com a nossa condição geral (136), pois no caso presente é

$$D=2;\ A'=2;\ \alpha'=0;\ A_{,}=\frac{A-1}{2}.$$

Legendre considera depois (pag. 253) que a congruencia (151) se refere ao modulo 2^m, e tendo separado os casos em que c é par, ou $m=2$, acha nos outros casos, por uma numeração algum tanto minuciosa, uma condição de resolubilidade, que reduz a

$$c=1+y\cdot 8,$$

que coincide inteiramente com a nossa formula geral (139) applicada ás presentes hypotheses.

Para completar o exame da possibilidade da congruencia

$$x^2\equiv c,$$

suppõe Legendre geralmente o modulo $N=A^\alpha B^\beta C^\gamma\ldots$ primo com c, e acha que é necessario verificar-se a possibilidade dessa congruencia para os modulos A^α, B^β, C^γ, etc. Ultimamente considera o caso de não ser N primo com c, expõe o modo de passar por outra congruencia em que essa circumstancia se não verifique, ou de reconhecer a impossibilidade da congruencia proposta pela natureza do divisor commum que houver entre c, e N.

As condições de possibilidade das congruencias binomias tinham pois sido achados unicamente para casos particulares.

A determinação do numero de raizes de (151) para um gráu qualquer, e para um modo multiplo (á excepção do caso particular tratado por Legendre, a que acima alludimos, e do caso discutido por Gauss, em que $c=1$ sendo o modulo potencia de um numero primo) tambem não nos consta que até agora tivesse sido publicada, posto que fosse bem facil achar esse numero pelo exame attento do processo de resolução de Legendre (T. II, pag. 21).

122. A congruencia

$$x^s\equiv c, \tag{152}$$

para um modulo qualquer N, e em que s não é divisor de ψN, uma vez que seja resoluvel, póde sempre substituir-se por outra relativa ao mesmo modulo, e cujo gráu seja o maximo divisor commum D entre s, e ψN, para o que bastará elevar (152) a uma potencia conveniente t. Com effeito, em

$$x^{ts} \equiv c^t$$

podemos determinar t de modo que

$$(153) \qquad ts = D + u\phi N, \quad \text{ou} \quad t \cdot \frac{s}{D} \equiv 1 \text{ M } \frac{\phi N}{D},$$

pois $\frac{s}{D}$, $\frac{\phi N}{D}$ são primos entre si. Suppondo em consequencia, por simplicidade, que na equação precedente se tomam, como é possivel, t, u positivos, e $t = < \phi N$, a penultima congruencia reduz-se a

$$(154) \qquad x^D \equiv c^t,$$

isto é, reconhece-se que todas as raizes de (152) satisfazem a (154): e como ambas ellas tem o mesmo numero de raizes (§ 114), conclue-se reciprocamente, que todas as raizes de (154) satisfazem a (152).

Tambem podiamos de (154) passar para (152) elevando a primeira á potencia $\frac{s}{D}$, pois que achariamos, em virtude de (153),

$$(155) \qquad x^s \equiv c^{\frac{st}{D}} \equiv c^{1 + u\frac{\phi N}{D}};$$

ora sendo possivel (154) será (§ 119) condição necessaria para isso,

$$c^\Delta \equiv 1 \text{ M } N;$$

porém tendo $D_{\prime}$, $D_{\prime\prime}$, $D_{\prime\prime\prime}$, etc. a significação indicida neste paragrapho, como é Δ divisor de

$$D_{\prime} D_{\prime\prime} D_{\prime\prime\prime} \ldots = \frac{\phi N}{D D' D'' \ldots}.$$

e sendo (§ 90) D divisor de $D' D'' D''' \ldots$, será Δ divisor de $\frac{\phi N}{D}$, e por conseguinte deduz-se da congruencia precedente

$$c^{\frac{\phi N}{D}} \equiv 1, \quad c^{u\frac{\phi N}{D}} \equiv 1,$$

o que reduz (155) á congruencia dada

$$x^s \equiv c.$$

A substituição da congruencia (152) por (154) que é a generalisação da transformação conhecida para quando $c = 1$, pois que então

$$x^s \equiv 1, \text{ equivale a } x^D \equiv 1,$$

em que D é o maximo divisor commum entre s, e φN, ou, como provámos, entre s, e ϕN, não tinha até agora sido feita senão para o caso de ser o modulo primo, porque depende de um dos dois principios que empregámos, o conhecimento do numero de raizes de (152), ou das suas condições de possibilidade.

123. Quando em (152) fôr s primo com ϕN essa congruencia será sempre possivel, e pelo que se viu no paragrapho antecedente teremos immediatamente o valor unico de x, que lhe satisfaz; por quanto fazendo então

$$ts = 1 + u\phi N,$$

deduz-se de (152)

$$x^{ts} = x^{1+u\phi N} \equiv x \equiv c^t;$$

isto é,

$$x \equiv c^{s^{\phi\phi N - 1}};$$

reciprocamente desta conclue-se

$$x^s \equiv c^{s^{\phi\phi N}} \equiv c.$$

Neste caso pois, achar o valor unico de $\sqrt[s]{c}$ equivale a elevar c a uma potencia determinada t, isto é, será

$$(156) \qquad \sqrt[s]{c} \equiv c^t \equiv c^{s^{\phi\phi N - 1}}.$$

124. Se fôr proposta a congruencia

$$(157) \qquad x^{sD} \equiv c,$$

que se suppõe possivel, e em que D é o maximo divisor commum entre ϕN, e sD; todas as suas raizes são todos os numeros que satisfazem a

$$(x')^D \equiv c,$$

isto é, a

$$(157') \qquad x' \equiv \sqrt[D]{c};$$

ora designando por ψD o numero de valores de $\sqrt[D]{c}$ (que é tambem o numero de valores de $\sqrt[D]{1}$) não se segue em geral, que no segundo membro de (157′) devam tomar-se todos esses valores, porque não se demonstra, que para todos elles seja possivel $\sqrt[\prime]{\sqrt[D]{c}}$. Effectivamente, como adiante se reconhecerá com facilidade, não se deverão adoptar todos esses valores, senão quando fôr s primo com ϕN.

Admittindo por em quanto esta hypothese, deve forçosamente dar-se ao segundo membro de (157′) todos os ψD valores que lhe competem, porque como a cada um delles corresponde (§ 123) um só valor de x em (157′), se nesta congruencia $\sqrt[D]{c}$ devesse ter menos de ψD valores, (157) teria menos de ψD raizes, o que não é verdade.

Suppondo pois ainda s primo com ϕN, e designando por $\sqrt[D]{_1 c}$, $\sqrt[D]{_2 c}$, $\sqrt[D]{_3 c}$, etc. os diversos valores de $\sqrt[D]{c}$, todas as raizes de (157) serão todos os valores de x, que satisfazem a alguma das seguintes congruencias

$$x' \equiv \sqrt[D]{_1 c}; \quad x' \equiv \sqrt[D]{_2 c}; \quad x' \equiv \sqrt[D]{_3 c}; \quad \text{etc.}$$

os quaes serão dados por

$$(158) \qquad x \equiv \sqrt[\prime]{\sqrt[D]{_1 c}}; \quad x \equiv \sqrt[\prime]{\sqrt[D]{_2 c}}; \quad x \equiv \sqrt[\prime]{\sqrt[D]{_3 c}}; \quad \text{etc.}$$

Por ser s primo com ϕN, estas congruencias reduzem-se em virtude da formula (156) a

$$(159) \qquad x \equiv \sqrt[\prime D]{_1 c} \equiv \left(\sqrt[D]{_1 c}\right)^{\prime}; \quad x \equiv \sqrt[\prime D]{_2 c} \equiv \left(\sqrt[D]{_2 c}\right)^{\prime}; \quad x \equiv \sqrt[\prime D]{_3 c} \equiv \left(\sqrt[D]{_3 c}\right)^{\prime}; \quad \text{etc.}$$

Como (157) tem ψD raizes, é forçoso que os ψD valores (159) sejam todos incongruos. Demais o numero t que entra em (159) satisfazendo a

$$(160) \qquad st = 1 + u\phi N = 1 + Du\frac{\phi N}{D},$$

equivale a um valor t que satisfaz a (153), que no caso actual se muda em

$$(160') \qquad sD \cdot t = D + u\phi N,$$

e para que isso aconteça basta suppor, que nesta equação se substitue u por uD; logo as raizes (159) equivalem a

$$\sqrt[D]{}_1 c^t, \quad \sqrt[D]{}_2 c^t, \quad \sqrt[D]{}_3 c^t, \quad \text{etc.},$$

isto é, teremos geralmente

$$(161) \qquad \sqrt[sD]{c} = \sqrt[s]{\sqrt[D]{c}} = \left(\sqrt[D]{c}\right)^t = \sqrt[D]{c^t},$$

em que t deve satisfazer á equação (160), e por conseguinte será primo com ϕN.

Se porém s não fôr primo com ϕN, isto é, se tiver um divisor commum a D, não podemos affiançar que todos os valores de $\sqrt[D]{c}$ tornam possivel (157′) e por conseguinte não podemos considerar (158) como as formulas de resolução de (157). Mas sem nos embaraçarmos com a escolha dos valores $\sqrt[D]{}_1 c$, $\sqrt[D]{}_2 c$, $\sqrt[D]{}_3 c$, etc., que são admissiveis, podemos tambem, no caso actual, chegar a uma conclusão analoga a (161), para o que basta tomar para t um valor qualquer que satisfaça a

$$(162) \qquad sDt = D + u^1 N,$$

e que seja primo com ϕN, propriedade que competirá a uma infinidade de numeros t, como passaremos a mostrar. Qualquer numero t, que satisfaz a (162) é primo com $\frac{\phi N}{D}$; logo para ter o numero procurado t, é sufficiente exprimir que t é primo com D; t é pois um numero qualquer que satisfaça ás duas equações

$$(162') \qquad \begin{cases} st = 1 + u\dfrac{\phi N}{D}; \\ xt = yD + 1; \end{cases}$$

e como a primeira dá, fazendo $\dfrac{\phi N}{D} = N'$,

$$t = s^{\phi N' - 1} + u'N',$$

deveremos satisfazer a

$$(163) \qquad x(s^{\phi N' - 1} + u'N') = yD + 1;$$

o que se consegue mui facilmente tomando

$$u' = q d^m d'^n d''^p \ldots,$$

sendo q um numero qualquer primo com todos os divisores primos de D, que dividem s, e d, d', d'', etc. todos os divisores primos de D que não entram em nenhum dos numeros s, q, N'. Satisfeitas estas condições, a equação (163) terá uma infinidade de soluções em numeros inteiros x, y, pois que os coeficientes destas incognitas são primos entre si, o que se reconhece sem difficuldade, advertindo que todos os divisores primos de D, são contidos separadamente nos dois termos

