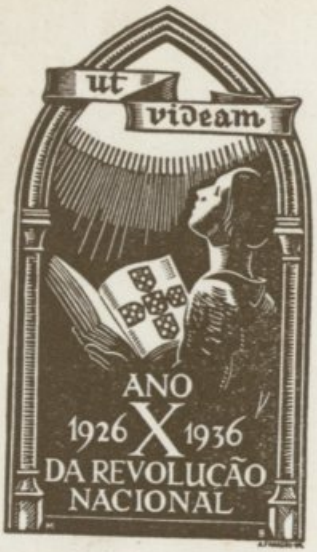

RESOLUÇÃO

DAS

EQUAÇÕES INDETERMINADAS

RESOLUÇÃO

DAS

EQUAÇÕES INDETERMINADAS

POR

FRANCISCO MIRANDA DA COSTA LOBO

COIMBRA
IMPRENSA DA UNIVERSIDADE
1885

DISSERTAÇÃO INAUGURAL

PARA O

ACTO DE CONCLUSÕES MAGNAS

NA

FACULDADE DE MATHEMATICA

DA

UNIVERSIDADE DE COIMBRA

DISSERTAÇÃO INAUGURAL

PARA O

ACTO DE CONCLUSÕES MAGNAS

NA

FACULDADE DE MATHEMATICA

DA

UNIVERSIDADE DE COIMBRA

A

SEU QUERIDO TIO

O SENHOR

GUMERSINDO MIRANDA CATALÃO

EM TESTEMUNHO DE MUITO AFFECTO E RECONHECIMENTO

O. e D.

Francisco Miranda da Costa Lobo.

PREFACIO

O problema, de que ora nos vamos occupar, tem merecido a maior attenção e interesse aos geometras mais notaveis.

E com quanto, de ha seculos, existam trabalhos importantes a este respeito, a solução do problema é ainda recente.

É para notar que ainda nos fins do seculo passado, quando os mais esclarecidos espiritos se haviam dedicado a este assumpto, pouco se tivesse adiantado sobre os resultados obtidos pelos geometras indianos, ha mil duzentos annos pelo menos.

E que estes resultados, ainda hoje pouco conhecidos na Europa, de certo o não eram na primeira metade d'este seculo.

As soluções apresentadas até Euler são de menor valia do que aquelles trabalhos antiquissimos.

Longe de nós a idêa de pretender sequer depreciar o seu valor, não só porque nos fallece a auctoridade, mas ainda porque todas manifestam a superioridade intellectual dos seus auctores.

Releve-se-nos porém uma simples observação. Nota-se uma falta importante no modo como são tractadas estas questões;

methodo ou direcção philosophica. Chasles faz este mesmo reparo quando se refere aos geometras, desde Diophantes até Euler. Seguindo as idêas de Wronski parece-nos que pode estender-se o periodo até este notabilissimo geometra.

Entre nós, pede a justiça que se diga, tambem existem de ha muito trabalhos importantes, a alguns dos quaes teremos occasião de nos referir.

D'entre os geometras europeus foi Diophantes o primeiro, que resolveu um grande numero de problemas de analyse indeterminada. D'ahi resultou chamar-se a esta analyse — *de Diophantes*. Resolveu já alguns problemas do segundo gráo a duas e mais variaveis.

Apesar de resolver as questões com muita sagacidade não apresenta systema determinado, o que é para estranhar, pois já então era conhecida no Oriente a resolução methodica das equações indeterminadas do segundo gráo.

Fermat que tractou a equação $Cx^2+1=y^2$ á qual decerto chegou partindo da equação $Cx^2 \pm A = y^2$ a que se reduzem as equações indeterminadas do segundo gráo, não indicou o seu methodo de resolução.

Brouncker, Wallis, Freniche e Ozonam resolveram a equação $Cx^2+1=y^2$, mas não se aproveitaram do resultado obtido; de modo que se deve a Euler a primeira resolução das equações indeterminadas do segundo gráo.

Este geometra resolveu um grande numero de problemas, alguns propostos por Fermat, e publicou um tractado especial sobre o assumpto.

Em seguida Lagrange occupou-se extensamente do problema, e applicou as fracções continuas á sua resolução.

Desde então têm apparecido importantes trabalhos, como os

de Legendre, Gauss, etc., e finalmente appareceu a resolução completa do problema effectuada por Wronski, em virtude do que ficou sem valor scientifico a asserção de Lagrange feita a pag. 377 das addições á algebra de Euler: «*Para resolver as equações indeterminadas de um gráo superior ao segundo só existem methodos particulares, e é de presumir que para estas equações a resolução geral seja impossivel, como o parece ser para as equações determinadas de gráo superior ao quarto.*»

Este nosso trabalho divide-se naturalmente em cinco partes.

Na primeira procurámos apresentar o mais completa e resumidamente possivel os resultados obtidos por notaveis geometras, á excepção de Wronski, e tambem os que o estudo proprio nos forneceu, para se conseguir a resolução das equações indeterminadas.

Como as equações indeterminadas estão intimamente relacionadas com as equações de congruencia, a ponto de, como veremos, deverem aquellas ser resolvidas por meio d'estas, fará objecto da segunda parte o estudo das congruencias, como são tratadas ainda ultimamente por aquelles que se occupam da sua resolução.

A terceira e quarta parte comprehendem a applicação do methodo teleologico á solução geral das congruencias e das equações indeterminadas.

Finalmente na quinta parte temos em vista a comparação das materias expostas, o que não é de grande difficuldade, attendendo aos resultados apresentados na terceira e quarta.

Em nosso estudo, conscios da nossa insufficiencia, procurámos sempre seguir as indicações de guias auctorisados.

Uma ultima explicação nos parece necessaria. Notando o ostra-

cismo, a que geralmente têm sido votados os trabalhos de Wronski, deveria exigir-se da nossa parte a maior circumspecção.

Duas razões, porém, justificam o nosso procedimento.

Em primeiro logar, parece-nos que os resultados estão obtidos com toda a exactidão, e sem darem logar a difficuldades, que poderiam apresentar-se a uma rapida observação dos trabalhos de Wronski.

Em segundo logar, se é certo que geometras de primeira ordem têm negado a estes trabalhos a importancia que elle lhes dava a ponto de os julgarem muito desfavoravelmente, tambem é verdade que hoje se repetem os estudos feitos sobre os trabalhos d'aquelle genio, tendendo a collocal-os no seu devido logar. N'este numero se contam os de Montferrier, Yvon Villarceau, West., Ch. Lagrange, etc., e entre nós, os estudos devidos ao sr. Dr. Pereira Falcão sobre a resolução das equações numericas de qualquer gráo, e outros publicados pelo sr. J. M. Rodrigues, etc.

PRIMEIRA PARTE

CONSIDERAÇÕES GERAES

1. *Objecto da analyse indeterminada.* — O problema geral da analyse indeterminada pode resumir-se do seguinte modo: — Sendo dadas equações desembaraçadas de radicaes e denominadores, em maior numero do que o das incognitas, determinar para estas os valores racionaes e inteiros mais geraes que lhes possam satisfazer.

Para que os valores achados sejam exactos, basta que verifiquem as equações dadas. Para que sejam completos, é necessario que sejam funcções pelo menos d'um numero de novas indeterminadas, egual á differença entre o numero das incognitas e o das equações a resolver.

Com effeito, as equações dadas devem ser consideradas como tendo resultado da eliminação das novas indeterminadas entre os valores das incognitas. Ora, se estes valores fossem funcções d'um numero de indeterminadas menor do que o excesso do numero de incognitas sobre o das equações, eliminando as indeterminadas, obter-se-hiam novas equações, a que teriam de satisfazer as incognitas: isto é, sujeitar-se-hiam as incognitas a condições estranhas á questão. Em conclusão: os valores achados não teriam a indeterminação que comporta o problema.

O numero das indeterminadas pode ser maior do que a differença entre o numero das incognitas e o das equações, comtanto que, effectuada a eliminação, resultem as equações dadas.

E bem se concebe que, qualquer que seja o numero das indeterminadas, estas podem estar de tal modo combinadas, que até a eliminação d'uma as faça desapparecer todas.

2. *Classificação das equações indeterminadas.* — Ha que attender ao gráo das incognitas e ao seu numero. Por isso temos em geral equações do gráo m, que se avalia do mesmo modo que nas equações determinadas, e a n variaveis.

Quando têm de considerar-se systemas de equações, reduzem-se a uma equação.

EQUAÇÕES INDETERMINADAS DO PRIMEIRO GRÁO

Resolução das equações a duas variaveis.

3. *Existe uma infinidade de systemas de raizes que ficam determinados conhecido um.* — Seja $x=\alpha$, $y=\beta$ um systema de raizes. Supponhamos á proposta, o que é possivel, a fórma $ax-by=c$, será

$$a\alpha-b\beta=c$$

e

$$ax-by=a\alpha-b\beta,$$

d'onde

$$\frac{x-\alpha}{y-\beta}=\frac{b}{a}$$

pelo que, sendo i um inteiro qualquer, deve ser

$$x=\alpha+ib \quad , \quad y=\beta+ia \ldots\ldots\ldots\ldots (1).$$

Pode sempre determinar-se i de modo que o valor absoluto de x seja inferior a $\frac{b}{2}$, e a $\frac{a}{2}$ o de y.

4. *Methodo de Bachet.* — Dada a equação

$$ax + by = c \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

é necessario, para que admitta soluções inteiras, que a e b sejam primos entre si, supprimidos os factores communs.

Fazendo

$$x = cx_1 \quad , \quad y = cy_1$$

a equação reduz-se a

$$ax_1 + by_1 = 1$$

e basta achar as raizes d'esta para termos as da proposta. O methodo que emprega Bachet é o do maior divisor commum.

5. *Methodo de Euler.* — Supponhamos á equação a forma $ax - by = c$. É

$$x = \frac{c + by}{a} = b_1 y + z$$

sendo

$$z = \frac{(b - ma)\, y + c}{a}$$

e por isso

$$az = (b - ma)\, y + c = dy + c.$$

Mas $b - ma < a$, logo

$$y = \frac{az - c}{d} = b_2 z + \frac{ez - c}{d};$$

far-se-hia em seguida $\frac{ez - c}{d} = t$, e assim successivamente até que os denominadores se reduzam á unidade. O resto da resolução é evidente.

6. *Methodo de Lagrange.* — 1.° Attendendo ao que vimos no n.° 3, Lagrange indica um methodo de tentativas, que consiste em determinar d'esse modo o systema de raizes comprehendidas entre $-\frac{b}{2}$, $+\frac{b}{2}$ e $-\frac{a}{2}$, $+\frac{a}{2}$. Os outros systemas seriam dados pelas formulas (1).

2.° Funda-se na applicação das fracções continuas.