$$s^{\phi N' - 1}, \quad u'N',$$

pois s é primo com N', e não contém nenhum dos divisores primos de D, que entram em u', e este ultimo numero contém todos os divisores primos de D, que não entram em s, ou em N': logo qualquer divisor primo de D dividirá só um dos dois termos precedentes, e por conseguinte serão primos entre si

$$D, \quad \text{e} \quad s^{\phi N' - 1} + u'N'.$$

Determinando pois t com as condições indicadas, demonstraremos actualmente, que todas as raizes da congruencia dada são não sómente, satisfazendo t á primeira das equações (162'), os ϕD numeros

$$\sqrt[D]{}_1 c', \quad \sqrt[D]{}_2 c', \quad \sqrt[D]{}_3 c', \text{ etc.}$$

como provámos geralmente (§ 118) mas tambem, se t satisfizer igualmente á segunda das equações (162'),

$$\left(\sqrt[D]{}_1 c\right)^t, \quad \left(\sqrt[D]{}_2 c\right)^t, \quad \left(\sqrt[D]{}_3 c\right)^t, \text{ etc.,}$$

para o que se deve verificar que qualquer destes numeros é raiz da congruencia dada

$$x^{t\,D} \equiv c,$$

e que todos elles são incongruos. A primeira proposição é mui facil de demonstrar, pois que fazendo vg. a substituição do primeiro termo da serie antecedente achamos

$$\left(\sqrt[D]{}_1 c\right)^{t.D} = \left(\sqrt[D]{}_1 c\right)^{D+u\phi N} \equiv \left(\sqrt[D]{}_1 c\right)^{D} = c$$

A verdade da segunda proposição reduz-se á impossibilidade vg. da congruencia seguinte

$$\left(\sqrt[D]{}_1 c\right)^t \equiv \left(\sqrt[D]{}_2 c\right)^t,$$

impossibilidade que se estabelece por um modo inteiramente analogo ao que nos serviu para demonstrar a nossa formula (74'); pois que sendo qualquer dos numeros $\sqrt[D]{}_1 c$, $\sqrt[D]{}_2 c$ primo com o modulo N, fazendo

$$z \equiv \frac{\sqrt[D]{}_1 c \text{ M } N}{\sqrt[D]{}_2 c}$$

achariamos pela substituição na congruencia precedente

$$z^t \equiv 1,$$

donde por ser t primo com ϕN, pois que ((162')) é t primo com $\frac{\phi N}{D}$, e com D',

$$z \equiv 1 \text{; e logo } \sqrt[D]{{}_1c} \equiv \sqrt[D]{{}_2c},$$

o que é contra a hypothese.

Podemos pois tambem no caso de nos ser dada a congruencia

$$x^{s^D} \equiv c,$$

em que s não é primo com ϕN, isto é, tem um divisor commum com D, estabelecer as congruencias (161), uma vez que t seja determinado com as condições indicadas.

125. Os theoremas que precedentemente demonstrámos conduzir-nos-hão a estabelecer os principios em que se deve fundar o calculo dos radicaes modulares multiplos, qualquer dos quaes vg. $\sqrt[s]{c}$ apresenta qualquer das raizes da congruencia, que suppomos possivel,

$$(164) \qquad x^s \equiv c \,\mathrm{M}\, N,$$

em que s, e N são quaesquer numeros. Esses principios, como se verá, tem bastante analogia com os que regulam o calculo dos radicaes algebricos multiplos, sendo porém indispensaveis, para os radicaes modulares, certas attenções especiaes, de que faremos uma desenvolvida exposição.

126 Em primeiro logar convirá recordar, que o numero de valores de $\sqrt[s]{c}$, é o numero de raizes da congruencia

$$x^D \equiv 1,$$

em que D é ainda o maximo divisor commum entre s e ϕN. Continuando a designar por ψ o numero de raizes de (164), ou do radical $\sqrt[s]{c}$, teremos

$$\psi s = \psi D.$$

127. Não sendo $c \equiv 1$, não será 1 nenhum dos valores de $\sqrt[s]{c}$, pois que é 1 raiz de

$$x^s \equiv 1,$$

128. Sendo possiveis $\sqrt[\prime]{c}$, $\sqrt[\prime]{c'}$, será possivel $\sqrt[\prime]{cc'}$, para o que basta que verifiquemos a existencia de um valor do ultimo radical; ora designando por $\sqrt[\prime]{}_1 c$, $\sqrt[\prime]{}_1 c'$ valores particulares dos dois primeiros radicaes, e fazendo

$$x_{\prime} \equiv \sqrt[\prime]{}_1 c\,;\quad x_{\prime\prime} \equiv \sqrt[\prime]{}_1 c',$$

teremos

$$x_{\prime}{}' \equiv c\,;\; x_{\prime\prime}{}' \equiv c'\,;\; (x_{\prime} x_{\prime\prime})' \equiv cc',\ \text{donde}\ x_{\prime} x_{\prime\prime} \equiv \sqrt[\prime]{cc'}.$$

Logo da possibilidade das raizes modulares $\sqrt[\prime]{c_1}$, $\sqrt[\prime]{c_2}$, $\sqrt[\prime]{c_3}$, etc. seguir-se-ha a possibilidade das seguintes

$$\sqrt[\prime]{c_1 c_2 c_3 \ldots},\ \sqrt[\prime]{c_1^{\,m}},\ \sqrt[\prime]{c_1^{\,m} c_2^{\,n} c_3^{\,q} \ldots},\ \text{etc.}$$

129. Sendo possiveis $\sqrt[\prime]{c}$, $\sqrt[\prime]{c'}$ sel-o-ha $\sqrt[\prime]{\frac{c}{c'}}$, designando por $\frac{c}{c'}$ qualquer dos valores da fracção modular $\frac{cMN}{c'}$; por quanto com as hypotheses do paragrapho precedente, empregando ainda a notação das fracções modulares, teremos (§ 4, 8.º), advertindo que $x_{\prime\prime}$, c' são primos com o modulo N,

$$\frac{x_{\prime}{}'}{x_{\prime\prime}{}'} \equiv \left(\frac{x_{\prime}}{x_{\prime\prime}}\right)' \equiv \frac{c}{c'},\ \text{donde}\ \frac{x_{\prime}}{x_{\prime\prime}} \equiv \sqrt[\prime]{\frac{c}{c'}}.$$

130. Da possibilidade de $\sqrt[\prime]{c}$, e de $\sqrt[\prime]{c'}$, concluir-se-ha pois (§§ 128, 129) a de $\sqrt[\prime]{\frac{c^m}{c'^{m'}}}$.

131. Sendo possivel $\sqrt[\prime]{c}$, e suppondo $s = s's_{\prime}$, será tambem possivel sempre $\sqrt[s_{\prime}]{c}$, pois de

$$x_{\prime} \equiv \sqrt[\prime]{c},\ \text{deduz-se}\ x_{\prime}{}' \equiv c \equiv (x_{\prime}^{s'})^{s_{\prime}},\ \text{e}\ x_{\prime}^{s'} \equiv \sqrt[s_{\prime}]{c}.$$

132. Reciprocamente não podemos concluir da possibilidade de $\sqrt[s_{\prime}]{c}$

a de $\sqrt[i]{c}$, que depende de ser resoluvel a congruencia $x^{i} \equiv c$; nem tão pouco podemos concluir a possibilidade de $\sqrt[i']{\sqrt[i'']{c}}$ para qualquer dos valores de $\sqrt[i'']{c}$, pois que alguns delles poderão tornar impossivel

$$x^{i'} \equiv \sqrt[i'']{c}.$$

133. Expostas estas noções preliminares, carecemos antes de passar a diante determinar os casos em que sendo

$$s = s_1\, s_2\, s_3 \ldots,$$

teremos

$$(165) \qquad \psi s = \psi s_1 \times \psi s_2 \times \psi s_3 \ldots.$$

Supponda ainda que a caracteristica ψ é referida ao modulo mais geral $N = A^{\alpha} B^{\beta} C^{\gamma} \ldots$, vejamos em primeiro logar quando a equação precedente se verifica em relação ao modulo A^{α}. Designando nesse caso por ψ_A a caracteristica correspondente, deverá ser

$$(166) \qquad \psi_A s = \psi_A s_1 \times \psi_A s_2 \times \psi_A s_3 \ldots.$$

Vê-se immediatamente que esta equação é verdadeira:

1.° Quando não entra em s nenhum dos factores primos de φA^{α}; então

$$\psi_A s = \psi_A s_1 = \psi_A s_2 = \ldots = 1.$$

2.° Quando qualquer f dos factores primos de φA^{α} não entra em dois, ou mais dos factores s_1, s_2, s_3, etc.

Resta pois discutir os casos em que f é divisor de mais de um dos numeros s_1, s_2, s_3, etc.

Supponhamos primeiro $A > 2$. Sendo f^p, f^q as mais altas potencias de f, que dividem respectivamente φA^{α}, e s, teremos a considerar os dois casos:

$$(167) \qquad q = \,< p;\ \text{ou}\ q > p.$$

Na primeira hypothese, sendo $f^{q'}$, $f^{q''}$, etc. as mais altas potencias de f, que dividem respectivamente s_1, s_2, etc., será

$$f^{q'} \cdot f^{q''} \ldots = f^{q}$$

a mais alta potencia de f, que divide o segundo membro de (166), e outro tanto acontece ao primeiro membro. Logo (166) subsistirá se para todos os factores primos communs a φA^{a}, e s, tiver logar a primeira das duas condições (167).

Na segunda hypothese seja n o numero de factores s_1, s_2, s_3, etc. em que entram potencias de f iguaes ou superiores a f^{p}; e represente $f^{q'}$ o producto das mais altas potencia de f, que entram nos outros factores s_1, s_2, etc., será f^{np+q_l} a mais alta potencia divisora do segundo membro de (166); logo essa potencia é o producto da que divide o primeiro membro multiplicada por $f^{(n-1)p+q_l}$; esta expressão, como é facil de reconhecer, tem a mesma significação quando $n=0$, advertindo que então $q_l = q$.

Por consequencia se forem f, f', etc. todos os factores primos communs a φA^{a}, e s, que entram em mais de um dos numeros s_1, s_2, s_3, etc., e que satisfazem á segunda condição (167) em vez de (166) devemos escrever geralmente

$$(168) \qquad f^{(n-1)p+q_l} f'^{(n'-1)p'+q_l'} \ldots \psi_A s = \psi_A s_1 \times \psi_A s_2 \times \psi_A s_3 \ldots$$

Supponhamos agora $A=2$; será $\varphi A^{a} = 2^{a-1}$. Tambem, como no caso precedente (166), subsistirá se nenhum dos factores s_1, s_2, etc., ou um só delles fôr divisivel por 2. No caso contrario o maximo divisor commum entre φA^{a}, e s terá uma das seguintes fórmas, sendo $q > 1$; $q' => 0$.

$$(169) \qquad 2^{a-q};\ 2^{a-1};\ 2^{a+q'}.$$

Adoptando a primeira dellas, e sendo 2^{a}, 2^{b}, 2^{c} as potencias que dividem respectivamente n dos factores s_1, s_2, s_3, etc., teremos

$$\psi_A s = 2^{a-q+1};\ \psi_A s_1 \times \psi_A s_2 \times \psi_A s_3 \ldots = 2^{a+1} \cdot 2^{b+1} \cdot 2^{c+1} \ldots = 2^{a-q+n};$$

logo será

$$(170) \qquad 2^{n-1} \psi_A s = \psi_A s_1 \times \psi_A s_2 \times \psi_A s_3 \ldots$$

Adoptando a segunda fórma, e sendo ainda n o numero dos factores s_1, s_2, s_3, etc., divisiveis por 2, teremos

$$\psi_A s = 2^{\alpha - 1}; \ \psi_A s_1 \times \psi_A s_2 \times \psi_A s_3 \ldots = 2^{\alpha - 1 + n},$$

e por conseguinte

(171) $$2^n \psi_A s = \psi_A s_1 \times \psi_A s_2 \times \psi_A s_3 \ldots .$$

Finalmente adoptando a terceira fórma, e sendo n o numero dos factores s_1, s_2, s_3, etc., em que entram potencia de 2 iguaes ou superiores a $2^{\alpha - 1}$, 2^{q_1} o producto das n' potencias de 2 divisoras dos outros numeros s_1, s_2, etc. será

$$\psi_A s = 2^{\alpha - 1}; \ \psi_A s_1 \times \psi_A s_2 \times \psi_A s_3 \ldots = 2^{n(\alpha - 1) + q_1 + n'},$$

e por tanto

(172) $$2^{(n-1)(\alpha - 1) - q_1 + n'} \psi_A s = \psi s_1 \times \psi s_2 \times \psi s_3 \ldots .$$

formula que comprehende o caso de ser $n = 0$, devendo então ser $q_1 = \alpha + q'$.

Resumindo a discussão precedente, vê-se que a formula (166) só deixará de ter logar

1.º Quando para $A > 2$ houver um factor primo f de φA^α, que divida mais de um dos numeros s_1, s_2, s_3, etc., com tanto porém que a mais alta potencia de f, que divide s seja superior á que divide φA^α.

2.º Quando para $A = 2$, forem pares dois, ou mais dos factores s_1, s_2, s_3, etc.

134. Podemos em relação a B^β, C^γ, estabelecer equações analogas a (168), isto é, teremos

$$F \psi_A s = \psi_A s_1 \times \psi_A s_2 \ldots$$

$$F' \psi_B s = \psi_B s_1 \times \psi_B s_2 \ldots$$

$$F'' \psi_C s = \psi_C s_1 \times \psi_C s_2 \ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

multiplicando ordenadamente estas equações, e advertindo que em geral (§ 102)

$$\psi_A s_n \times \psi_B s_n \times \psi_C s_n \ldots = \psi s_n,$$

acharemos

$$(173) \qquad \ldots F'' F' F \psi s = \psi s_1 \times \psi s_2 \times \psi s_3 \ldots$$

que nos prova que o segundo membro desta equação é sempre divisivel por ψs.

Por conseguinte a equação (165) terá logar sempre que

$$F = F' = F'' = \cdots = 1,$$

condições que envolvem a não existencia dos casos de exclusão (§ 133, 1.º, 2.º) em relação a cada um dos numeros φA^{α}, φB^{β}, φC^{γ}, etc.

135. Ora vg. relativamente a φA^{α} a condição de exclusão (§ 133, 1.º) equivale a que não sendo s_1, s_2, s_3, etc. primos entre si, não haja entre $\frac{s}{D'}$, e D' (maximo divisor commum de s, e φA) um divisor primo, que divida dois dos factores s_1, s_2, s_3, etc. e como similhantemente se dirá a respeito de $\frac{s}{D''}$, e D'', etc. reconheceremos finalmente que (165) terá logar unicamente:

1.º Se s_1, s_2, s_3, etc. forem primos entre si.

2.º Se, sendo impares A, B, C, etc., e não se dando a condição precedente, forem $\frac{s}{D'}$, $\frac{s}{D''}$, $\frac{s}{D'''}$, etc. respectivamente primos com D', D'', D''', etc. ou simplesmente primos com estes em relação aos divisores que entram em mais de um dos factores s_1, s_2, s_3, etc.

3.º Se, sendo vg. $A = 2$, além da condição precedente não fôr par mais de um dos numeros s_1, s_2, s_3, etc.

136. Tambem se conhece facilmente que a existencia da equação (165) exige que se verifique uma equação analoga em relação a qualquer numero dos factores s_1, s_2, s_3, etc., isto é, vg.

$$\psi s_1 \times \psi s_2 \times \psi s_3 = \psi s_1 s_2 s_3;$$

pois que se fosse necessario para tornar verdadeira esta equação multiplicar o segundo membro por $F_i > 1$, (165) sómente seria verdadeira multiplicando pelo menos por F_i o seu primeiro membro.

137. Quando nos fôr dada a expressão

$$(171) \qquad \sqrt[s]{\sqrt[s]{\sqrt[s]{\ldots c}}},$$

que suppomos possivel, deve entender-se que em cada uma das extracções $\sqrt[s_n]{\ }$ se deve adoptar qualquer dos ψs_n valores, que lhe correspondem. Nessas hypotheses a expressão dada terá um numero de valores designado por

$$\psi s_1 \times \psi s_2 \times \psi s_3 \ldots,$$

os quaes serão todos incongruos; por quanto suppondo que até inclusivamente á extracção $\sqrt[s_n]{\ }$ se obtiveram valores incongruos, isto é, que

$$\sqrt[s_n]{\sqrt[s_{n+1}]{\sqrt[s_{n+2}]{\ldots c}}}$$

tem

$$\psi s_n \times \psi s_{n+1} \times \psi s_{n+2} \ldots$$

valores distinctos representados por

$$\rho_1, \rho_2, \rho_3, \text{ etc.},$$

serão tambem distinctos todos os

$$\psi s_{n-1} = \psi s_n \times \psi s_{n+1} \times \psi s_{n+2} \ldots$$

valores

$$\sqrt[s_{n-1}]{\rho_1}, \sqrt[s_{n-1}]{\rho_2}, \sqrt[s_{n-1}]{\rho_3}, \text{ etc.},$$

para o que basta provar, que um dos valores destes radicaes não póde ser congruo com um valor de outro; com effeito de

$$\sqrt[s_n - 1]{\rho_q} = \sqrt[s_n - 1]{\rho \ldots}$$

concluir-se-hia pela elevação á potencia $s_n - 1$

$$i_q = i_{q'},$$

o que é contra a hypothese

138. Supondo ainda

$$s = s_1\, s_2\, s_3 \ldots,$$

o radical modular $\sqrt[s]{c}$ poderá ser representado por

$$\sqrt[s_1]{\sqrt[s_2]{\sqrt[s_3]{\ldots c}}}, \tag{174'}$$

unicamente quando se verificar a condição (165); por quanto supondo possivel a expressão precedente, e por conseguinte possiveis todos os valores correspondentes ás extracções successivas, como (174′) elevada successivamente ás potencias s_1, s_2, s_3, etc., isto é, á potencia s, produz c, todos os valores de (174′) serão valores de $\sqrt[s]{c}$; logo (174′) daria (§ 137)

$$\psi s_1 \times \psi s_2 \times \psi s_3 \ldots$$

valores incongruos de $\sqrt[s]{c}$, e por conseguinte esse numero não póde ser maior que ψs, numero de todos os valores de $\sqrt[s]{c}$, isto é, verificar-se-ha (165).

Reciprocamente da possibilidade de $\sqrt[s]{c}$, e da existencia da condição (165) conclue-se a possibilidade de (174′); pois da congruencia

$$x^s = c, \text{ ou } x^{s_1 s_2 s_3 \ldots s_n} = c,$$

por ser (§ 136)

$$\psi s = \psi s_n \times \psi s_1\, s_2 \ldots s_{n-1},$$

conclue-se que

$$x^{s_1 s_2 \ldots s_{n-1}} = \sqrt[s_n]{c}$$

deve ter ψs_n, valores para que

$$x = \sqrt[\frac{s}{s_n}]{\sqrt[s_n]{c}}$$

possa ter ψs valores. Similhantemente se demonstra que

$$x^{s_1 s_2 \ldots s_{n-2}} = \sqrt[s_{n-1}]{\sqrt[s_n]{c}},$$

deve ter

$$\psi s_{n-1} \times s_n = \psi s_{n-1} s_n$$

valores, e assim por diante até demonstrarmos que (174') deve ter ψs valores, isto é, os correspondentes a todas as extracções successivas, que por conseguinte serão todas possiveis.

A substituição de um radical simples $\sqrt[s]{c}$ por um radical composto (174') deve pois sempre ser sujeita á condição (165).

139. Não só é indifferente a ordem das extracções successivas (174'), mas tambem decompondo s em outros factores s'_1, s'_2, s'_3, etc. de modo que seja

$$\psi s = \psi s'_1 \times \psi s'_2 \times \psi s'_3 \ldots$$

será

$$\sqrt[s_1]{\sqrt[s_2]{\sqrt[s_3]{\ldots c}}} = \sqrt[s'_1]{\sqrt[s'_2]{\sqrt[s'_3]{\ldots c}}},$$

isto é, cada um dos ψs valores do primeiro membro corresponderá a um valor do segundo.

140. Sendo $s = s_1 s_2$, e s_1 primo com $\frac{1}{2}N$, será $\psi s_1 = 1$, e o maior divisor commum entre s, e $\frac{1}{2}N$, sendo o mesmo que entre este ultimo numero e s_2, teremos sempre

$$\psi s = \psi s_1 \times \psi s_2 ; \quad \sqrt[s]{c} = \sqrt[s_1]{\sqrt[s_2]{c}}.$$

141. Nas hypotheses do § precedente, depois de obtidos os ψs_2 va

lores de $\sqrt[s_2]{c}$, para effeituar a extracção $\sqrt[s_1]{\ }$, isto é, para achar os valores de x em

$$x^{s_1} = \sqrt[s_2]{c}$$

entendendo-se que o segundo membro póde ter todos os ψs_2 valores correspondentes) deveremos (§§ 123, 124) tomar um valor qualquer t dado por

$$t = s_1^{\psi\phi s - 1} M \psi N,$$

e será

$$x = \sqrt[s]{c} = \left(\sqrt[s_2]{c}\right)^t = \sqrt[s_2]{c^t},$$

isto é, a extracção $\sqrt[s_1]{\ }$ correspondente a qualquer factor s_1 primo com ψN equivale á elevação da potencia t de todos os valores obtidos pelas extracções antecedentes, ou tambem é dada pela extracção $\sqrt[s_2]{\ }$ de c^t.