Supponhamos como sempre é possivel $a>b$: $\frac{a}{b}$ é uma fracção irreductivel, de que a geração por meio das fracções continuas terá a forma

$$\alpha_1+\cfrac{1}{\alpha_2+\cfrac{1}{\alpha_3+\cfrac{1}{\ddots\cfrac{1}{\alpha_\mu}}}}$$

Por meio dos quocientes successivos podemos formar as duas series de mediadores

$$\begin{aligned} P_1 &= \alpha_1, & Q_1 &= 1 \\ P_2 &= \alpha_2 P_1 + 1, & Q_2 &= \alpha_2 Q_1 \\ P_3 &= \alpha_3 P_2 + P_1, & Q_3 &= \alpha_3 Q_2 + Q_1 \\ &\cdots\cdots\cdots\cdots & &\cdots\cdots\cdots\cdots\cdots \\ P_\mu &= \alpha_\mu P_{\mu-1} + P_{\mu-2}, & Q_\mu &= \alpha_\mu Q_{\mu-1} + Q_{\mu-2} \end{aligned}$$

As fracções principaes que dão os valores approximados de $\frac{a}{b}$ são

$$\frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \ldots, \frac{P_{\mu-1}}{Q_{\mu-1}}, \frac{P_\mu}{Q_\mu}$$

sendo $$\frac{P_\mu}{Q_\mu}=\frac{a}{b}.$$

Mas a differença entre duas fracções consecutivas é $(-1)^{\mu}$, logo

$$a\,Q_{\mu-1} - b\,P_{\mu-1} = (-1)^{\mu},$$

ou para $\mu = 2n$

$$a\,(c\,Q_{\mu-1}) - b\,(c\,P_{\mu-1}) = c,$$

portanto os valores $cQ_{\mu-1}$, $cP_{\mu-1}$ constituem um systema de raizes da equação $ax - by = c$, e assim temos

$$\alpha = c\,Q_{\mu-1} \quad \text{e} \quad \beta = c\,P_{\mu-1}.$$

Por isso as formulas comprehendendo os dois casos de β par ou impar, são

$$x = \pm c\,Q_{\mu-1} + ib \quad , \quad y = \pm c\,P_{\mu-1} + ia$$

ou antes

$$x = (-1)^{\mu}.\,c\,Q_{\mu-1} + ib \quad , \quad y = (-1)^{\mu}.\,c\,P_{\mu-1} + ia.$$

Para a equação $ax + by = c$
temos

$$x = (-1)^{\mu}.\,c\,Q_{\mu-1} + ib \quad , \quad y = (-1)^{\mu+1}.\,c\,P_{\mu-1} - ia.$$

3. *Resolução fundada no theorema de Fermat.* — Basta achar as raizes de $ax - by = 1$.

Sendo (α, β) um systema de raizes, vimos já que eram todas dadas pelas formulas

$$x = \alpha + ib \quad , \quad y = \beta + ia.$$

Sabemos que b deve ser primo com a: pode comtudo ser um numero primo ou um producto de factores primos.

Seja $b = p$. Pelo theorema de Fermat sabemos que se tomarmos $\beta = \frac{a^{p-1}-1}{p}$, será β um numero inteiro, e como é

$$a\alpha = 1 + p\beta \quad \text{será} \quad \alpha = a^{p-2}$$

logo

$$x = a^{p-2} + ip \quad , \quad y = -\frac{1-a^{p-1}}{p} + ia.$$

Para $b = pp'$ tomando $a\alpha = 1 - (1-a^{p-1})(1-a^{p'-1})$, α será inteiro. Fica

$$pp'\beta = a\alpha - 1 = -(1-a^{p-1})(1-a^{p'-1})$$

d'onde tambem se tira β inteiro, e resulta

$$x = \frac{1-(1-a^{p-1})(1-a^{p'-1})}{a} + ib$$

$$y = -\frac{(1-a^{p-1})(1-a^{p'-1})}{b} + ia.$$

Em geral para $b = p \,.\, p' \,.\, p'' \,.\, \ldots \,.\, p^{(n)}$ em que p, p', $\ldots$ são numeros primos eguaes ou deseguaes, teremos

$$x = \frac{1-(1-a^{p-1})(1-a^{p'-1})\ldots(1-a^{p^{(n)}-1})}{a} + ib$$

$$y = -\frac{(1-a^{p-1})(1-a^{p'-1})\ldots\ldots(1-a^{p^{(n)}-1})}{b} + ia.$$

Se fossem $p_1, p_1', \ldots p_1^{(n)}$ os factores primos de a teriamos da

mesma maneira as formulas analogas

$$x = \frac{(1-b^{p_1-1})(1-b^{p_1'-1}\ldots(1-b^{p_1^{(n)}-1})}{a} + ib$$

$$y = -\frac{1-(1-b^{p_1-1})(1-b^{p_1'-1})\ldots(1-b^{p_1^{(n)}-1})}{b} + ia.$$

D'este modo temos formulas que nos dão immediatamente as raizes em funcção dos coefficientes da equação dada, conhecendo o systema de factores primos em que pode decompor-se o coefficiente de x ou y.

8. *Resolução fundada no theorema de Wilson.* — Segundo o theorema de Wilson é

$$\frac{1.2.3\ldots(p-1)+1}{p} = i.$$

Tratando-se pois da equação $ax - by = 1$, tomemos para y o valor

$$\beta = -\frac{1.2.3\ldots(p-1)+1}{p}$$

que é inteiro; e supponhamos $b = p$ sendo $b > a$, virá para x o valor tambem inteiro

$$\alpha = -\frac{1.2.3\ldots(p-1)}{a}.$$

E os valores geraes de x e y serão

$$x = -\frac{1.2.3\ldots(b-1)}{a} + ib \quad y = -\frac{1.2.3\ldots(b-1)}{b} + ia.$$

Se fosse $a > b$, teriamos

$$x = \frac{1.2.3\ldots(a-1)+1}{a} + ib \quad y = \frac{1.2\ldots(a-1)}{b} + ia.$$

9. *Systemas de equações, em que o numero das incognitas é egual ao das equações mais um.* — N'este caso, eliminam-se as variaveis; e, qualquer que seja o numero das equações, chegaremos sempre a uma equação a duas incognitas, de que se calcularão as raizes como fica dicto. Estes valores, substituidos nas equações que se tiverem formado auxiliarmente, dar-nos-hão os valores das outras incognitas, quando o problema for susceptivel de resolução.

10. *Caso em que a differença entre o numero das incognitas e o das equações é maior do que um.* — Este caso comprehende o de uma equação com um numero qualquer de variaveis.

Seja dado o systema de n equações a m variaveis

$$\left.\begin{aligned}
&a'_1 x_1 + a'_2 x_2 + a'_3 x_3 + \ldots + a'_m x_m = A' \\
&a''_1 x_1 + a''_2 x_2 + a''_3 x_3 + \ldots + a''_m x_m = A'' \\
&a'''_1 x_1 + a'''_2 x_2 + a'''_3 x_3 + \ldots + a'''_m x_m = A''' \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&a^{(n)}_1 x_1 + a^{(n)}_2 x_2 + a^{(n)}_3 x_3 + \ldots + a^{(n)}_m x_m = A^{(n)}
\end{aligned}\right\} \ldots\ldots (3).$$

Conforme ao que se disse no n.º 1 sabemos que as expressões de $x_1, x_2, \ldots x_m$ devem ser da fórma

$$x_1 = x' + F'_1 \alpha_1 + F'_2 \alpha_2 + \ldots + F'_{m-n} \alpha_{m-n} + F'_{m-n+1} \alpha_{m-n+1} + \ldots$$

$$x_2 = x'' + F''_1 \alpha_1 + F''_2 \alpha_2 + \ldots + F''_{m-n} \alpha_{m-n} + F''_{m-n+1} \alpha_{m-n+1} + \ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$x_m = x^{(m)} + F^{(m)}_1 \alpha_1 + F^{(m)}_2 \alpha_2 + \ldots + F^{(m)}_{m-n} \alpha_{m-n} + F^{(m)}_{m-n+1} \alpha_{m-n+1} + \ldots$$

onde $\alpha_1, \alpha_2, \ldots \alpha_{m-n}, \ldots$ representam indeterminadas, pelo menos, em numero $m - n$, e $F_{\alpha}^{(\beta)}$ são coefficientes a determinar.

Substituido estes valores nas equações (3) vem

$$\left.\begin{array}{l} a_1' x' + a_2' x'' + a_3' x''' + \ldots + a_m' x^{(m)} \\ + \left(a_1' F_1' + a_2' F_1'' + a_3' F_1''' + \ldots + a_m' F_1^{(m)}\right)\alpha_1 \\ + \left(a_1' F_2' + a_2' F_2'' + a_3' F_2''' + \ldots + a_m' F_2^{(m)}\right)\alpha_2 \\ + \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ + \left(a_1' F_{m-n}' + a_2' F_{m-n}'' + a_3' F_{m-n}''' + \ldots + a_m' F_{m-n}^{(m)}\right)\alpha_{m-n} \\ + \left(a_1' F_{m-n+1}' + a_2' F_{m-n+1}'' + a_3' F_{m-n+1}''' + \ldots + a_m' F_{m-n+1}^{(m)}\right)\alpha_{m-n+1} \\ + \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}\right\} = A'$$

$$\left.\begin{array}{l} a_1'' x' + a_2'' x'' + a_3'' x''' + \ldots + a_m'' x^{(m)} \\ + \left(a_1'' F_1' + a_2'' F_1'' + a_3'' F_1''' + \ldots + a_m'' F_1^{(m)}\right)\alpha_1 \\ + \left(a_1'' F_2' + a_2'' F_2'' + a_3'' F_2''' + \ldots + a_m'' F_2^{(m)}\right)\alpha_2 \\ + \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ + \left(a_1'' F_{m-n}' + a_2'' F_{m-n}'' + a_3'' F_{m-n}''' + \ldots + a_m'' F_{m-n}^{(m)}\right)\alpha_{m-n} \\ + \left(a_1'' F_{m-n+1}' + a_2'' F_{m-n+1}'' + a_3'' F_{m-n+1}''' + \ldots + a_m'' F_{m-n+1}^{(m)}\right)\alpha_{m-n+1} \\ + \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}\right\} = A''$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\left.\begin{array}{l}
a_1^{(n)}x' + a_2^{(n)}x'' + a_3^{(n)}x''' + \ldots + a_m^{(n)}x^{(m)} \\
+\left(a_1^{(n)}F_1' + a_2^{(n)}F_1'' + a_3^{(n)}F_1''' + \ldots + a_m^{(n)}F_1^{(m)}\right)\alpha_1 \\
+\left(a_1^{(n)}F_2' + a_2^{(n)}F_2'' + a_3^{(n)}F_2''' + \ldots + a_m^{(n)}F_2^{(m)}\right)\alpha_2 \\
+ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
+\left(a_1^{(n)}F_{m-n}' + a_2^{(n)}F_{m-n}'' + a_3^{(n)}F_{m-n}''' + \ldots + a_m^{(n)}F_{m-n}^{(m)}\right)\alpha_{m-n} \\
+\left(a_1^{(n)}F_{m-n+1}' + a_2^{(n)}F_{m-n+1}'' + a_3^{(n)}F_{m-n+1}''' + \ldots + a_m^{(n)}F_{m-n}^{(m)}\right)\alpha_{m-n+1} \\
+ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{array}\right\} = A^{(n)}$$

d'onde, attendendo á significação das quantidades α_i, resultam os seguintes systemas d'equações

$$\left.\begin{array}{l}
a_1'x' + a_2'x'' + a_3'x''' + \ldots + a_m'x^{(m)} = A' \\
a_1''x' + a_2''x'' + a_3''x''' + \ldots + a_m''x^{(m)} = A'' \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
a_1^{(n)}x' + a_2^{(n)}x'' + a_3^{(n)}x''' + \ldots + a_m^{(n)}x^{(m)} = A^{(n)}
\end{array}\right\} \ldots\ldots (4)$$

$$\left.\begin{array}{l}
a_1'F_1' + a_2'F_1'' + a_3'F_1''' + \ldots + a_m'F_1^{(m)} = 0 \\
a_1'F_2' + a_2'F_2'' + a_3'F_2''' + \ldots + a_m'F_2^{(m)} = 0 \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
a_1'F_{m-n}' + a_2'F_{m-n}'' + a_3'F_{m-n}''' + \ldots + a_m'F_{m-n}^{(m)} = 0 \\
a_1'F_{m-n+1}' + a_2'F_{m-n+1}'' + a_3'F_{m-n+1}''' + \ldots + a_m'F_{m-n+1}^{(m)} = 0 \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{array}\right\} \ldots\ldots (5)$$

$$\left.\begin{array}{l}
a_1''F_1' + a_2''F_1'' + a_3''F_1''' + \ldots + a_m''F_1^{(m)} = 0 \\
a_1''F_2' + a_2''F_2'' + a_3''F_2''' + \ldots + a_m''F_2^{(m)} = 0 \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
a_1''F_{m-n}' + a_2''F_{m-n}'' + a_3''F_{m-n}''' + \ldots + a_m''F_{m-n}^{(m)} = 0 \\
a_1''F_{m-n+1}' + a_2''F_{m-n+1}'' + a_3''F_{m-n+1}''' + \ldots + a_m''F_{m-n+1}^{(m)} = 0 \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{array}\right\} \ldots (6)$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\left.\begin{array}{l}
a_1^{(n)}F_1' + a_2^{(n)}F_1'' + a_3^{(n)}F_1''' + \ldots + a_m^{(n)}F_1^{(m)} = 0 \\
a_1^{(n)}F_2' + a_2^{(n)}F_2'' + a_3^{(n)}F_2''' + \ldots + a_m^{(n)}F_2^{(m)} = 0 \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
a_1^{(n)}F_{m-n}' + a_2^{(n)}F_{m-n}'' + a_3^{(n)}F_{m-n}''' + \ldots + a_m^{(n)}F_{m-n}^{(m)} = 0 \\
a_1^{(n)}F_{m-n+1}' + a_2^{(n)}F_{m-n+1}'' + a_3^{(n)}F_{m-n+1}''' + \ldots + a_m^{(n)}F_{m-n+1}^{(m)} = 0 \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{array}\right\} \ldots (7)$$

As equações (4) analogas ás primitivas servirão para achar os valores de x', x'', $\ldots$ $x^{(n)}$. Os systemas (5), (6), (7) vão aproveitar-nos para determinar os valores dos $F_\alpha^{(\beta)}$.

Para isso formemos as equações de condição a que devem satisfazer estas quantidades no caso geral d'um numero n de

equações a m variaveis. São ellas, adoptando a notação abreviada dos determinantes:

$$\left(a_2' a_3'' \ldots\ldots a_{n+1}^{(n)}\right) a_1' - \left(a_1' a_3'' \ldots\ldots a_{n+1}^{(n)}\right) a_2' + \ldots\ldots\ldots\ldots + (-1)^n \left(a_1' a_2'' \ldots a_n^{(n)}\right) a_{n+1}' = 0$$

$$\left(a_2' a_3'' \ldots a_n^{(n-1)} a_{n+2}^{(n)}\right) a_1' - \left(a_1' a_3'' \ldots a_n^{(n-1)} a_{n+2}^{(n)}\right) a_2' + \ldots\ldots\ldots\ldots + 0\, a_{n+1}' + (-1)^n \left(a_1' a_2'' \ldots a_n^{(n)}\right) a_{n+2}' = 0$$

$$\left(a_2' a_3'' \ldots a_{n+1}^{(n-1)} a_{n+2}^{(n)}\right) a_1' - \left(a_1' a_3'' \ldots a_{n+1}^{(n-1)} a_{n+2}^{(n)}\right) a_2' + \ldots\ldots\ldots\ldots + (-1)^{n-1} \left(a_1' a_2'' \ldots a_{n+2}^{(n)}\right) a_{n+1}' + (-1)^n \left(a_1' a_2'' \ldots a_{n+1}^{(n)}\right) a_{n+2}' = 0$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\left(a_3' \ldots a_{n+1}^{(n-1)} a_{n+2}^{(n)}\right) a_1' + 0\, a_2' - \left(a_1' a_4'' \ldots a_{n+2}^{(n)}\right) a_3' + \ldots + (-1)^{n-1} \left(a_1' a_3'' \ldots a_{n+2}^{(n)}\right) a_{n+1}' + (-1)^n \left(a_1' a_3'' \ldots a_{n+1}^{(n)}\right) a_{n+2}' = 0$$

$$0\, a_1' + \left(a_3' a_4'' \ldots\ldots a_{n+2}^{(n)}\right) a_2' - \left(a_2' a_4'' \ldots a_{n+2}^{(n)}\right) a_3' + \ldots + (-1)^{n-1} \left(a_2' a_3'' \ldots a_{n+2}^{(n)}\right) a_{n+1}' + (-1)^n \left(a_2' a_3'' \ldots a_{n+1}^{(n)}\right) a_{n+2}' = 0$$

$$\left(a_2' \ldots a_n^{(n-1)} a_{n+3}^{(n)}\right) a_1' - \left(a_1' a_3'' \ldots a_n^{(n-1)} a_{n+3}^{(n)}\right) a_2' + \ldots\ldots\ldots\ldots + 0\, a_{n+1}' + 0\, a_{n+2}' \ldots\ldots + (-1)^n \left(a_1' a_1'' \ldots a_n^{(n)}\right) a_{n+3}' = 0$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$0\,a_1' + 0\,a_2' + \left(a_4' \ldots a_{n+2}^{(n-1)}\, a_{n+3}^{(n)}\right) a_3' - \ldots +$$
$$+ (-1)^{n-1}\left(a_3' a_4'' \ldots a_{n+3}^{(n)}\right) a_{n+2}' + (-1)^n \left(a_3' a_4'' \ldots a_{n+2}^{(n)}\right) a_{n+3}' = 0$$

. . . . . .

$$\left(a_2' a_3'' \ldots a_n^{(n-1)}\, a_m^{(n)}\right) a_1' - \left(a_1' a_3'' \ldots a_n^{(n-1)}\, a_m^{(n)}\right) a_2' + \ldots\ldots\ldots\ldots +$$
$$+ (-1)^{n-1}\left(a_1' a_2'' \ldots a_m^{(n)}\right) a_n' + (-1)^n \left(a_1' a_2'' \ldots a_n^{(n)}\right) a_m' = 0$$

$$\left(a_2' a_3'' \ldots a_{n+1}^{(n-1)}\, a_m^{(n)}\right) a_1' - \left(a_1' a_3'' \ldots a_{n+1}^{(n-1)}\, a_m^{(n)}\right) a_2' + \ldots\ldots\ldots\ldots +$$
$$+ 0\,a_n' + (-1)^{n-1}\left(a_1' a_2'' \ldots a_m^{(n)}\right) a_{n+1}' +$$
$$+ (-1)^n \left(a_1' a_2'' \ldots a_{n+1}^{(n)}\right) a_m' = 0$$

. . . . . .

$$\left(a_{m-n+1}' a_{m-n+2}'' \ldots a_{m-1}^{(n-1)}\, a_m^{(n)}\right) a_1' + \ldots\ldots\ldots + \ldots\ldots\ldots +$$
$$+ (-1)^{n-1}\left(a_1' a_{m-n+1}'' a_m^{(n)}\right) a_{m-1}' + (-1)^n \left(a_1' a_{m-n+1}'' a_{m-1}^{(n)}\right) a_m' = 0$$

$$0\,a_1' + \left(a_3' \ldots a_{n+1}^{(n-1)}\, a_m^{(n)}\right) a_2' + \ldots\ldots + \ldots\ldots +$$
$$+ (-1)^{n-1}\left(a_2' a_3'' \ldots a_m^{(n)}\right) a_{n+1}' +$$
$$+ \ldots\ldots + (-1)^n \left(a_2' a_3'' \ldots a_{n+1}^{(n)}\right) a_m' = 0$$

. . . . . .

$$0\,a_1' + \left(a_{m-n+2}' a_{m-n+3}'' \ldots a_{m-n}^{(n-1)}\, a_m^{(n)}\right) a_2' + \ldots\ldots + \ldots\ldots +$$
$$+ (-1)^{n-1}\left(a_2' a_{m-n+2}'' \ldots a_m^{(n)}\right) a_{m-1}' + (-1)^n \left(a_2' a_{m-n+2}'' a_{m-1}^{(n)}\right) a_m' = 0$$

. . . . . .

$$0\,a_1' + \qquad 0\,a_2' + \qquad +$$
$$+\left(a'_{m-n+1}\ldots a_m^{(n)}\right)a'_{m-n} - \left(a'_{m-n}\ldots a_{m-1}^{(n-1)}\,a_m^{(n)}\right)a'_{m-n+1} + \ldots\ldots +$$
$$+(-1)^{n-1}\left(a'_{m-n}a''_{m-n+1}\ldots a_m^{(n)}\right)a'_{m-1} + (-1)^n\left(a'_{m-n}a''_{m-n+1}\ldots a_{m-1}^{(n)}\right)a'_m = 0.$$

Logo

$$F_1' = \left(a_2'a_3''\ldots\ldots a_{n+1}^{(n)}\right),\quad F_1'' = -\left(a_1'a_3''\ldots\ldots a_{n+1}^{(n)}\right),\ldots\ldots,$$
$$F_1^{(n+1)} = (-1)^n\left(a_1'a_2''\ldots a_n^{(n)}\right),\quad F_1^{(n+2)} = 0\qquad,$$

$$F_2' = \left(a_2'a_3''\ldots a_n^{(n-1)}\,a_{n+2}^{(n)}\right),\quad F_2'' = -\left(a_1'a_3''\ldots a_n^{(n-1)}\,a_{n+2}^{(n)}\right),\ldots\ldots,$$
$$F_2^{(n+1)} = 0\qquad,\quad F_2^{(n+2)} = (-1)^n\left(a_1'a_2''\ldots a_n^{(n)}\right),$$
$$F_2^{(n+3)} = 0\qquad,\quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$F_3' = \left(a_2'a_3'\ldots a_{n+1}^{(n-1)}\,a_{n+2}^{(n)}\right),\quad F_3'' = -\left(a_1'a_3''\ldots a_{n+1}^{(n-1)}\,a_{n+2}^{(n)}\right),\ldots\ldots,$$
$$F_3^{(n+1)} = (-1)^{n-1}\left(a_1'a_2''\ldots a_{n+2}^{(n)}\right),\quad F_3^{(n+2)} = (-1)^n\left(a_1'a_2''\ldots a_{n+1}^{(n)}\right),$$
$$F_3^{(n+3)} = 0\qquad,\quad \ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$F_{n+2}' = \left(a_3'\ldots a_{n+1}^{(n-1)}\,a_{n+2}^{(n)}\right),\quad F_{n+2}'' = 0\qquad,\ldots\ldots,$$
$$F_{n+2}^{(n+1)} = (-1)^{n-1}\left(a_1'a_3''\ldots a_{n+2}^{(n)}\right),\quad F_{n+2}^{(n+2)} = (-1)^n\left(a_1'a_3''\ldots a_{n+1}^{(n)}\right),$$
$$F_{n+2}^{(n+3)} = 0\qquad,\quad \ldots\ldots\ldots\ldots\ldots\ldots$$

$$F_{n+3}' = 0\qquad,\quad F_{n+3}'' = -\left(a_3'a_4''\ldots\ldots a_{n+2}^{(n)}\right),\ldots\ldots,$$
$$F_{n+3}^{(n+1)} = (-1)^{n-1}\left(a_2'a_3''\ldots a_{n+2}^{(n)}\right),\quad F_{n+3}^{(n+2)} = (-1)^n\left(a_2'a_3''\ldots a_{n+1}^{(n)}\right),$$
$$F_{n+3}^{(n+3)} = 0\qquad,\quad \ldots\ldots\ldots\ldots\ldots\ldots$$