142. Se feita a decomposição

$$s = s_1 s_2 s_3 \ldots$$

sujeita á condição (165) houver entre os factores s_1, s_2, s_3, etc. alguns divisiveis por numeros primos com ψN, (165) subsistirá ainda (§ 140) separando em factores distinctos esses numeros; podemos pois suppor

$$s = s_1 s_2 s_3 \ldots s',$$

sendo s_1, s_2, s_3, ... primos com ψN, e para ter $\sqrt[s']{c}$, depois de obtidos todos os valores $\sqrt[s']{c}$, achar-se-ha successivamente (§§ 123, 124)

$$\sqrt[s_1]{\sqrt[s']{c}} = \left(\sqrt[s]{c}\right)^t = \sqrt[s]{c^t}; \quad \sqrt[s_1]{\sqrt[s_2]{\sqrt[s]{c}}} = \sqrt[s]{\left(\sqrt[s]{c}\right)^t} = \left(\sqrt[s]{c}\right)^{tt'} = \sqrt[s_2]{\sqrt[s]{c^t}} = \sqrt[s']{c^{tt'}};$$

$$\sqrt[s_1]{\sqrt[s_2]{\sqrt[s]{\cdots\sqrt[s]{c}}}} = \left(\sqrt[s]{c}\right)^{tt't''\cdots} = \sqrt[s]{c^{tt't''\cdots}};$$

sendo t, t', t'', etc. dados por

$$t \equiv s_1^{\phi\phi N-1};\ t' \equiv s_2^{\phi\phi N-1};\ t'' \equiv s_3^{\phi\phi N-1};\ \text{etc.}$$

e por conseguinte

$$tt't''\ldots \equiv (s_1 s_2 s_3 \ldots)^{\phi\phi N-1},$$

como se veria *à priori*.

143. Sendo $s = s'D$, e D o maior divisor commum entre s e ϕN, teremos (§ 124) tambem para s' não primo com ϕN, isto é, com D,

$$(175)\qquad \sqrt[s]{c} = \sqrt[s']{\sqrt[D]{{}_{,}c}} = \sqrt[D]{c^t} = \left(\sqrt[D]{c}\right)^t,$$

indicando $\sqrt[D]{{}_{,}c}$ os valores de $\sqrt[D]{c}$, que não tornam impossivel a extracção $\sqrt[s']{}$, e e sendo t dado por

$$s'tD \equiv D + u\phi N,$$

ou

$$t \equiv s^{\phi\frac{\phi N}{D}-1}\,\mathrm{M}\,\phi N,$$

advertindo que a ultima equação (175) para ser verdadeira, deve ser t primo com ϕN, o que se obtem da maneira indicada (§ 124).

Se fôr $s = s''s'D$, teremos igualmente para s'' não primos com D,

$$\sqrt[s]{c} = \sqrt[s'']{\sqrt[s']{\sqrt[D]{{}_{,}c}}} = \sqrt[s'']{\sqrt[D]{{}_{,}c^{t}}} = \sqrt[D]{c^{t''}} = \left(\sqrt[D]{c^{t}}\right)^{t'} = \left(\sqrt[D]{c}\right)^{tt'},$$

sendo tambem t' sujeito a condições analogas ás indicadas.

E geralmente para

$$s = s_1 s_2 s_3 \ldots D,$$

sendo alguns dos factores s_1, s_2, s_3, etc. ou todos elles não primos com D,

$$(176)\qquad \sqrt[s]{c} = \sqrt[D]{c^{tt't''\ldots}} = \left(\sqrt[D]{c}\right)^{tt't''\ldots}.$$

determinando-se t, t', t'', etc. similhantemente ao que temos indicado, e verificando-se a ultima equação unicamente quando t, t', t'', etc. forem primos com $¿N$, isto é, com D.

A formula (176) obter-se-hia immediatamente pelo que dissemos no principio deste §, fazendo

$$\sqrt[s]{c} = \sqrt[s_1 s_2 \ldots]{\sqrt[D]{c}},$$

e determinando T pela congruencia

$$T \equiv (s_1 s_2 s_3 \ldots)^{\phi \frac{\phi N}{D} - 1} \text{ M } ¿N, \tag{177}$$

que daria

$$\sqrt[s]{c} = \sqrt[D]{c^T} = \left(\sqrt[D]{c}\right)^T,$$

verificando-se a ultima equação unicamente quando fôr T primo com $¿N$, isto é, com D.

O valor T dado por (177) visivelmente é o producto dos valores t, t', t'', etc. acima empregados, e que são obtidos por congruencias analogas a (177), em que successivamente se substitue $s_1 s_2 s_3 \ldots$ por s_1, s_2, s_3, etc.

144. A elevação dos radicaes modulares a potencias quaesquer inteiras requer certas attenções particulares.

Em primeiro logar é evidente que

$$\left(\sqrt[s]{c}\right)^s = c;\quad \left(\sqrt[s]{c}\right)^{ss'} = c^{s'}. \tag{178}$$

Se fôr

$$¿ss' = ¿s \times ¿s', \tag{179}$$

será

$$\left(\sqrt[ss']{c}\right)^s = \left(\sqrt[s']{\sqrt[s]{c}}\right)^s = \sqrt[s']{c}. \tag{180}$$

Na mesma hypothese teremos

$$\left(\sqrt[ss']{c}\right)^{s's} = \left(\sqrt[s]{\sqrt[s]{c}}\right)^{ss} = \left(\sqrt[s]{c}\right)^{s} \tag{181}$$

Deixando porém de existir a condição (179), não serão licitas as reducções (180, 181), isto é, em vez dellas teremos, como é facil de reconhecer,

(181) $$\left(\sqrt[ss']{c}\right)^{s'} = \sqrt[s]{}_1 c:\ \left(\sqrt[ss']{c}\right)^{s\,s'} = \left(\sqrt[s]{}_1 c\right)^{s'}:$$

designando $\sqrt[s]{}_1 c$ qualquer dos valores de $\sqrt[s]{c}$, que não torna impossivel $\sqrt[s']{\sqrt[s]{c}}$.

145. Se s, s' forem primos entre si, ou mais geralmente se o maximo divisor commum s'' entre esses numeros fôr primo com ψN, isto é, se tivermos $\psi s'' = 1$, será

(182) $$\left(\sqrt[s]{c}\right)^{s'} = \sqrt[s]{c^{s'}}$$

Em primeiro logar demonstra-se facilmente, que cada um dos valores do primeiro membro é dado por um dos valores do segundo, por quanto qualquer daquelles valores satisfaz a congruencia

$$x^s \equiv c^s \text{ M } N,$$

a qual por conseguinte é possivel, como tambem se vê do (§ 128); e todas as raizes d'esta são dadas pelo segundo membro de (182).

Em segundo logar, como o segundo membro de (182) tem ψs valores distinctos, a demonstração dessa formula reduz-se agora a provar que os ψs valores do primeiro membro são todos incongruos para o modulo N. Ora se fosse, vg.

(183) $$\left(\sqrt[s]{}_1 c\right)^{s'} \equiv \left(\sqrt[s]{}_2 c\right)^{s'},$$

como $\sqrt[s]{}_1 c$, $\sqrt[s]{}_2 c$ são primos com N, podemos achar

(184) $$z \equiv \frac{\sqrt[s]{}_1 c \text{ M } N}{\sqrt[s]{}_2 c}, \text{ ou } z \equiv \frac{\sqrt[s]{}_1 c}{\sqrt[s]{}_2 c},$$

o que muda (183) em

$$z^{s'} \equiv 1:$$

mas de (184) deduz-se

$$z^s \equiv 1,$$

e como s, s' só pódem ter o maior divisor commum s'', que dá $\psi s''=1$, teriamos

$$z^{s''}=1,\quad z=1,$$

e por conseguinte

$$\sqrt[s]{}_1 c=\sqrt[s]{}_2 c,$$

contra a hypothese.

Se não fosse $\psi s''=1$, a formula (182) deixaria de ser verdadeira, pois que o segundo membro teria ψs valores differentes, ao passo que os ψs valores do primeiro membro não seriam incongruos. Com effeito, a congruencia (183) subsistiria, tomando

$$\sqrt[s]{}_1 c=\sqrt[s]{}_2 c\times\sqrt[s']{1},$$

o que sempre é possivel, pois todos os valores $\sqrt[s'']{1}$ são valores $\sqrt[s]{1}$; e por isso $\sqrt[s]{}_1 c$, $\sqrt[s]{}_2 c$ seriam dois valores incongruos de $\sqrt[s]{c}$, uma vez que se adoptasse um valor de $\sqrt[s'']{1}$ differente de 1.

146. A multiplicação de radicaes modulares do mesmo grau é dada pela formula

(185) $$\sqrt[s]{c_1}\times\sqrt[s]{c_2}=\sqrt[s]{c_1 c_2}.$$

Com effeito qualquer valor

$$\sqrt[s]{}_m c_1\times\sqrt[s]{}_n c_2$$

do primeiro membro satisfaz a congruencia

$$x^s\equiv c_1 c_2,$$

a qual por conseguinte é possivel, como tambem se via (§ 128); e como todas as ψs raizes desta são dadas pelo segundo membro de (185), a exactidão desta formula demonstra-se uma vez que se reconheça, que o seu primeiro membro não tem menos de ψs valores; ora effectivamente os ψs numeros incongruos

$$\sqrt[s]{}_1 c_1, \quad \sqrt[s]{}_2 c_1, \quad \sqrt[s]{}_3 c_1, \ \ldots \ \sqrt[s]{}_{\psi s} c_1$$

multiplicados vg. por $\sqrt[s]{}_m c_2$ dão ψs productos incongruos.

Se $c_1 = c_2 = c$ não podemos fazer geralmente

$$\sqrt[s]{c} \cdot \sqrt[s]{c} = \left(\sqrt[s]{c}\right)^2,$$

pois que os valores do primeiro membro são dados pela serie

$$\sqrt[s]{}_1 c^2, \quad \sqrt[s]{}_2 c^2, \quad \sqrt[s]{}_3 c^2, \text{ etc.},$$

e os do segundo membro pela serie

$$\left(\sqrt[s]{}_1 c\right)^2, \ \left(\sqrt[s]{}_2 c\right)^2, \ \left(\sqrt[s]{}_3 c\right)^s, \text{ etc.}$$

Se porém s fôr impar, e só neste caso teremos (§ 145)

$$\sqrt[s]{c} \times \sqrt[s]{c} = \sqrt[s]{c^2} = \left(\sqrt[s]{c}\right)^2$$

Uma reflexão analoga se deve fazer em relação aos radicaes algebricos multiplos.

147. De (185) conclue-se

$$(186) \qquad \sqrt[s]{c_1} \times \sqrt[s]{c_2} \times \sqrt[s]{c_3} \ldots = \sqrt[s]{c_1 c_2 c_3 \ldots}$$

Se $c_1 = c_2 = c_3 \ldots = c$, a formula precedente dá, sendo n o numero dos factores

$$\sqrt[s]{c} \times \sqrt[s]{c} \times \sqrt[s]{c} \ldots = \sqrt[s]{c^n},$$

e sómente (§ 145) quando o maximo divisor commum d entre s, e n der $\psi d = 1$, poderemos escrever

$$\sqrt[s]{c} \times \sqrt[s]{c} \times \sqrt[s]{c} \ldots = \left(\sqrt[s]{c}\right)^n.$$

148. Os valores de $\sqrt[s]{c_1}\times\sqrt[s]{c_2}$ sendo dados pela serie

$$\sqrt[s]{_m c_1}\times\sqrt[s]{_1 c_2},\ \sqrt[s]{_m c_1}\times\sqrt[s]{_2 c_2},\ \sqrt[s]{_m c_1}\times\sqrt[s]{_3 c_2},\ \text{etc.}$$

isto é, sendo

$$\sqrt[s]{c_1 c_2}=\sqrt[s]{_m c_1}\times\sqrt[s]{c_2},$$

se tivermos um valor a de $\sqrt[s]{c_1}$, isto é, se fôr $c_1\equiv a^s$, teremos

$$(187)\qquad \sqrt[s]{c_1 c_2}=\sqrt[s]{a^s c_2}=\sqrt[s]{_m a^s}\times\sqrt[s]{c_2}=a\sqrt[s]{c_2}.$$

149. O quociente dos dois radicaes do mesmo grau é dado pela formula

$$(188)\qquad \frac{\sqrt[s]{c_1}}{\sqrt[s]{c_2}}=\sqrt[s]{\frac{c_1}{c_2}},$$

em que o primeiro membro representa qualquer dos valores de x dados pela congruencia

$$x\sqrt[s]{c_2}\equiv\sqrt[s]{c_1},$$

e sendo no segundo membro $\frac{c_1}{c_2}$ qualquer dos valores x dados por

$$x\cdot c_2\equiv c_1.$$

A verdade da formula (188) reconhece-se advertindo, que qualquer valor do primeiro membro satisfaz á congruencia

$$x^s\equiv\frac{c_1}{c_2};$$

a qual por conseguinte é possivel, como tambem se conclue do § 129: e como esse membro tem pelo menos $\frac{1}{2}s$ valores $\frac{\sqrt[s]{c_1}}{\sqrt[s]{_m c_2}}$, que é o numero de raizes da ultima congruencia, segue-se que todos os valores do primeiro membro de (188) são dados por todas as raizes da ultima congruencia, isto é, são representados pela expressão $\sqrt[s]{\frac{c_1}{c_2}}$.

150. Indaguemos quando dois radicaes modulares $\sqrt[s]{c}$, $\sqrt[s']{c'}$ terão o mesmo numero de valores, o que equivale a haver igual numero de raizes nas congruencias correspondentes.

A propriedade supposta

$$(189) \qquad \psi s = \psi s',$$

muda-se, chamando D, D' os maximos divisores communs entre s, e ψN, e entre s', e ψN, em

$$(190) \qquad \psi D = \psi D'.$$

Desta equação concluir-se-ha necessariamente a igualdade de D, e D'. Porque, em primeiro logar supposdo A, B, C, etc. impares, qualquer divisor primo vg. de D divide ψD, e reciprocamente (§ 106); e por isso D, D' devem ter os mesmos divisores primos; supponhamos que são f, f', f'', etc. esses factores primos communs; a equação precedente equivale (§ 135) a

$$(191) \qquad \psi f^m \times \psi f'^n \times \psi f''^p \ldots = \psi f^{m'} \times \psi f'^{n'} \times \psi f''^{p'} \ldots;$$

e como em ψf^m, $\psi f'^n$, etc. só entram respectivamente f, f', etc., de (191) concluir-se-ha

$$(192) \qquad \psi f^m = \psi f^{m'}; \quad \psi f'^n = \psi f'^{n'}; \quad \psi f''^p = \psi f''^{p'}; \text{ etc.}$$

Estejam dispostas por ordem decrescente as maximas potencias

$$f^\mu,\ f^{\mu'},\ f^{\mu''},\ \text{etc.}$$

respectivamente divisoras de

$$\psi A^\alpha,\ \psi B^\beta,\ \psi C^\gamma,\ \text{etc.}$$

será vg. para a primeira das equações (192)

$$(193)\qquad \begin{cases} \psi f^{m} = \psi_A f^{m} \times \psi_B f^{m} \times \psi_C f^{m} \ldots = f^{\genfrac{}{}{0pt}{}{m}{u}} f^{\genfrac{}{}{0pt}{}{m}{u'}} f^{\genfrac{}{}{0pt}{}{m}{u''}} \ldots ; \\[2ex] \psi f^{m'} = \psi_A f^{m'} \times \psi_B f^{m'} \times \psi_C f^{m'} \ldots = f^{\genfrac{}{}{0pt}{}{m'}{u}} f^{\genfrac{}{}{0pt}{}{m'}{u'}} f^{\genfrac{}{}{0pt}{}{m'}{u''}} \ldots ; \end{cases}$$

entendendo-se que nos expoentes ambiguos dos ultimos membros destas equações deve adoptar-se o numero superior quando não é maior, que o inferior, e adoptar-se-ha este no caso contrario.

Supponhamos por um momento, que apezar de verificada a primeira das equações (192) é $f^m > f^{m'}$, ou $m > m'$; como é sempre $m =< u$, e por conseguinte $m' < u$, infere-se destas condições

$$f^{\genfrac{}{}{0pt}{}{m}{u}} = f^{m} > f^{m'} = f^{\genfrac{}{}{0pt}{}{m'}{u}}.$$

Proseguindo nos factores seguintes a $f^{\genfrac{}{}{0pt}{}{m}{u}}$, $f^{\genfrac{}{}{0pt}{}{m'}{u}}$, reconhece-se que em quanto não fôr indispensavel na equação superior adoptar o numero inferior do expoente ambiguo, isto é, em quanto $m =< u_{,}$, será na linha inferior $m' < u_{,}$, e os factores superiores f^m serão maiores que os inferiores $f^{m'}$. E logo que na linha superior tivermos $m > u_{,}$, será na linha inferior $m' =< u_{,}$: na primeira hypothese

$$f^{\genfrac{}{}{0pt}{}{m}{u_{,}}} = f^{u_{,}} = f^{\genfrac{}{}{0pt}{}{m'}{u_{,}}},$$

e na segunda

$$f^{\genfrac{}{}{0pt}{}{m}{u_{,}}} = f^{u_{,}} > f^{m'} = f^{\genfrac{}{}{0pt}{}{m'}{u_{,}}}.$$

Logo finalmente nos ultimos membros de (193) os factores do membro superior são iguaes, ou maiores que os da linha inferior, sendo sempre o primeiro dos superiores maior, que o primeiro dos inferiores: segue-se pois que para

$$m > m', \text{ é } \psi f^{m} > \psi f^{m'}:$$

e como a segunda desigualdade não se verifica (192), tambem não existe a primeira. Applicando a mesma demonstração a todos os outros factores, achar se-ha por tanto

$$f^m = f^{m'};\ f'^n = f'^{n'};\ f''^p = f''^{p'}:\ \text{etc.}$$

e por conseguinte

$$f^m f'^n f''^p \ldots = D = f^{m'} f'^{n'} f''^{p'} \ldots = D'.$$

Supponhamos agora que é vg. $A = 2$. A maneira como de D se forma ψD nos indicará, que esses dois numeros são simultaneamente pares, ou impares; e tambem se reconhecerá, como no caso precedente, que qualquer outro factor primo de D sel-o-ha de ψD, e reciprocamente: logo D, D' devem ter ainda os mesmos divisores primos, o que nos conduz ás equações (191), e destas a (192). Se D, D' forem impares a demonstração do caso precedente, é applicavel actualmente, pois não ha a considerar a hypothese de ser

$$\psi_A f^m = 2 f^{\overset{m}{u_1}}.$$

Se $f = 2$, serão impares f', f'', etc., e teremos, pelo que fica demonstrado,

$$(194)\qquad f'^n = f'^{n'};\ f''^p = f''^{p'};\ \text{etc.}$$

Suppondo então em (193) u', u'', etc. dispostos em ordem decrescente de grandeza, aquellas equações subsistirão duplicando em alguns casos um dos ultimos membros, ou ambos elles: e, considerando os factores do membro superior, e do inferior seguintes aos primeiros, se $m > m'$, e $m =< u'$, provaremos como precedentemente que

$$(195)\qquad f^{\overset{m}{u'}} f^{\overset{m}{u''}} \ldots > f^{\overset{m'}{u'}} f^{\overset{m'}{u''}} \ldots :$$

e se $m > u'$, concluiremos pelos mesmos principios

$$(195')\qquad f^{\overset{m}{u'}} f^{\overset{m}{u''}} \ldots => f^{\overset{m'}{u'}} f^{\overset{m'}{u''}} \ldots$$

Para compararmos agora os primeiros factores $\varphi_A f^m$, $\varphi_A f^{m'}$, supporemos primeiro $u = o$. Será $m =< u'$, verificar-se-ha (195), e teremos

$$\psi_A f^m = 1;\ \psi_A f^{m'} = 1;\ \psi f^m > \psi f^{m'}.$$

Sendo porém

$$u > 0, \text{ e } m = > u = \alpha - 1$$

será $m = < u'$, verificar-se-ha (195), e teremos

$$\psi_d f^m = f^{\alpha - 1};\ \psi_d f^{m'} = < f^{\alpha - 1};\ \psi f^m > \psi f^{m'}.$$

Finalmente sendo

$$u > 0, \text{ e } m < u = \alpha - 1,$$

será $m = u'$, verificar-se-ha (195), e como se suppõe m, e $m' > 0$, teremos

$$\psi_d f^m = 2 f^m > 2 f^{m'} = \psi_d f^{m'}:\ \psi f^m > \psi f^{m'}.$$

A ultima desigualdade terá pois logar em todos os casos, sempre que se suppozer $m > m'$; e como a dita desigualdade não é permittida (192), conclue-se que são inadmissiveis as desigualdades

$$m > < m',\ n > < n', \text{ etc.}$$

e será necessariamente sempre

$$f^m f'^n f''^p \ldots = f^{m'} f'^{n'} f''^{p'} \ldots, \text{ ou } D = D'.$$

151. Para que dois radicaes $\sqrt[s]{c}$, $\sqrt[s']{c'}$ sejam equivalentes é necessario em primeiro logar, que tenham o mesmo numero de valores, isto é, que o maximo divisor commum D entre s e $\dot{c}N$, seja o mesmo que entre s' e $\dot{c}N$. Nessa hypothese determinando os valores de t, t', que satisfazem ás equações

(196) $$\begin{cases} s t = D + u \dot{c} N: \\ s' t = D + u' \dot{c} N; \end{cases}$$

será

$$\sqrt[s]{c} = \sqrt[D]{c^t};\ \sqrt[s']{c'} = \sqrt[D]{c'^{t'}}:$$

e como de

$$\sqrt[D]{c^t} = \sqrt[D]{c'^{t'}}$$

se deduz

$$c^t \equiv c'^{t'} \tag{197}$$

esta congruencia e a equação $\psi s = \psi s'$, serão as condições necessarias, e sufficientes para a equivalencia dos radicaes dados.