$$F'_{n+4}=\left(a'_2\ldots a_n^{(n-1)}\,a_{n+3}^{(n)}\right),\quad F''_{n+4}=-\left(a'_1a''_3\ldots a_n^{(n-1)}\,a_{n+3}^{(n)}\right),\ldots\ldots,$$

$$F_{n+4}^{(n+1)}=0\quad,\quad F_{n+4}^{(n+2)}=0\quad,$$

$$F_{n+4}^{(n+3)}=(-1)^n\left(a'_1a''_2\ldots a_n^{(n)}\right)\quad,\quad F_{n+4}^{(n+4)}=0\quad,\ldots\ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$F'_{C^2_{n+3}}=0\quad,\quad F''_{C^2_{n+3}}=0\quad,\ldots\ldots,$$

$$F_{C^2_{n+3}}^{(n+2)}=(-1)^{n-1}\left(a'_3a''_4\ldots a_{n+3}^{(n)}\right),$$

$$F_{C^2_{n+3}}^{(n+3)}=(-1)^n\left(a'_3a''_4\ldots a_{n+2}^{(n)}\right)\quad,\quad F_{C^2_{n+3}}^{(n+4)}=0\quad,\ldots\ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$F'_{C^{n+1}_{m-1}+1}=\left(a'_2a''_3\ldots\ldots a_n^{(n-1)}\,a_m^{(n)}\right)\quad,$$

$$F'_{C^{n+1}_{m-1}+1}=-\left(a'_1a''_3\ldots a_n^{(n-1)}\,a_m^{(n)}\right)\quad,\ldots\ldots\ldots\ldots,$$

$$F_{C^{n+1}_{m-1}+1}^{(n)}=(-1)^{n-1}\left(a'_1a''_2\ldots a_m^{(n)}\right)\quad,\quad F_{C^{n+1}_{m-1}+1}^{(n+1)}=0\quad,$$

$$\ldots\ldots\ldots\ldots\quad,\quad F_{C^{n+1}_{m-1}+1}^{(m)}=(-1)^n\left(a'_1a''_2\ldots a_n^{(n)}\right)$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$F'_{C^{n+1}_{m-1}+C^{n-1}_{m-2}}=\left(a'_{m-n+1}a''_{m-n+2}\ldots a_{m-1}^{(n-1)}\,a_n^{(n)}\right)\quad,$$

$$F''_{C^{n+1}_{m-1}+C^{n-1}_{m-2}}=0\quad,\ldots\ldots\ldots\ldots,$$

$$F^{(m-1)}_{C^{n+1}_{m-1}+C^{n-1}_{m-2}} = (-1)^{n-1}\left(a_1' a_{m-n+1}'' \ldots a_m^{(n)}\right),$$

$$F^{(m)}_{C^{n+1}_{m-1}+C^{n-1}_{m-2}} = (-1)^{n}\left(a_1' a_{m-n+1}'' \ldots a_{m-1}^{(n)}\right)$$

$$F'_{C^{n+1}_{m-1}+C^{n-1}_{m-2}+1} = 0 \quad ,$$

$$F''_{C^{n+1}_{m-1}+C^{n-1}_{m-2}+1} = \left(a_3' \ldots a_{n+1}^{(n-1)} a_m^{(n)}\right) \quad , \ldots\ldots\ldots\ldots,$$

$$F^{(n+1)}_{C^{n-1}_{m-1}+C^{n-1}_{m-1}+1} = (-1)^{n-1}\left(a_2' a_3'' \ldots a_m^{(n)}\right) \quad , \ldots\ldots,$$

$$F^{(m)}_{C^{n+1}_{m-1}+C^{n-1}_{m-2}+1} = (-1)^{n}\left(a_2' a_3'' \ldots a_{n+1}^{(n)}\right)$$

. . . . . .

$$F'_{C^{n+1}_{m-1}+C^{n-1}_{m-2}+C^{n-1}_{m-2}} = 0 \quad ,$$

$$F''_{C^{n+1}_{m-1}+C^{n-1}_{m-2}+C^{n-1}_{m-3}} = \left(a_{m-n+2}' a_{m-n+3}'' \ldots a_{m-n}^{(n-1)} a_m^{(n)}\right) \quad , \ \ldots \ ,$$

$$F^{(m-1)}_{C^{n+1}_{m-1}+C^{n-1}_{m-1}+C^{n-1}_{m-3}} = (-1)^{n-1}\left(a_2' a_{m-n+2}'' \ldots a_m^{(n)}\right)$$

$$F^{(m)}_{C^{n+1}_{m-1}+C^{n-1}_{m-2}+C^{n-1}_{m-3}} = (-1)^{n}\left(a_2' a_{m-n+2}'' \ldots a_{m-1}^{(n)}\right)$$

. . . . . .

$$F'_{C^{n+1}_{m}} = 0 \quad ,$$

$$F''_{C^{n+1}_{m}} = 0 \quad , \ldots\ldots\ldots\ldots,$$

$$F^{(m-n)}_{C^{n+1}_m} = \left(a'_{m-n+1} \ldots a^{(n)}_m\right) \quad , \quad F^{(m-n+1)}_{C^{n+1}_m} = -\left(a'_{m-n} \ldots a^{(n)}_m\right) \ldots ,$$

$$F^{(m)}_{C^{n+1}_m} = (-1)^n \left(a'_{m-n} a''_{m-n+1} \ldots a^{(n)}_{m-1}\right).$$

Portanto se tivermos uma equação com m variaveis

$$a'_1 x_1 + a'_2 x_2 + a'_3 x_3 + \ldots\ldots\ldots\ldots + a'_m x_m = 0$$

será

$$x_1 = x' + a'_2 \alpha_1 + a'_3 \alpha_2 + a'_4 \alpha_4 + \ldots\ldots\ldots + a'_m \alpha_{C^2_{m-1}+1}$$

$$x_2 = x'' - a'_1 \alpha_1 + a'_3 \alpha_4 + a'_4 \alpha_5 + \ldots\ldots\ldots + a'_m \alpha_{C^2_{m-1}+2}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$x_m = x^{(m)} - a'_1 \alpha_{C^2_{m-1}+1} - a'_2 \alpha_{C^2_{m-1}+2} - \ldots\ldots - a'_{m-1} \alpha_{C^2_m}$$

Para um systema de duas equações a m variaveis

$$a'_1 x_1 + a'_2 x_2 + a'_3 x_3 + \ldots\ldots\ldots + a'_m x_m = 0$$
$$a''_1 x_1 + a''_2 x_2 + a''_3 x_3 + \ldots\ldots\ldots + a''_m x_m = 0$$

temos

$$x_1 = x' + \left(a'_2 a''_3\right)\alpha_1 + \left(a'_2 a''_4\right)\alpha_2 + \left(a'_3 a''_4\right)\alpha_4 + \ldots + \left(a'_2 a''_m\right)\alpha_{C^3_{m-1}} +$$

$$+ \left(a'_2 a''_m\right)\alpha_{C^3_{m-1}} \ldots\ldots \quad + \left(a'_{m-1} a''_m\right)\alpha_{C^3_{m-1}+(m-2)}$$

$$x_2 = x'' - \left(a'_1 a''_3\right)\alpha_1 - \left(a'_2 a''_4\right)\alpha_2 - \left(a'_3 a''_4\right)\alpha_3 + \ldots + \left(a'_2 a''_m\right)\alpha_{C^3_{m-1}+1} +$$

$$+ \ldots + \left(a'_3 a''_m\right)\alpha_{C^3_{m-1}+(m-2)+1} + \ldots + \left(a_{m-2} a''_m\right)\alpha_{C^3_{m-1}+(m-2)+(m-3)}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$x_m = x^{(m)} + \left(a'_1 a''_2\right)\alpha_{C^3_{m-1}+1} + \left(a'_1 a''_{m-1}\right)\alpha_{C^3_{m-1}+(m-2)} + \ldots + \left(a'_{m-2} a''_{m-1}\right)\alpha_{C^3_m} .$$

Finalmente as formulas que resolvem o systema (3) de n equações a m variaveis, são

$$x_1 = x' + \left(a_2' a_3'' \ldots a_{n+1}^{(n)}\right)\alpha_1 + \left(a_2' a_3'' \ldots a_n^{(n-1)} a_{n+2}^{(n)}\right)\alpha_2 + \left(a_2' a_3'' \ldots a_{n+2}^{(n)}\right)\alpha_3 +$$

$$+ \ldots\ldots + \left(a_3' \ldots a_{n+1}^{(n-1)} a_{n+2}^{(n)}\right)\alpha_{n+2} + \left(a_2' \ldots a_n^{(n-1)} a_{n+3}^{(n)}\right)\alpha_{n+4} + \ldots\ldots +$$

$$+ \left(a_2' \ldots a_n^{(n-1)} a_m^{(n)}\right)\alpha_{C_{m-1}^{n+1}+1} + \ldots + \left(a_{m-n+1}' a_{m-n+2}'' \ldots a_{m-1}^{(n-1)} a_m^{(n)}\right)\alpha_{C_{m-1}^{n+1}+C_{m-2}^{n-1}}$$

$$x_2 = x'' - \left(a_1' a_3'' \ldots a_{n+1}^{(n)}\right)\alpha_1 - \left(a_1' a_3'' \ldots a_n^{(n-1)} a_{n+2}^{(n)}\right)\alpha_2 - \left(a_1' a_3'' \ldots a_{n+2}^{(n)}\right)\alpha_3 -$$

$$- \ldots - 0\,\alpha_{n+2} - \left(a_3' a_4'' \ldots a_{n+2}^{(n)}\right)\alpha_{n+3} - \ldots - \left(a_1' a_3'' \ldots a_n^{(n-1)} a_m^{(n)}\right)\alpha_{C_{m-1}^{n+1}+1} -$$

$$- \ldots + \left(a_3' \ldots a_{n+1}^{(n-1)} a_m^{(n)}\right)\alpha_{C_{m-1}^{n+1}+C_{m-2}^{n-1}+1} + \ldots\ldots\ldots\ldots\ldots +$$

$$+ a_{m-n+2}' a_{m-n+3}'' \ldots a_{m-n}^{(n-1)} a_m^{(n)}\Big)\alpha_{C_{m-1}^{n+1}+C_{m-2}^{n-1}+C_{m-3}^{n-1}}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$x_m = x^{(m)} + (-1)^n \left(a_1' a_2'' \ldots a_n^{(n)}\right)\alpha_{C_{m-1}^{n+1}+1} + \ldots\ldots\ldots\ldots\ldots +$$

$$+ (-1)^n \left(a_1' a_{m-n+1}'' \ldots a_{m-1}^{(n)}\right)\alpha_{C_{m-1}^{n+1}+C_{m-2}^{n-1}} + \ldots\ldots\ldots\ldots\ldots +$$

$$+ (-1)^n \left(a_2' a_3'' \ldots a_{n+1}^{n}\right)\alpha_{C_{m-1}^{n+1}+C_{m-2}^{n+1}+1} + \ldots\ldots\ldots\ldots\ldots +$$

$$+ (-1)^n \left(a_2' a_{m-n+2}'' \ldots a_{m-1}^{(n)}\right)\alpha_{C_{m-1}^{n+1}+C_{m-2}^{n-1}+C_{m-3}^{n-1}} + \ldots\ldots\ldots\ldots +$$

$$+ (-1)^n \left(a_{m-n}' a_{m-n+1}'' \ldots a_{m-1}^{(n)}\right)\alpha_{C_m^{n+1}}.$$

RESOLUÇÃO DAS EQUAÇÕES INDETERMINADAS DO SEGUNDO GRÁO

Reducção da equação geral do segundo gráo entre duas variaveis.

11. *Reducção á fórma* $At^2 + B = u^2$, *por Lagrange.* — Seja a equação

$$ay^2 + bxy + cx^2 + dy + cx + f = 0 \ldots\ldots\ldots (8).$$

Esta equação pode escrever-se do seguinte modo:

$$2ay + bx + d = \sqrt{(bx + d)^2 - 4a\,(cx^2 + ex + d)}.$$

E fazendo

$$b^2 - 4ac = A \quad , \quad bd - 2ae = g \quad , \quad d^2 - 4af = h$$

para se obterem as soluções de (8) em numeros inteiros é necessario que seja

$$Ax^2 + 2gx + h = t^2$$

ou $$Ax + g = \sqrt{At^2 + g^2 - Ah}.$$

Por isso fazendo $g - Ah = B$

deve ainda ser satisfeita a equação

$$At^2 + B = u^2 \ldots\ldots\ldots\ldots\ldots (9).$$

12. *Reducção da equação* (9) *a* $Ct^2 - 2ntz + Bz^2 = 1$, *por Lagrange.* — Faça-se

$$u = nt - Bz.$$

A equação (9) torna-se em

$$(n^2 - A)\,t^2 - 2nBtz + B^2z^2 = B \ldots\ldots\ldots (10)$$

onde $(n^2 - A)\,t^2$ deve ser divisivel por B e por isso

$$\frac{n^2 - A}{B} = C$$

que reduz (10) á fórma

$$Ct^2 - 2ntz + Bz^2 = 1 \ldots\ldots\ldots\ldots (11).$$

13. *Reducção feita por Legendre á fórma* $at^2 + btu + cu^2 = M$. Substituindo em (8)

$$y = \frac{t + \alpha}{\theta} \quad , \quad x = \frac{u + \beta}{\theta}$$

fazendo

$$2a\alpha + b\beta + d\theta = 0 \quad , \quad 2c\beta + b\alpha + f\theta = 0$$

isto é

$$\frac{\alpha}{\theta} = \frac{2cd - bf}{b^2 - 4ac} \quad , \quad \frac{\beta}{\theta} = \frac{2af - bd}{b^2 - 4ac}$$

e $$M = -(af^2 - bdf + cd^2)(b^2 - 4ac) - g\,(b^2 - 4ac)^2$$

a equação (8) torna-se em

$$at^2 + btu + cu^2 = M \ldots\ldots\ldots\ldots (12).$$

14. *Reducção feita por Gauss.* — Gauss obtem uma formula analoga á precedente, suppondo

$$u = (b^2 - ac)\,y + bd - ce \quad , \quad t = (b^2 - ac)\,x + be - ad.$$

Como opera de modo que na proposta os termos em xy, y

e x tenham os coefficientes $2b$, $2d$, e $2e$ a transformada é

$$at^2 + 2btu + cu^2 = M \ldots\ldots\ldots\ldots (13)$$

sendo $M = -(cd^2 - 2bde + ac^2)(b^2 - ac) - f(b^2 - cc)$.

15. *Resolução de Brahmegupta.* — Ultimamente têm sido vertidos para inglez trabalhos antiquissimos dos geometros indianos, e o seu valor faz sentir que o não tivessem sido ha mais tempo. Foi d'elles que Chasles tirou a idêa da resolução geometrica das equações indeterminadas do segundo gráo. São ainda d'elles as duas regras seguintes:

1.ª Sendo a, b um systema qualquer de raizes de

$$At^2 + 1 = u^2 \ldots\ldots\ldots\ldots\ldots (14)$$

t', u' um systema de raizes de

$$At^2 + B = u^2 \ldots\ldots\ldots\ldots\ldots (9')$$

as raizes d'esta equação são dadas pelas formulas

$$t = au' + bt' \quad , \quad u = Bbu' + at' \ldots\ldots\ldots (15).$$

2.ª Sendo a, b um systema de raizes de $(9')$ as raizes de (14) são

$$u = \frac{Aa^2 + B^2}{B} \quad , \quad t = \frac{2ab}{B}.$$

Substituindo $B = l^2 - Aa^2$

e fazendo $l = 1$, resultam as expressões de Fermat, Brounker, etc.

Euler foi o primeiro que na Europa descobriu as expressões (15).

Resolução da equação $u^2 + t^2 = B$.

16. *Methodo de Fibonaci.* — Fibonaci geometra italiano an-

terior a Euler, apezar de pouco conhecido, deixou trabalhos importantes.

Para achar as formulas que dão as raizes de

$$u^2+t^2=B \ldots\ldots\ldots\ldots\ldots\ldots (16)$$

conhecido um systema de raizes u', t', toma dois numeros n, n' de que a somma dos quadrados seja um quadrado. Teremos

$$u'^2+t'^2=B \quad , \quad n^2+n'^2=N^2 \ldots\ldots\ldots (17).$$

E as expressões geraes das raizes de (16) são

$$u=\frac{nt'+n'u'}{N} \quad , \quad t=\frac{nu'-n't'}{N} \ldots\ldots\ldots (18).$$

Partindo d'estas expressões facilmente acharíamos as das raizes de (9).

A solução de Diophante conduz a

$$u=\frac{(n^2-1)u'+2nt}{n^2+1} \quad , \quad t=\frac{2nu'-(n^2-1)t'}{n^2+1}.$$

Expressões que não são proprias para a resolução em numeros inteiros, contendo uma só indeterminada, e não se usando da relação auxiliar $n^2+n'^2=N^2$.

17. *Methodo geometrico de Chasles.* — Consideremos um triangulo rectangulo ABC em que os lados BA e BC são as raizes racionaes u', t' (*). Tire-se por C uma recta e prolongue-se até encontrar em D o prolongamento de AB, e por A uma perpendicular AE a CD. AE, CE é um systema de raizes da proposta.

Vejamos as condições a que deve satisfazer a construcção para que sejam racionaes.

(*) A simplicidade da figura dispensa-nos apresental-a.

Construindo-se sobre BC o triangulo rectangulo BCD com a condição de serem racionaes os lados BD e CD, o que pode effectuar-se d'uma infinidade de maneiras, serão no triangulo ACD racionaes os lados, e por isso tambem as perpendiculares abaixadas dos vertices sobre elles.

A raiz AE, uma d'estas perpendiculares, é portanto racional e egualmente a raiz CE por ser

$$CE = \frac{\overline{CD}^2 + \overline{AC}^2 - \overline{AD}^2}{2\overline{CD}}.$$

18. *Deducção das formulas analiticas* (18) *partindo da construcção geometrica antecedente.* — As expressões das raizes deduzidas da construcção, são

$$AE = \frac{\overline{BC}.\overline{AD} + \overline{BC}.\overline{AB}}{CD} \quad , \quad CE = \frac{\overline{BC}^2 - \overline{AB}.\overline{BD}}{\overline{CD}}.$$

Mas é $AB = u'$, $BC = t'$, $AE = u$, $CE = t$,

e fazendo $BD = u$, $CD = N$

vem $$u = \frac{nt' + u't'}{N} \quad , \quad t = \frac{nu' - t'^2}{N}$$

sendo $N^2 - n^2 = t'^2$.

Por isso $$u = \frac{nt' + n'u'}{N} \quad , \quad t = \frac{nu' - n't'}{N}$$

formulas identicas a (18).

19. *Theorema de Lagrange sobre a resolução* $x^2 - Ay^2 = \pm 1$. *A equação* $x^2 - Ay^2 = +1$ *é soluvel quando* A *não é um quadrado perfeito, qualquer que seja o numero dos termos do periodo do desenvolvimento de* $\sqrt{A}$ *em fracção continua; e* $x^2 - Ay^2 = -1$ *quando este numero é par.*

*

O desenvolvimento de $\sqrt{A}$ em fracção continua dá

$$x = \sqrt{A} = a + \frac{\sqrt{A} - a}{1}$$

$$x' = \frac{1}{\sqrt{A} - a} = \frac{\sqrt{A} + a}{b} = \text{etc.}$$

As leis por meio das quaes se deduz d'um quociente completo qualquer $\frac{\sqrt{A} + I}{D}$ o seguinte $\frac{\sqrt{A} + I'}{D'}$ são

$$I = \mu D - I \quad , \quad D' = \frac{A - I'^2}{D}$$

μ sendo o maior inteiro comprehendido em $\frac{\sqrt{A} + I}{D}$. Logo se forem $\frac{p_0}{q_0}$, $\frac{p}{q}$ duas fracções consecutivas convergentes para $\sqrt{A}$ e $\frac{\sqrt{A} + I}{D}$ o quociente completo correspondente a $\frac{p}{q}$, teremos

$$pI + p_0 D = qA$$

$$qI + q_0 D = p,$$

d'onde

$$(pq_0 - p_0 q) I = qq_0 A - pp_0$$

$$(pq_0 - p_0 q) D = p^2 - Aq^2 \ldots\ldots\ldots\ldots (19)$$

sendo $pq_0 - p_0 q$ sempre do signal de $p^2 - Aq^2$ e por isso D positivo.

D e I são inteiros, I positivo

$$I < a \quad \text{e} \quad D < 2a.$$

De mais sendo

$$a\ ,\ \alpha\ ,\ \beta, \ldots . \lambda\ ,\ \mu : \alpha\ ,\ \beta, \ldots . . \lambda\ ,\ \mu : \ldots .$$

e $$\frac{1}{0}\ ,\ \frac{a}{1}\ ,\ \ldots . . . \frac{p_0}{q_0}\ ,\ \frac{p}{q} : \frac{p_1}{q_1}\ ,\qquad ,\ \frac{p'_0}{q'_0}\ ,\ \frac{p'}{q'} : \ldots .$$

as series dos quocientes, e das fracções convergentes que lhe correspondem no desenvolvimento de $\sqrt{A}$; teremos chamando z ao quociente completo correspondente ao ultimo quociente do primeiro periodo

$$z - \mu = \sqrt{A} - a \quad \text{ou} \quad z = \mu - a + \sqrt{A}$$

e $$p(\mu - a) + p_0 = Aq\ ,\ q(\mu - a) + q_0 = p$$

por onde se vê que é

$$\mu - a = a \quad \text{e} \quad \nu = 2a.$$

Logo a equação $$I_0 + I = D\mu$$

dá $$I = I_0 = a \quad \text{e} \quad D = 1$$

e a equação (19) torna-se em

$$p^2 - Aq^2 = \pm 1$$

± 1 conforme for $\frac{p}{q} \gtrless \sqrt{A}$.

Mas o quociente $2a$ existe com certeza no desenvolvimento de $\sqrt{A}$, logo é verdadeiro o theorema. E vê-se além disso que quando houver uma solução haverá uma infinidade, pois n'esse caso o quociente $2a$ repete-se uma infinidade de vezes.

20. *Resolução de* $x^2 - Ay^2 = \pm 1$, *em numeros inteiros por Legendre.* — Attendendo ao theorema antecedente vê-se que se for $\frac{p}{q}$ a primeira e mais simples fracção convergente corres-

pondente ao mesmo quociente $2a$ os valores de x e y são

$$x = \frac{(p - q\sqrt{A})^m + (p - q\sqrt{A})^m}{2}$$

$$y = \frac{(p + q\sqrt{A})^m - (p - q\sqrt{A})^m}{2\sqrt{A}}$$

que resolvem $x^2 - Ay^2 = \pm 1$ quando o numero dos termos do periodo é impar, e $x^2 - Ay^2 = +1$ quando esse numero é par.

Methodo de Euler.

21. *Resolução de* $1 + x^2 = y^2$. — Euler indica dois caminhos a seguir.