Em virtude de (196) póde substituir-se (197) por

$$c^{\left(\frac{s}{D}\right)^{\phi \frac{\phi N}{D} - 1}} \equiv c'^{\left(\frac{s'}{D}\right)^{\phi \frac{\phi N}{D} - 1}}. \tag{198}$$

152. Para que os radicaes modulares

$$\sqrt[s]{c}, \quad \sqrt[s']{c'} \quad \sqrt[s'']{c''}, \text{ etc.}$$

se possam substituir por outros equivalentes, referidos todos ao mesmo grau, é necessario e sufficiente que

$$\psi s = \psi s' = \psi s'' = \ldots$$

determinando pois nessa hypothese os numeros t, t' t'', etc. que satisfazem ás equações

$$t s = D + u \delta N:$$

$$t' s' = D + u' \delta N:$$

$$t'' s'' = D + u'' \delta N:$$

$$\ldots\ldots\ldots\ldots\ldots.$$

os radicaes dados poderão ser substituidos por

$$\sqrt[D]{c^t}, \quad \sqrt[D]{c'^{t'}}, \quad \sqrt[D]{c''^{t''}}, \text{ etc.}$$

153. Procuremos agora quando os radicaes $\sqrt[s]{c}$, $\sqrt[s]{c'}$ podem ter valores communs, e, na dita hypothese, determinemos esses valores.

Supponhamos primeiro que os radicaes dados tem um valor commum ρ; será

$$\sqrt[s]{c} = \rho \sqrt[s]{1}: \quad \sqrt[s']{c'} = \rho \sqrt[s']{1}:$$

logo todos os valores communs serão dados pelas equivalencias precedentes tomando nellas os valores communs de $\sqrt[s]{1}$, $\sqrt[s']{1}$, isto é, suppondo d o maximo divisor commum entre s, s' será ψd o numero de valores communs dos radicaes dados, ou de outro modo o numero de raizes communs ás congruencias

$$(199) \qquad x^s \equiv c, \quad x^{s'} \equiv c'.$$

A condição necessaria para que os dois radicaes dados tenham ψd valores communs deduz-se facilmente das congruencias precedentes; porquanto elevando a primeira á potencia $\frac{s'}{d}$, e a segunda á potencia $\frac{s}{d}$ acharemos

$$(200) \qquad c^{\frac{s'}{d}} \equiv c'^{\frac{s}{d}},$$

condição, que, como depois veremos, é tambem sufficiente para a existencia daquelles valores communs.

Havendo esses valores communs e querendo determinal-os, tomaremos dois numeros positivos u, v que satisfaçam a

$$(201) \qquad su - s'v = d,$$

equação possivel; deduziremos de (199)

$$x^{su} \equiv c^u; \quad x^{s'v} \equiv c'^v$$

donde

$$(202) \qquad x^{su - s'v} \equiv x^d \equiv \frac{c^u}{c'^v},$$

congruencia possivel, na hypothese de terem raizes communs as congruencias (199). Os valores communs aos radicaes dados serão todas as raizes da ultima congruencia; com effeito, elevando-a successivamente ás potencias $\frac{s}{d}$, $\frac{s'}{d}$, acharemos, em virtude da condição (200), e da hypothese (201)

$$(203)\quad \begin{cases} x^s \equiv \dfrac{c^{u\frac{s}{d}}}{c^{v\frac{s}{d}}} \equiv \dfrac{c^{u\frac{s}{d}}}{c'^{v\frac{s'}{d}}} \equiv c^{u\frac{s}{d} - v\frac{s'}{d}} \equiv c; \\[3ex] x^{s'} \equiv \dfrac{c^{u\frac{s'}{d}}}{c^{v\frac{s'}{d}}} \equiv \dfrac{c^{u\frac{s}{d}}}{c'^{v\frac{s'}{d}}} \equiv c'^{u\frac{s}{d} - v\frac{s'}{d}} \equiv c'. \end{cases}$$

Podiamos substituir a esta verificação um raciocinio directo mui simples para provar a proposição indicada. Com effeito os ψd valores communs dos radicaes dados devendo satisfazer a (179) serão esses todas as raizes desta, cujo numero é tambem ψd.

Reciprocamente satisfeita (200) os radicaes dados terão ψd valores communs dados pela congruencia (202) porquanto suppondo-se possiveis $\sqrt[s]{c}$, $\sqrt[s]{c'}$ sel-o-hão (§ 125) $\sqrt[d]{c^u}$, $\sqrt[d]{c'^v}$, e por conseguinte tambem $\sqrt[d]{\frac{c^u}{c'^v}}$, isto é, (202) terá ψd raizes; ora desta possibilidade de resolução, da condição (200), e da hypothese (201) deduzem-se (203); logo todas as raizes de (202) satisfazem simultaneamente ás congruencias (200).

154. Para conhecermos quando podem ter raizes communs as congruencias

$$x^s \equiv c;\quad x^{s'} \equiv 1,$$

ou quando alguns dos valores de $\sqrt[s]{c}$ podem ser dados por alguns dos valores de $\sqrt[s']{1}$, designaremos por D, D' os maximos divisores communs entre s, e ψN, e entre s', e ψN, hypotheses que darão (§ 118)

$$\sqrt[s]{c} = \sqrt[D]{c^t};\quad \sqrt[s']{1} = \sqrt[D']{1};$$

e se fôr d o maximo divisor commum entre D, e D', será (200)

$$(204) \qquad c^{t\frac{D'}{d}} \equiv 1, \quad \text{ou} \quad c^{\frac{D'}{d}\left(\frac{s}{D}\right)^{\phi\frac{\phi N}{D}-1}} \equiv 1,$$

condição necessaria e sufficiente para que os radicaes dados tenham valores communs. Determinando pois u de modo que

$$(205) \qquad \frac{D}{d}u - \frac{D'}{d}v = 1,$$

esses valores communs serão dados pelas ψd raizes de

$$(206) \qquad x^d \equiv c^{tu}$$

155. Quando fôr $\psi d = 1$, será $d = 1$, e $\sqrt[D]{c^t}$ terá um valor immediatamente determinavel, que será uma potencia de c^t. Reciprocamente se quizermos saber quando $\sqrt[D]{c^t}$ poderá ter um valor

$$x \equiv c^{tu},$$

como desta congruencia se deduzirá então

$$(207) \qquad x^D \equiv c^{tuD} \equiv c^t,$$

se fôr n o menor numero que faz

$$c^{tn} \equiv 1,$$

como se deduz de (207)

$$(c^t)^{uD-1} \equiv 1,$$

será (§ 13)

$$(208) \qquad uD - 1 = vn, \quad \text{ou} \quad uD = 1\,\mathrm{M}\,n.$$

Para que haja um valor de u, que satisfaça a ultima congruencia é necessario e sufficiente que D, n sejam primos entre si. Verificada essa condição uma raiz u da congruencia precedente dará ((207)), um valor c^{tu} que será raiz de

$$x^D \equiv c^t M N.$$

Vê-se tambem que, existindo a condição indicada, esta congruencia não póde ter senão uma raiz de c^{tu}, porquanto devendo todos os valores u satisfazer a (208), dois delles quaesquer u, u', dos quaes seja o maior o primeiro, darão

$$c^{tu} \equiv c^{t(u+qn)} \equiv c^{tu'}.$$

A determinação dos casos em que $x^D \equiv c$ tem uma raiz da fórma c^u foi primeiro feita por Gauss (obra citada § 64, e segg.) na hypothese de ser o modulo primo. Foi tambem nessa hypothese restricta que Poinsot desenvolveu em alguns pontos aquella solução. (*Réfl. sur les princ* etc. pag. 97 e segg.) O modo porém como este demonstra parte das proposições, que vimos de provar para a hypothese absolutamente geral, não nos parece simples nem directo. Julgámos que offereceria algum interesse scientifico resolver geralmente este problema, fazendo-o depender de um caracter primordial, que é a existencia de um só valor de $\sqrt[s]{c}$ representavel por uma raiz da unidade.

156. Ainda que a congruencia (206) dá os valores de $\sqrt[D]{c^t}$ communs a $\sqrt[D']{1}$, as raizes dessa congruencia não são nunca, pelo processo exposto, expressamente representadas por numeros raizes da unidade, isto é, não será nunca

$$c^{tu} \equiv 1;$$

não sendo c^t congruo com 1; porquanto tendo n a significação designada no § antecedente, seria esse numero divisor do numero u que entra em

(206); e como pela condição (204) tambem n dividiria $\frac{D'}{d}$; a equação (205) exigiria que n divisor de u, e de $\frac{D'}{d}$ fosse 1, isto é $c^1 \equiv 1$.

A esta conclusão se chegaria mais facilmente advertindo, que não é possivel que todas as raizes da primeira das congruencias

$$x^d \equiv 1, \quad x^D \equiv c^1$$

sejam raizes da segunda, pois tal não acontece em relação á raiz 1, não supposto $c^1 \equiv 1$.

157. Podemos porém demonstrar geralmente, que, mesmo prescindindo do valor 1 de $\sqrt[D']{1}$, não é possivel que todos os outros sejam valores de $\sqrt[D]{c^1}$, se não fôr $\psi D' = 2$; porquanto sendo

$$x^d \equiv c^{1u},$$

a congruencia que fornece todos os valores communs aos dois radicaes, teriamos

$$\psi d = \psi D - 1: \tag{209}$$

ora, sendo d divisor de D', como vimos (§ 135) será

$$\psi D' = q \psi d.$$

Este valor substituido em (209) dá

$$\psi d = 1, \text{ logo } \psi D' = 2.$$

A ultima equação exige que tenhamos $D' = 2$, e além disto que o modulo N seja simplesmente B^β, ou $2B^\beta$.