1.° Fazer $\sqrt{1 + x^2} = x + p$ d'onde $x = \frac{1 - p^2}{2p}$.

Dando a p valores quaesquer obteremos para x valores racionaes; os inteiros serão os procurados. Por meio d'estes immediatamente conheceremos os de y.

2.° Fazer $\sqrt{1 + x^2} = 1 + \frac{mx}{n}$ d'onde $x = \frac{2mn}{n^2 - m^2}$

e segue-se o mesmo raciocinio.

22. *Resolução de* $Ay^2 + 1 = x^2$. — É claro que não ha soluções se fôr A uma quantidade negativa, ou um quadrado. O methodo que Euler apresenta não se applica para um numero A qualquer.

Indicaremos para dois casos o modo como procede.

Seja $2y^2 + 1 = x^2$.

Fazendo $2y^2 + 1 = (y + p)^2$

vem $y = p + \sqrt{2p^2 - 1}$

que para $p = 1$ dá $y = 2$, $x = 3$.

Para $5y^2 + 1 = x^2$.

Fazendo $5y^2 + 1 = (2y + p)^2$

vem $y = 2p + \sqrt{5p^2 - 1}$

e como é $\sqrt{5p^2 - 1} > 2p$

deve ser $y = 4p + q$, $p = 2q + \sqrt{q^2 + 1}$

que dão para $q = 0$, $p = 1$

e por isso $y = 4$, $x = 9$.

Este processo torna-se porém muito laborioso, e já para $A = 13$ é bastante complicado.

23. *Resolução da equação* $t^2 - Au^2 = 1$ *por Lagrange.* — Se A for negativo só pode satisfazer-se-lhe em numeros inteiros fazendo $u = 0$, $t = 1$, e o mesmo succede sendo A positivo e quadrado.

Se A é um numero positivo não quadrado $t^2 - Au^2 = 1$ tem uma infinidade de soluções em numeros inteiros: bastará porém, achar os valores mais pequenos de t e u para os conhecermos todos.

Para isso desde que na serie P', P'', P'''... chegarmos a um termo egual á unidade calcularemos os termos correspondentes das duas series p', p'', p''',...; q', q'', q''',... os quaes representam os valores de t e u.

Sejam t_1, u_1 os mais pequenos valores de t e u que satisfazem a $t^2 - Au^2 = 1$, os valores de t e u estam relacionados com os

valores t_1, u_1 pelas formulas

$$t = \mathrm{T}t_1 + \mathrm{A}\mathrm{V}u_1 \quad , \quad u = \mathrm{T}u_1 + \mathrm{V}t_1$$

onde T e V são determinados pela relação $\mathrm{T}^2 - \mathrm{A}\mathrm{V}^2 = 1$ similhante á proposta.

Podemos por isso fazer

$$\mathrm{T} = t_1 \quad , \quad \mathrm{V} = u_1$$

do que resulta

$$t = t_1^2 + \mathrm{A}u_1^2 \qquad u = t_1 u_1 + t_1 u_1$$

ou $$t_2 = t_1^2 + \mathrm{A}u_1^2 \qquad u_2 = 2t_1 u_1$$

e $$t = \mathrm{T}t_2 + \mathrm{A}\mathrm{V}u_2 \quad , \quad u = \mathrm{T}u_2 + \mathrm{V}t_2$$

e continuando a proceder analogamente vemos que em geral achariamos para os valores de t e u

$$\left.\begin{aligned} t &= \mathrm{T}^m + \frac{m(m-1)}{2}\mathrm{A}\mathrm{T}^{m-2}\mathrm{V}^2 + \\ &+ \frac{m(m-1)(m-2)(m-3)}{2.3.4}\mathrm{A}^2\mathrm{T}^{m-4}\mathrm{V}^4 + \ldots \\ u &= m\mathrm{T}^{m-1}\mathrm{V} + m\frac{(m-1)(m-2)}{2.3}\mathrm{A}\mathrm{T}^{m-3}\mathrm{V}^3 + \\ &+ \frac{m(m-1)(m-2)(m-3)(m-4)}{2.3.4.5}\mathrm{A}^2\mathrm{T}^{m-5}\mathrm{V}^5 + \ldots \end{aligned}\right\} (20).$$

Estas expressões dar-nos-hão todos os valores de t e u tomando para m um numero inteiro qualquer e para T e V os menores valores que satisfazem a $t^2 + \mathrm{A}u^2 = 1$.

24. *Resolução da equação* $\mathrm{C}t^2 - 2\mathrm{n}tz + \mathrm{B}z^2 = 1$, *por Lagrange.*

1.° *Methodo.* Como t e z devem ser numeros inteiros, o pri-

meiro membro de (11) será um numero inteiro: logo achar os valores de t e z que lhe satisfazem, equivale a determinar esses valores para a condição de que o primeiro membro se reduza ao menor numero inteiro.

Temos tres casos a considerar conforme é $n^2 - BC$ menor ou maior do que nada, e ainda um quadrado perfeito.

1.° Caso $n^2 - BC < 0$. Reduzindo $\frac{n}{C}$ em fracção continua, e formando as fracções convergentes para $\frac{n}{C}$ os systemas que resultam de tomar para t os numeradores e para z os denominadores, quando satisfazem á proposta, são as raizes da proposta.

2.° Caso $n^2 - BC > 0$. A resolução effectua-se immediatamente com toda a facilidade.

3.° Caso $n^2 - BC = k^2$. O primeiro membro de (11) decompõe-se no producto de dois factores racionaes, e pode escrever-se do seguinte modo:

$$\frac{[Ct \pm (n+a)z][Ct \pm (n-a)y]}{C}$$

é pois necessario que seja $(n+a)(n-a)$ divisivel por C: ou sendo $C = bc$ deve ser

$$n + a = fb \quad , \quad n - a = gc,$$

e para satisfazermos a (11) é necessario que seja

$$ct \pm fz = \pm 1 \quad , \quad bt \pm gz = \pm 1$$

equações que nos determinam t e z.

2.° *Methodo*. Supponhamos $C < B$, o que sempre é possivel, e para facilidade

$$C = B' \quad , \quad z = t'.$$

Substituindo $t = mt' + t''$, temos fazendo

$$n - mB' = n' \quad , \quad m^2B' - 2mn + B = B''$$

$$B't''^2 - 2n't't'' + B''t'^2 = 1$$

e continuando a proceder analogamente chega-se a uma expressão da fórma

$$L\alpha^2 - 2M\alpha\beta + N\beta^2 = 1 \ldots\ldots\ldots\ldots (21)$$

sendo $M^2 - LN = n^2$, $CB = A$, α, β inteiros

e $2N < L$, $2N < M$ e $2M < L$.

Ora sendo $L > M$ a equação (19) multiplicada por M dá suppondo

$$\nu = M\beta - N\alpha$$

$$\nu - A\alpha^2 = M \ldots\ldots\ldots\ldots\ldots (22).$$

Temos dois casos a considerar:
1.° Caso $A < 0$. A equação (22) torna-se em

$$\nu^2 + A\alpha^2 = M \ldots\ldots\ldots\ldots\ldots (23).$$

É $$A \geqq \frac{3}{4} LM$$

e com mais razão $$M \leqq \frac{4}{3} \sqrt{A}.$$

Para que (23) possa subsistir é necessario que seja

$$\alpha = 0 \quad , \quad \nu^2 = M$$

M deve portanto ser um quadrado, $M = \lambda^2$.

Logo $\alpha = 0 \quad , \quad \nu = \pm \mu$

ou $\mu^2 \beta = \pm \mu \quad , \quad \beta = \pm \frac{1}{\mu}$

e β só será inteiro sendo $M = 1$.

Consequentemente a proposta só pode resolver-se no caso de $M = 1$ e por isso quando (23) se reduz a

$$\nu^2 + A\alpha^2 = 1.$$

2.° Caso $A > 0$. Pode se $M^2 \gtreqless A$.

Para $M^2 = A$ a proposta só pode subsistir sendo A um quadrado: então a resolução faz-se immediatamente com toda a facilidade.

Para $M^2 < A$ a equação resolve-se pelo methodo dos minimos.

25. *Deducção das soluções possiveis de* $Ct^2 - 2ntz + Bz^2 = 1$ *conhecida uma.*

Sejam p, q os valores achados

$$Cp^2 - 2npq + Bq^2 = 1 \ldots\ldots\ldots\ldots (24).$$

Tomando r e s taes que seja $ps - qr = 1$, se suppozermos

$$t = pt' + rz' \qquad z = qt' + sz'$$

fazendo

$$Cp^2 - 2npq + Bq^2 = P \quad , \quad Cpr - n(ps + qr) + Bqs = Q$$

$$Cr^2 - 2ns + Bs^2 = R$$

a equação (11) transforma-se em

$$Pt'^2 + 2Qt'z' + Rz'^2 = 1 \ldots\ldots\ldots\ldots (25)$$

onde é $P=1$ e em geral

$$r=\rho\sigma+mp \quad , \quad s=\sigma+mq$$

ρ e σ sendo valores que satisfazem a $pr-qs=1$, e m uma quantidade qualquer.

Portanto é

$$Q=Cps-n(p\sigma+qs)+Bq\sigma+mP$$

e como é $P=1$, tomando

$$m=-Cp\rho+n(p\sigma+q\rho)Bq\sigma$$

vem $Q=0$ e a equação (25) torna-se em

$$t'^2-Az'^2=1 \ldots\ldots\ldots\ldots\ldots (26).$$

Resolvida a equação (26) em numeros inteiros, pelos valores calculados para t' e z' obteremos os de t e z.

Com effeito attendendo ao valor de m temos

$$r=\rho(1-Cp^2)-Bpq\sigma+np(p\sigma+q\rho)$$

$$s=\sigma(1-Bq^2)-Cpq\rho+nq(p\sigma+q\rho)$$

e em virtude de (24)

$$r=(Bq-np)(p\rho-p\sigma)=-Bq+np$$

$$s=(Cp-nq)(p\sigma-q\rho)=\quad Cp-nq$$

portanto

$$t=pt'-(Bq-np)z'$$

$$z=qt'+(Cp-nq)z'.$$

26. *Resolução da equação* $Ap^2+Bq^2=z^2$, *por Lagrange.*—

Lagrange apresentou esta resolução nas *Memorias da Academia de Berlin, 1767*. Podemos suppor A e B positivos e A > B.

Vamos ver como se podem reduzir os coefficientes até que um d'elles seja egual á unidade.

Temos $$Ap^2 = z^2 - Bq^2.$$

Deve ser $z^2 - Bq^2$ divisivel por A.

Fazendo $$z = nq - Aq'$$

n e q' indeterminadas, teremos

$$z^2 = Bq^2 = (n^2 - B)\,q^2 - 2nAqq' + Aq'^2$$

onde deve ser $n^2 - B$ tambem divisivel por A, não sendo $n > \frac{A}{2}$.

Se para nenhum valor de n for satisfeita esta condição, segue-se que a equação dada não pode resolver-se em numeros inteiros.

Supponhamos que existem, e seja $\frac{n^2 - B}{A} = A'$. A proposta tornar-se-ha em

$$p^2 = A'q^2 - 2nqq' + Aq'^2$$

sendo $A' < A$.

Se A' for um quadrado fazendo $q' = 0$, $q = 1$ termina-se immediatamente a solução vindo

$$p = \sqrt{A'}.$$

Se A' não é um quadrado, mas for $A' < B$.

Multiplicaremos a equação acima por A'.

Fazendo $AA' - n^2 = -B'$, resulta

$$A'p^2 = (A'q - nq')^2 - B'q^2$$

devendo portanto ser $A'p^2 + B'q^2$ um quadrado, e temos uma equação analoga á proposta em que os coefficientes são menores.