Fragmento.

Passemos ao que diz respeito á resolução da congruencia $x^s \equiv c$.

1. Para achar as raizes de $x^s \equiv c$, decomponha-se $s = s_1 s_2 s_3 \ldots s_n$ de modo que $\psi s = \psi s_1 \psi s_2 \ldots$, será

$$x = \sqrt[s_1]{\sqrt[s_2]{\sqrt[s_3]{\ldots c}}}$$

isto é, x será dado resolvendo successivamente as congruencias

$$x^{s_n} \equiv c;\ x^{s_{n-1}} \equiv x_1;\ x^{s_{n-2}} \equiv x_2 \ldots;\ x^{s_1} \equiv x_{n-1}\,.$$

em que cada um dos numeros $x_1\, x_2 \ldots x_{n-1}$, vg. x_m é uma qualquer das raizes da congruencia antecedente

$$x^{s_{n-(m-1)}} \equiv x_{m-1}.$$

2. Se na congruencia $x^D \equiv c$ em que D é divisor de ϕN forem D', D'', D''', etc. primos entre si, será $D = D' D'' D''' \ldots$, e $\frac{D}{D'}$ será primo com D'; $\frac{D}{D''}$ com D'', etc.; logo neste caso qualquer que seja a decomposição

$$D = d_1 d_2 d_3 \ldots d_n$$

será sempre

$$(A) \qquad x = \sqrt[D]{c} = \sqrt[d_1]{\sqrt[d_2]{\sqrt[d_3]{\ldots \sqrt[d_n]{c}}}}$$

3. Se a congruencia $x^D \equiv 1$ tiver raizes primitivas ou se forem D', D', D'', etc. primos entre si, isto é, $D = D' D'' D'''$, e por isso $\psi D = D$,

$$x = \sqrt[d_1]{\sqrt[d_2]{\ldots \sqrt[d_n]{1}}}$$

suppondo $d_1 d_2 d_3 \dots d_{n-1} = d_q$, o que muda a precedente em

$$x = \sqrt[d_q]{\sqrt[d_n]{1}}$$

se não houver em d_1 factor primo algum que não entre em d_n, a formula precedente dará todas as raizes primitivas, tomando em $\sqrt[d_n]{1}$ sómente os valores que são raizes primitivas correspondentes, os quaes designados por $\sqrt[d_n]{}'_p 1$, serão todas as raizes primitivas

$$(A') \qquad x = \sqrt[d_q]{}'\,\sqrt[d_n]{}'_p\,1$$

Com effeito procuremos a minima potencia m que dá $x^m = 1$; seja δ o maior divisor commum de d_q e m, isto é

$$d_q = d_{q'}\,\delta;\ m = m_\prime\,\delta;\ d_{q'},\ m_\prime$$

primos entre si: logo

$$x^m = \left(\sqrt[d_q]{}'\,\sqrt[d_n]{}'_p\,1\right)^m = \sqrt[d_{q'}]{}'\left(\sqrt[d_n]{}'_p\,1\right)^{m_\prime}$$

$$m_\prime = m_{\prime\prime}\, d_n,\ \text{logo}\ m = m_{\prime\prime}\,\delta\, d_n$$

mas os factores primos de $d_{q'}$ entram em d_n, logo em $m_\prime$, e por isso $d_{q'}$, e $m_\prime$ não podem ser primos senão sendo

$$d_{q'} = 1,\ \text{logo}\ d_q = \delta;\ m = m_\prime\, d_q = m_{\prime\prime}\, d_n\, d_q$$

donde o menor valor de $m = d_n\, d_q$.

Reciprocamente para que (A'), ou a serie de extracções de que aquella depende deem todas as raizes primitivas é necessario que

$$(B) \qquad d_q\, d = d_n\, d$$

se todos os divisores primos de d_q não são contidos em d_n, seja $d_q = d_{q'} d_{n'}$, contendo $d_{q'}$ todos esses excluidos teremos

$$\varphi d_q d_n = \varphi d_{q'} d_{n'} d_n = \varphi d_{q'} \varphi d_{n'} \cdot d_n = \varphi d_{q'} \times d_{n'} \varphi d_n$$

mas (B) é

$$\varphi d_q d_n = d_{q'} d_{n'} \varphi d_n, \text{ logo } d_{q'} = \varphi d_{q'}$$

ora se q' não fosse 1 seria geralmente

$$G^\alpha H^\beta L^\gamma \ldots = G^{\alpha-1} H^{\beta-1} L^{\gamma-1} \ldots (G-1)(H-1)(L-1)$$

ou

$$GHL \ldots = (G-1)(H-1)(L-1) \ldots$$

equação impossivel, logo $d_{q'} = 1$, e todos os factores primos de d_q serão contidos em d_n.

Logo finalmente é condição necessaria e sufficiente para que (A') dê todas as raizes primitivas que a decomposição $d_1 d_2 d_3 \ldots d_{n-1}$, d_n se faça de maneira que todos os factores primos contidos em $d_1 d_2 d_3 \ldots d_{n-1}$ entrem em d_n.

A representação das raizes primitivas pela formula (A') com a condição indicada é a generalisação de um theorema particular conhecido para quando o modulo N é primo, e são

$$d_1 = d_2 = d_3 \ldots = d_n = q$$

divisor primo do modulo $N-1$; então demonstra-se (V. Serret, *Algebr. Sup.)* que todas as raizes primitivas da congruencia

$$x^{q^\alpha} \equiv 1 \text{ M } N$$

são dadas pelas congruencias

$$x^q \equiv 1\,;\; x^q \equiv x_1\,;\; x^q \equiv x_2\,;\; \ldots\; x^q \equiv x_{\alpha-1}$$

tendo x_1, x_2, x_3, etc. a significação indicada acima.

X.

VARIAS APPLICAÇÕES.

(Resumo.)

§ 1

Numero de decomposições de um producto $N = A^{\alpha} B^{\beta} C^{\gamma}\ldots$ (em que é k o numero dos numeros primos A, B, C, etc.) em dois factores.

Suppondo que em todas as decomposições os dois factores tem constantemente o maximo divisor commum m, designaremos por $\psi_m N$ o respectivo numero de decomposições. Consideremos pois os seguintes casos:

1.º Sendo os dois factores primos entre si, ou $m = 1$.

O numero das decomposições é o mesmo de $N' = ABC\ldots$

Seja $P \times Q$ qualquer das decomposições de um producto de $k-1$ letras $BC\ldots$; esse dará duas decomposições para k letras, isto é, $PA.Q$, $P.QA$ por conseguinte, designando por fk o valor $\psi_1 N'$ para um producto de k letras

$$fk = 2f(k-1) = 2^2 f(k-2) = \ldots = 2^{k-1} f(k-(k-1)) = 2^{k-1} f1;$$

mas $f1 = 1$; logo

$$\psi_1 N = fk = 2^{k-1} \tag{A}$$

2.° Tendo os dois factores um só divisor primo, ou vg. $m = A^a$. Deve sempre ser $\alpha \overline{\overline{>}} 2a$, e teremos

$$\psi_{A^a} N = \psi_1 A^{\alpha - 2a} B^\beta C^\gamma \ldots ;$$

Se fôr $\alpha > 2a$, será

(B) $$\psi_{A^a} N = 2^{k-1},$$

e se $\alpha = 2a$,

(C) $$\psi_{A^a} N = 2^{k-2}.$$

3.° Tendo só dois divisores primos, ou vg. $m = A^a B^b$. Deve sempre ser $\alpha \overline{\overline{>}} 2a$, e $\beta \overline{\overline{>}} 2b$, e teremos

$$\psi_{A^a B^b} N = \psi_1 A^{\alpha - 2a} B^{\beta - 2b} C^\gamma \ldots ;$$

Se fôr $\alpha > 2a$, $\beta > 2b$, será

(D) $$\psi_{A^a B^b} N = 2^{k-1};$$

se $\alpha > 2a$, $\beta = 2b$,

(E) $$\psi_{A^a B^b} N = 2^{k-2};$$

finalmente se $\alpha = 2a$, $\beta = 2b$,

(F) $$\psi_{A^a B^b} N = 2^{k-3}.$$

4.° Tendo n divisores primos, ou vg. $m = A^a B^b C^c \ldots$ Será sempre

$$\alpha \overline{\overline{>}} 2a, \ \beta \overline{\overline{>}} 2b, \ \gamma \overline{\overline{>}} 2c, \text{ etc.}$$

e teremos

(G) $$\psi_m = 2^{k-1-s}.$$

sendo s o numero das precedentes equações-desigualdades, que se reduzem a equações.

5.° Podendo ter varios divisores primos.

Neste caso todas as decomposições classificam-se em varios grupos, a que respectivamente correspondem diversos maximos divisores p, q, r, etc., e será o numero total das decomposições

$$(H) \qquad \psi_{p, q, r, \ldots} N = \psi_p N + \psi_q N + \psi_r N + \ldots$$

Por conseguinte ter-se-ha vg. para $\varkappa > 2a$,

$$(I) \qquad \psi_{1..t} N = 2^{t-1} + 2^{t-1} = 2^t,$$

e se $\varkappa = 2a$,

$$(J) \qquad \psi_{1..t} N = 2^{t-1} + 2^{t-2} = 3 \cdot 2^{t-2}.$$

§ 2.

Theorema de Wilson generalisado por Gauss.

A demonstração deste theorema depende, como fez vêr Gauss, da determinação de quando é par ou duplamente par o numero de raizes de $x^2 \equiv 1 \text{ M } N$.

Gauss disse apenas que essa indagação requeria *certas attenções* particulares.

Poinsot desenvolvendo essa rapida indicação deu uma demonstração do theorema citado, a qual tem duas inexactidões, que lhe tiram todo o rigor; uma consiste em suppôr que não ha systemas de raizes communs ás decomposições da congruencia acima em duas

$$x - 1 \equiv 0 \text{ M } P, \quad x + 1 \equiv 0 \text{ M } Q,$$

(sendo $PQ = N$): a outra existe em admittir que quando N fôr só *parmente par*, tambem 2^{t-1} designa o numero de decomposições em dois factores sem outro divisor commum além do numero 2.

Imitando o processo de Poinsot poderemos substituir a sua demonstração do seguinte modo.