Porém, se não é $A' < B$, nem pode tornar-se dividindo pelo maior quadrado possivel, faremos $q = \nu q' + q''$.

Fica $$p^2 = A'q''^2 - 2n'q''q' + A''q'^2$$

sendo $$n' = n - \nu A' \quad , \quad A'' = A'\nu^2 - 2n\nu + A = \frac{n'^2 - B}{A'}.$$

Tomando ν de modo que seja $n' < \frac{A''}{2}$ será $A'' < A'$.

Em seguida procede-se como antecedentemente. E no terceiro caso em que $A'' > B$, faremos

$$q' = \nu' q'' + q'''.$$

Resulta $$p^2 = A'''q'^2 - 2n''q''q''' + A''q'''^2$$

sendo $$n'' = n' - \nu' A'', \quad A''' = A''\nu'^2 - 2n'\nu' + A' = \frac{n''^2 - B}{A''}.$$

E é claro que continuando com o mesmo processo havemos de chegar a um coefficiente $A^{(n)} < B$; e temos a tractar, como se disse, uma equação em que os coefficientes são menores do que na proposta.

Continuando do mesmo modo temos a certeza de chegar a uma equação em que um dos coefficientes A ou B se reduzem á unidade. Seja

$$A^{(n)} p^2 + q^2 = z^2$$

a equação a que chegamos.

Decomponhamos $A^{(n)}$ em dois factores D, E, differentes. Substituindo

$$A = D \cdot E \qquad q = r \cdot s$$

resulta

$$(z + p)(z - p) = D \cdot E r^2 \cdot s$$

a que satisfaremos geralmente, tomando

$$z+p=\mathrm{D}.r^2 \quad , \quad z-p=\mathrm{E}.s^2$$

$$z=\frac{\mathrm{D}.r^2+\mathrm{E}.s^2}{2} \quad , \quad p=\frac{\mathrm{D}.r^2-\mathrm{E}s^2}{2} \quad q=r.s.$$

Em $Ap^2+Bq^2=z^2$ suppondo $A>B$, poderemos determinar para q e z valores taes $z=M$, $q=N$ que seja

$$M=nN-q'A.$$

Sendo M, N, A numeros primos entre si, e n, q' quantidades indeterminadas.

Será $z=nq-Aq'$, valor que substituido na proposta dá

$$\frac{n^2-B}{A}q^2-2nqq'+Aq'^2=z^2 \ldots\ldots\ldots (27)$$

equação que só pode subsistir sendo

$$\frac{n^3-B}{A}=\text{int.} \ldots\ldots\ldots\ldots (28).$$

Supponhamos por isso $n^2-B=AA'k^2$, (27) torna-se em

$$A'k^2q^2-2nqq'+Aq'^2=z^2 \ldots\ldots\ldots (29).$$

Havendo um numero n que satisfaça a (28), este numero pode ser augmentado ou diminuido d'um multiplo qualquer de A, e podemos suppor que o valor de que se tracta está comprehendido entre $-\frac{1}{2}A$ e $+\frac{1}{2}A$. No caso de nenhum valor de n comprehendido entre aquelles limites satisfizer, conclue-se que não ha solução.

Encontrando-se um ou muitos valores de n que satisfaçam, para cada um continuaremos como se segue.

Multiplicando (29) por $A'k$ e fazendo

$$A'k^2q - nq' = z' \quad , \quad kp = p',$$

resulta a equação

$$A'p'^2 + Bq'^2 = z'^2$$

onde é $$A' < \frac{1}{4}A:$$

e continuarimos a proceder do mesmo modo, obtendo que os coefficientes vão successivamente diminuindo.

Resolução da equação (9) $At^2 + B = u^2$.

27. *Methodo de Lagrange.* — Achando-se resolvida pelos numeros antecedentes 24 e 25 a equação (11), conheceremos immediatamente as raizes t de (9), e as raizes u pela relação

$$u = nt - Bz$$

estabelecida no n.° 12.

28. *Resolução por meio da equação* $Ap^2 + Bq^2 = z^2$ — Fazendo $u = \frac{z}{q}$, $t = \frac{p}{q}$ a equação (9) torna-se em

$$A\frac{p^2}{q^2} + B = \frac{z^2}{q^2} \quad \text{ou} \quad Ap^2 + Bq^2 = z^2$$

que se acha resolvida pelo n.° 26, e nos servirá para achar as raizes de (9).

29. *Methodo de Legendre.* — Sabe-se que $\frac{u}{t}$ deve ser uma fracção convergente para $\sqrt{A}$.

É portanto necessario desenvolver $\sqrt{A}$ em fracção continua, calcular os valores successivos dos quocientes completos $\frac{\sqrt{A}+I}{B}$;

se entre elles ha um de denominador egual ao segundo termo da proposta teremos uma solução de

$$At^2 + B = u^2 \quad \text{ou} \quad At^2 - B = u^2.$$

Calculando a fracção convergente $\frac{p}{q}$, se é de ordem impar teremos uma solução de $At^2 + B = u^2$, se é de ordem par será de $At^2 - B = u^2$.

No caso de não se encontrar B entre os denominadores dos quocientes completos do primeiro periodo a equação não pode resolver-se em numeros inteiros.

De cada primeiro systema de soluções t', u' podem deduzir-se uma infinidade de outras t, u

$$u = pu' \pm Aqt' \quad , \quad t = pt' \pm qu'.$$

30. *Methodo geometrico de Chasles.* — Á proposta podemos dar a fórma $A't^2 + u^2 = B'$.

Sejam t' u' duas raizes dadas e construa-se o triangulo ABC (é a mesma figura do n.° 17), tomando

$$AB = t'\sqrt{A'} \quad , \quad BC = u'.$$

Será $$\overline{AB}^2 + \overline{BC}^2 = B'$$

N'um segundo triangulo rectangulo AEC, temos

$$\overline{AE}^2 + \overline{EC}^2 = B'$$

tomando $$AE = t\sqrt{A'} \quad \text{e} \quad EC = u.$$

Portanto é necessario que seja

$$AE = t\sqrt{A'}.$$

Ora, temos $$\frac{AE}{BC} = \frac{AD}{CD}$$

logo AE tem o valor $t\sqrt{A'}$, se for $AD = n\sqrt{A'}$ e CD um numuro n.

Mas $$AD = t'\sqrt{A'} + BD$$

deve pois ser $$BD = \alpha\sqrt{A'}.$$

Por consequencia é preciso construir sobre BC um triangulo de que o segundo lado BD seja $\alpha\sqrt{A'}$, e de que a hypothenusa seja racional, o que se consegue por meio da formula

$$4m^2n^2 + (m^2 - n^2)^2 = (m^2 + n^2)^2$$

da qual, fazendo $n^2 = A'$, resulta

$$\frac{4A'm^2 \cdot \overline{BC}^2}{(m^2 - A')} + \overline{BC}^2 = \frac{(m^2 + A')^2}{(m^2 - A')^2} \cdot \overline{BC}^2.$$

E teremos os valores desejados de BD e CD tomando

$$BD = \frac{2m \cdot \overline{BC}}{m^2 - A'}\sqrt{A'} \quad , \quad CD = \frac{m^2 + A'}{m^2 - A'} \cdot \overline{BC}.$$

31. *Deducção das raizes de* (9) *partindo da solução de* (16).— Mudando na equação (16) t em $t\sqrt{A}$, e t' em $t'\sqrt{A}$, n em $n\sqrt{A}$ nas equações (17), tornam-se estas equações em

$$At^2 + u^2 = B \quad , \quad At'^2 + u'^2 = B \quad , \quad An^2 + n'^2 = N^2$$

e as raizes de (16) em

$$t\sqrt{A} = \frac{n\sqrt{A}u' - n'\sqrt{A}t'}{N} \quad , \quad u = \frac{n\sqrt{A}t' + n'u'}{N}$$

ou $$t = \frac{nu' - n't'}{N} \quad , \quad u = \frac{n\sqrt{A}t' + n'u'}{N}$$

que resolvem o problema.

32. *Resolução da equação* $At^2 + Bu^2 = C$ *pelo methodo de exclusão de Gauss.* — t deve ser uma quantidade tal que $\frac{C - At^2}{B} = D$ seja um numero positivo, inteiro e quadrado, e por isso

$$t < \sqrt{\frac{C}{A}}.$$

A segunda condição tem logar quando for $B = 1$.

Sendo B differente de 1 é necessario que $\frac{C}{A}$ seja um residuo quadratico de B e que t esteja comprehendido n'uma das fórmas

$$Bp + r \quad , \quad Bp - r \quad , \quad Bp + r' \quad , \quad Bp - r',$$

Substituiriamos em seguida por t todos os numeros d'estas fórmas, menores do que $\sqrt{C}$ de que representaremos o conjuncto por w e que tornam D um quadrado.

O methodo de exclusão de Gauss consiste em tomar muitos numeros a que se chama *excluentes,* e procurar os valores de t para os quaes D é um residuo não quadratico d'estes excluentes, e regeitar de w estes valores de t.

Não devem empregar-se como excluentes senão numeros primos ou potencias de numeros primos.

Para um excluente do ultimo genero, só temos a regeitar dos valores de D os não residuos que são residuos das potencias inferiores do mesmo numero primo, se já tivermos empregado esta potencia.

Seja o excluente $E = p^{\mu}$; p um numero primo que não divide A, μ um inteiro qualquer.

Supponhamos $p^{(n)}$ a mais alta potencia de p que não pode dividir n. Sejam $a, b, c, \ldots$ os residuos não quadraticos de E e procuremos os valores de z que satisfazem ás relações

$$mz = A - na + mEp^{\nu}$$

$$mz = A - nb + mEp^{\nu}$$

$$\ldots\ldots\ldots\ldots\ldots$$

e designemo-los por $\alpha, \beta, \gamma \ldots$.

Se para um valor de x for

$$x^2 = a + Mep^{\nu}$$

o valor de ν será $a + ME$, isto é, não será residuo de E, bem como os valores $\alpha, \beta, \gamma \ldots$

Posto isto, escolhendo entre os numeros $\alpha, \beta, \gamma \ldots$ os que são residuos quadraticos de Ep^{ν} e chamando-os $g, g', g'', \ldots$, calculemos os valores de $\sqrt{g}, \sqrt{g'}, \sqrt{g''}, \ldots$, os quaes designaremos por $h, h', h'', \ldots$.

Podemos regeitar de w todas as fórmas

$$Ep^{\nu}t \pm h \quad , \quad Ep^{\nu}t \pm h' \quad , \quad Ep^{\nu}t \pm h'', \ldots$$

e nenhum dos valores que ficam podem corresponder a um valor de ν da fórma

$$Eu + a \quad , \quad Eu + b \quad , \quad \ldots.$$

Empregando analogamente outros excluentes, podemos diminuir o numero dos valores de x a ensaiar.

Notemos que sendo p um divisor primo impar de m, nem p nem as suas potencias podem ser tomadas como excluentes.

Finalmente, como por mudanças convenientes podemos procurar o valor de y do mesmo modo que o de x; pode applicar-se de dois modos o methodo de exclusão. Deve preferir-se aquelle para o qual w contém um menor numero de termos.

Se depois de empregarmos alguns excluentes desapparecerem de w todos os numeros segue-se que a proposta não admitte soluções.

33. *Theorema de Legendre sobre a possibilidade da resolução das equações indeterminadas do segundo gráo.*

Ve-se, que para poder resolver-se $Ax^2+By^2=z^2$ sendo $A>B$ é necessario determinar um numero $\alpha<\frac{1}{2}A$ de modo que $\frac{\gamma^2-B}{A}$ seja inteiro.