Sejam a, b, c, etc. todos os numeros menores que N e primos com elle. Tomando um delles r acha-se outro s e só um tal que

$$rs \equiv 1 \text{ M } N$$

do mesmo modo *associaremos* todos os outros, podendo acontecer que para alguns delles x tenhamos

$$(K) \qquad x^2 \equiv 1.$$

Todas as congruencias analogas a estas multiplicadas pelo quadrado daquellas em que r, s são differentes dão

$$(abcd\ldots)^2 \equiv 1,$$

ou

$$(L) \qquad (abcd\ldots + 1)(abcd\ldots - 1) \equiv 0.$$

Indaguemos agora quaes são os valores x que satisfazem a (K) equivalente a

$$(M) \qquad (x-1)(x+1) \equiv 0.$$

1. Para qualquer valor possivel de x, seja D o maior divisor commum entre $x-1$ e $N = DE$; será $x+1$ divisivel por E. Logo qualquer valor real de x torna um dos dois binomios $x-1$, $x+1$ divisivel por um factor de N, e o outro binomio divisivel pelo outro factor de N.

2. Reciprocamente se tivermos, sendo $N = PQ$,

$$(N) \qquad x - 1 \equiv 0 \text{ M } P \quad x + 1 \equiv 0 \text{ M } Q$$

o valor x que satisfaz a estas equações resolve

$$mP + 2 = m'Q.$$

Logo todas as soluções (K) são dadas por todas as soluções (N) em que N se decompõe de todas as maneiras em dois factores. Como de (N) se conclue

$$mP + 2 = m'Q$$

segue-se que para ter todas as soluções x, devem-se formar só os systemas (N) que resultam da decomposição P, Q tal que P, Q sejam entre si primos, ou quando muito tenham 2 por maximo divisor commum.

Ha pois tantos systemas (N) quanto é o dobro $2\psi_{1,2}N$ do numero dessas decomposições, visto que a decomposição $P\cdot Q$ além do systema (N) dá tambem

$$(O) \qquad x - 1 \equiv 0 \,\mathrm{M}\, Q;\ \ x + 1 \equiv 0 \,\mathrm{M}\, P.$$

É facil de vêr que a cada solução x' de (N) corresponde uma solução $x'' = PQ - x'$ em (O) e será

$$(P) \qquad x'x'' \equiv (PQ - x')x' \equiv -1,$$

advertindo que nunca será $x' = x''$: logo todas as soluções x repartem-se em grupos x', x'' que satisfazem a (P), pois que não podia outra solução x''' differente de x', x'' dar

$$x'x''' \equiv -1.$$

Se o numero dos grupos fôr par temos

$$x'x''\cdot x'''x''''\ldots \equiv 1$$

e se impar

$$x'x''\cdot x'''x^{IV}\ldots \equiv -1,$$

e como as outras raizes a, b, c satisfazem a uma congruencia similhante á primeira das duas ultimas, segue-se que será sempre

$$abcd\ldots \equiv \pm 1,$$

conforme fôr par ou impar o numero dos grupos x.

Se N fôr impar, cada systema (N) dará uma só resolução x, porque sendo P, Q primos entre si, tira-se de (N)

$$x \equiv r + m\cdot PQ.$$

concluir-se-ha que

$$abcd\ldots \equiv -1,$$

se $N = 2p^{\varepsilon'}$, e

$$abcd\ldots \equiv 1,$$

se $N = 2p^{\varepsilon'}q^{\eta'}\ldots$

Consideremos finalmente o caso em que N é divisivel por 4, ou $N = 4P_1Q_1$.

Todos os systemas (N) serão os que resultam de decompôr N em dois factores primos entre si, ou em dois factores $2P$, $2Q$ sendo P, Q primos entre si.

Ora cada systema

$$(R) \qquad x-1 \equiv 0 \,\mathrm{M}\, 2P \quad x+1 \equiv 0 \,\mathrm{M}\, 2Q,$$

dá duas soluções $< 4PQ$ contidas na congruencia

$$x \equiv r + 2PQ \cdot m,$$

mas qualquer dellas é contida nos systemas (N) em que N se decompoz em dois factores primos entre si; porquanto sendo x' uma dessas soluções $x'-1$, ou $x'+1$ necessariamente é divisivel por 4 visto que ambos pares; se fôr vg. divisivel por 4 o primeiro binomio, o systema

$$x'-1 \equiv 0 \,\mathrm{M}\, 2P \quad x'+1 \equiv 0 \,\mathrm{M}\, 2Q$$

equivale a

$$x'-1 \equiv 0 \,\mathrm{M}\, 4P \quad x'+1 \equiv 0 \,\mathrm{M}\, Q$$

que tem uma só solução.

Logo todas as soluções x são dadas por todos os systemas (N) em que N se decompõe em dois factores primos entre si, isto é, o numero de grupos binarios x será $\psi_1 N$, numero daquellas decomposições, por isso se fôr $N = 2^{\alpha}$, $\psi_1 N = 1$, e se N contiver outro, ou outros factores primos como é então $k > 1$, será $\psi_1 N = 2^{k-1}$ par, e por conseguinte

$$abcd\ldots \equiv 1 \,\mathrm{M}\, N.$$

Resumindo teremos que na congruencia

$$abcd\ldots \equiv \pm 1 \,\mathrm{M}\, N$$

deve tomar-se o signal — nos seguintes casos:

1.° Quando N contiver um só factor primo.

2.° Quando $N = 2R$, sendo R impar e contendo R um só divisor primo.

Tomar-se-ha o signal + naquella congruencia em todos os outros casos.

Os casos em que temos

$$abcd\ldots + 1 \equiv 0 \text{ M } N$$

enunciam-se mais simplesmente assim:

A congruencia precedente tem logar quando N só tem um divisor primo, ou é o dobro de um numero dessa especie.

Nos outros casos

$$abcd\ldots - 1 \equiv 0$$

Mas dispensando o longo processo precedente, o theorema demonstrado na Memoria (§ 87) dá immediatamente o numero de raizes de

$$x^2 \equiv 1 \text{ M } N,$$

e por conseguinte a demonstração do theorema de Wilson generalisado.

§ 3.

Demonstração da formula de Binet (*Comptes rendus*, etc. Tom. XXXII, n.° 26) para a somma das potencias m dos numeros menores que N e primos com elle.

O nosso theorema (13) foi achado antes de vêrmos a formula citada de Binet, de que aquelle theorema é um caso particular. A nossa formula (9) dará a de Binet, imitando o processo que seguimos para obter (13), isto é, substituindo successivamente em (9) pelos differentes symbolos s_a, s_b, etc. as sommas correspondentes das potencias dos numeros naturaes expressas por meio dos numeros bernouillianos B_1, B_2, B_3, etc.

Qualquer dessas sommas vg.

$$1^m + 2^m + 3^m + \ldots a^m$$

é dada pela serie

$$\frac{(a+1)^{m+1}-1}{m+1} - ((a+1)^m - 1)\, B_1 + m\,((a+1)^{m-1} - 1)\, B_2$$

$$+ m\,\frac{m-1}{2}\,\frac{m-2}{3}\,((a+1)^{m-3} - 1)\, B_4 + \text{etc.}$$

ou pela melhor formula

$$\frac{a^{m+1}}{m+1} + a^m B_1 + m\,a^{m-1} B_2 + m\,\frac{m-1}{2}\,\frac{m-2}{3}\,a^{m-3} B_4 + \text{etc.}$$

na qual se deve supprimir o termo affecto de a^{m-m}, por isso que na serie de que resulta a precedente é $x^x = 1$ para $x = 0$. (Vid. Kramp, *Elém. de Arithm. univers.* §§ 597, 598.)

§ 4.

Applicação dos principios contidos na Memoria a dizima periodica (numero de casas de cada periodo, etc.)

§ 5.

Applicação ás fracções continuas.

FIM.

INDICE.

ERRATAS.

PAG	LIN.	ERROS	EMENDAS
15	17	$a^{\varphi p} \equiv \text{M} p$	$a^{\varphi p} \equiv 1\,\text{M} p$
27	6	$\pm x = - q' z +$	$\pm x = \mp q' z +$
37	13	$[4 - {}_s]$	$[1 - {}_s]$
38	12	$y_i^B,\ y_i'^B$	$y_i^B y_i'^B$
40	6	$q^\alpha r^\beta s\ \ldots$	$q^\alpha r^\beta s^\gamma \ldots$
48	17	$a'^C m^{2BC(n-1)}$	$q'^C m'^{2BC(n'-1)}$
66	5	em p	em que p
125	4	§ 118	§ 122
126	1	$\frac{\varphi N}{D}$	$\frac{\phi N}{D}$
»	2	D'	D
»	12	apresenta	representa
127	2	$(x_i^{\prime_i})$	$(x_i^{\prime_i})^{\prime}$
128	2	$\sqrt[i']{\sqrt[i']{c}}$	$\sqrt[i_i]{\sqrt[i']{c}}$
»	4	$x^{\prime\prime} \equiv$	$x^{\prime_i} \equiv$
»	7	$s \equiv s_1\, s_2\, s_3 \ldots$	$s = s_1\, s_2\, s_3 \ldots$
129	9	$f^{q'}$	f^{q_i}
»	19	$q_i f^{q'\,n-1\,r'}$	$q_i f^{q'(n-1)r'}$
130	7	potencia	potencias
131	16	(615)	(165)
134	6	$\psi s_{n-1} \times s_n$	$\psi s_{n-1} \times \psi s_n$

PAG.	LIN	ERROS	EMENDAS
134	17	$\sqrt[s_1]{\ }\sqrt[s'_2]{\ }\sqrt[s'_3]{\ }$	$\sqrt[s'_1]{\ }\sqrt[s'_2]{\ }\sqrt[s'_3]{\ }$
135	11	da potencia	á potencia
140	10	$\left(\sqrt[s]{\ }_5\, c\right)^s$	$\left(\sqrt[s]{\ }_3\, c\right)^2$
141	14	$x \cdot c_2 = c_1$	$x \cdot c_2 \equiv c_1$
148	2	$\dfrac{c^{u\frac{t}{d}}}{c'^{\,v\frac{t'}{d}}}$	$\dfrac{c^{u\frac{t}{d}}}{c^{v\frac{t'}{d}}}$
»	3	$\dfrac{c^{u\frac{t}{d}}}{c'^{\,v\frac{t'}{d}}}$	$\dfrac{c'^{\,u\frac{t}{d}}}{c'^{\,v\frac{t'}{d}}}$
»	10	(§ 125)	(§ 129)
»	$\dot{2}$	(§ 118)	(§ 122)
150	10	$c^{tu} \equiv c^{t(u' + qn)}$	$c^{tu} = c^{t(u' + qn)}$
»	15	pag. 97	pag. 79
156	2	$a \overset{=}{>} 2a$	$\alpha \overset{=}{>} 2a$
157	$\dot{6}$	$x + 1 = 0 \text{ M } Q$	$x + 1 \equiv 0 \text{ M } Q$