Formemos em seguida as equações

$$\alpha^2-B=A\,A'\,k^2 \qquad \alpha'=\mu\,A'\pm\gamma \qquad \alpha<\frac{1}{2}A'$$

$$\alpha'^2-B=A'\,A''\,k'^2 \qquad \alpha''=\mu'\,A''\pm\gamma' \qquad \alpha'<\frac{1}{2}A''$$

$$\alpha''^2-B=A''A'''k''^2 \qquad \alpha'''=\mu''A'''\pm\gamma'' \qquad \alpha''<\frac{1}{2}A'''$$

$$\ldots\ldots\ldots\ldots \qquad \ldots\ldots\ldots\ldots \qquad \ldots\ldots\ldots$$

Os termos A, A', A''.... são positivos e cada um menor do que $\frac{1}{4}$ do precedente; decrescerão portanto até $A^{(n)}$ ou $C<B$ e a proposta terá para transformadas successivas

$$\left.\begin{array}{l} A'x^2+By^2=z^2 \\ A''x^2+By^2=z^2 \\ \ldots\ldots\ldots\ldots \\ C\,x^2+By^2=z^2 \end{array}\right\}\ldots\ldots\ldots\ldots(30).$$

Estas equações acham-se relacionadas de modo que conhecendo as soluções d'uma d'ellas ficam conhecidas as de todas.

Para resolver a ultima das equações (30) é necessario achar um valor tal θ, que $\frac{\theta^2 - C}{B} = \text{int.}$ Teremos, satisfeita esta condição, uma nova serie de equações

$$Cx^2 + B'y^2 = z^2$$

$$Cx^2 + B''y^2 = z^2$$

$$\ldots\ldots\ldots\ldots$$

$$Cx^2 + Dy^2 = z^2$$

em que é $D < C$. E claro é que continuando a proceder analogamente havemos de chegar a um valor $D^{(n)} = 1$.

Vamos provar que não será necessario continuar no curso d'esta operação desde que para uma transformada

$$Ex^2 + Fy^2 = z^2$$

forem satisfeitas as condições $\frac{\beta^2 - F}{E} = \text{int.}$ $\frac{\gamma^2 - F}{E} = \text{int.}$

E, vamos ver, que basta que estas condições se verifiquem na equação proposta, e na sua primeira transformada para se darem em todas as equações.

Sejam as duas primeiras equações

$$Ax^2 + By^2 = z^2 \quad , \quad A'^2 + By^2 = z^2$$

e supponhamos que temos

$$\frac{\alpha^2 - B}{A} \quad , \quad \frac{\alpha'^2 - B}{A'} \quad , \quad \frac{\beta^2 - A}{B} \quad , \quad \frac{\beta'^2 - A'}{B} \ldots . (31)$$

sendo α, α', β, β' numeros inteiros taes que estas expressões tambem são numeros inteiros.

Seja θ um numero primo que divide B, será

$$\frac{\beta^2 - A}{\theta} = \text{int.} \quad , \quad \frac{\beta'^2 - A}{\theta} = \text{int.}$$

Procuremos um numero λ tal, que seja $\frac{\lambda^2 - A''}{\theta} = \text{int.}$, não ha difficuldade se A'' for divisivel por θ.

Supponhamos porém que θ não divide A'', temos dois casos a considerar segundo θ divide ou não A'.

1.° Será

$$\frac{Ak^2 - A''k'^2}{\theta} = \text{int.}$$

e por isso

$$\frac{\beta^2 k^2 - A''k'^2}{\theta} = \text{int.}$$

Mas k' é primo com B e portanto com θ, podemos pois fazer

$$k\beta = nk' - m\theta$$

do que resultará

$$\frac{n^2 - A''}{\theta} = \text{int.}$$

2.° Teremos

$$\frac{A''k'^2\beta'^2 - \alpha'^2}{\theta} = \text{int.},$$

e como β', k' e θ' são primos pode fazer-se $\alpha' = n\beta' k' - m\theta$ d'onde resulta

$$\frac{n^2 - A''}{\theta} = \text{int.}$$

Conseguintemente vê-se que não só é $\frac{\beta'' - A''}{B} = \text{int.}$, mas até

que é facil achar o valor de β'' á priori. E como já tinhamos $\frac{\alpha'^2 - B}{A''} = A'k^2$ conclue-se que com effeito as condições (31) têm logar na transformada

$$A''x^2 + By^2 = z^2.$$

Vejamos como no segundo systema de transformadas succede a mesma cousa.

Sejam

$$A_{(n-1)}x^2 + By^2 = z^2 \quad A_{(n)}x^2 + By^2 = z^2$$

as duas ultimas equações do primeiro systema, as quaes podemos suppor satisfazem ás condições $\frac{\alpha^2 - B}{A_{(n-1)}} = \text{int.}$, $\frac{\beta^2 - A_{(n-1)}}{B} = \text{int.}$, $\frac{\alpha'^2 - B}{A_{(n)}} = \text{int.}$, $\frac{\beta'^2 - A_{(n)}}{B} = B'f^2$, e seja

$$B'x^2 + A_{(n)}y^2 = z^2$$

a transformada seguinte do segundo systema.

Sendo θ um dos numeros primos que dividem A_n procuremos ψ de modo que seja $\frac{\psi^2 - B'}{\theta} = \text{int.}$ Se B' é divisivel por θ será ψ egual a um multiplo de θ. Se B' não é divisivel temos dois casos a considerar, correspondente a ser ou não θ um divisor de B.

No primeiro, attendendo a que é

$$\alpha^2 - B = A_n A_{n-1} k^2 \quad , \quad \beta^2 - A_n = BB'f^2$$

será θ um divisor de α e β', e portanto

$$B'^2 f^2 k^2 \beta^2 - B' = \text{int.} \times \theta \quad \text{ou} \quad \psi = B'fk\beta \quad \text{e} \quad \frac{\psi^2 - B'}{\theta} = \text{int.}$$

No segundo, teremos

$$\frac{\alpha^2 - B}{\theta} = \text{int.}, \quad \frac{\alpha^2 f^2 B' - BB'}{\theta} = \text{int.}, \quad \frac{\alpha^2 f^2 B' - \beta'^2}{\theta} = \text{int.},$$

e como pode suppor-se $\beta' = \alpha\psi f - m\theta$, segue-se que é

$$\frac{\psi^2 - B'}{\theta} = \text{int.}$$

Podendo fazer-se o mesmo raciocinio para todos os divisores primos de A_n, conclue-se que pode sempre satisfazer-se á condição $\frac{\psi^2 - B'}{A_n} = \text{int.}$

A condição $\frac{\psi^2 - A_n}{B} = \text{int.}$ é satisfeita por ser $\frac{\beta^2 - A_n}{B'} = Bf^2$.

Resulta portanto o theorema de Legendre.

A equação $Ax^2 + By^2 = z^2$ *pode resolver-se sendo satisfeitas as tres condições* $\frac{\alpha^2 - B}{A} = \text{int.}$, $\frac{\beta^2 - A}{B} = \text{int.}$, $\frac{\beta'^2 - A'}{B} = \text{int.}$ *A ultima é desnecessaria quando* A *e* B *forem primos entre si.*

Resolução das equações completas do segundo gráo entre duas variaveis.

34. *Methodo de Lagrange.* — Vimos que a equação do segundo gráo se reduzia á fórma (9) e conhecidos para esta os valores de t e u como se diz a pag. 48 os de x e y serão

$$x = \frac{\pm t - g}{A} \qquad y = \frac{\pm u - d - bt}{2a},$$

onde para que x e y sejam inteiros é necessario que $\pm t - g$ seja divisivel por A e $\pm u - d - bt$ o seja por $2a$.

Quando A for uma quantidade negativa ou um quadrado, ha um numero limitado de valores para t e u; se nenhum satisfizer á condição indicada a proposta é insoluvel.

Sendo A uma outra qualquer quantidade, notemos que as expressões x, y attendendo aos valores de t e z achado no n.° 25 são

$$y = \frac{\alpha t' + \beta u' + \gamma}{\delta} \quad , \quad x = \frac{\alpha' t' + \beta' u' + \gamma'}{\delta},$$

t' e u' sendo dados pelas formulas (20).

É necessario dar a m valores taes que y e x sejam inteiros.

Imaginemos para isso uma expressão composta de t, u e numeros inteiros, e que se procurava o expoente m de modo que fosse divisivel por um numero Δ.

Façamos $m = 1, 2, 3 \ldots$, M; sendo M o menor valor de m que torna $t - 1$ e u divisiveis por Δ. Se nenhum d'estes valores torna a proposta divisivel por Δ conclue-se que não pode tornar-se, qualquer que seja o valor de m.

Achando um ou muitos valores para m, a cada um corresponderia um systema de valores da forma $N + iM$.

Posto isto, achamo-nos habilitados para resolver o problema, sendo no nosso caso as expressões

$$\alpha t + \beta u + \gamma \quad , \quad \alpha' t + \beta' u + \gamma',$$

e os divisores δ e δ'

35. *Methodo de Legendre.* — Attendendo ao n.° 13 sabemos que as raizes de (8) são em funcção das raizes de (12)

$$y = \frac{t + 2cd - fb}{b^2 - 4ac} \quad , \quad x = \frac{u + 2af - db}{b^2 - 4ac}.$$

Estes valores mostram que no caso de ser $b^2 - 4ac = 0$ não é possivel a transformação indicada.

Se $b^2 - 4ac < 0$ ou é um quadrado o numero das soluções da transformada é limitado. É mais simples substituir os valores achados para t e u, e ver os que dão y e x inteiros.

Se $b^2 - 4ac > 0$, e não é um quadrado: sendo a equação proposta possivel a transformada terá uma infinidade de soluções, encerradas em um ou muitos systemas cada um da fórma

$$t = \gamma F + \delta G \quad , \quad u = \varepsilon F + \vartheta G$$

$$(\varphi + \psi \sqrt{b^2 - 4ac})^n = F + G \sqrt{b^2 - 4ac}.$$

Resta-nos achar para n valores taes que

$$y = \frac{\gamma F + \delta G + \alpha}{b^2 - 4ac} \quad \text{e} \quad \frac{\varepsilon F + \vartheta G + \beta}{b^2 - 4ac}$$

sejam numeros inteiros. Temos

$$F = \varphi^n + \frac{n(n-1)}{2} \varphi^{n-2} \psi^2 (b^2 - 4ac) + \ldots$$

$$G = n\varphi^{n-1}\psi + \frac{n(n-1)(n-2)}{1.2.3} \varphi^{n-3} \psi^3 (b^2 - 4ac) + \ldots$$

é por isso necessario que

$$\frac{\gamma \varphi^n + \delta n \varphi^{n-1} \psi + \alpha}{b^2 - 4ac}, \quad \text{e} \quad \frac{\varepsilon \varphi^n + \vartheta n \varphi^{n-1} \psi + \beta}{b^2 - 4ac}$$

sejam numeros inteiros.

No caso de ser $n = 2m$, será

$$\varphi - \psi^2 (b^2 - 4ac) = 1$$

e m depende das equações do primeiro gráo

$$\frac{(\alpha + \gamma)\psi + 2\delta\psi m}{b^2 - 4ac} = \text{int.} \quad , \quad \frac{(\beta + \varepsilon)\varphi + 2\vartheta\psi m}{b^2 - 4ac} = \text{int.}$$

as quaes devem concordar.

Sendo $n = 2m+1$, m dependerá das equações

$$\frac{\gamma\varphi+\alpha+(2m+1)\delta\psi}{b^2-4ac} = \text{int.} \quad , \quad \frac{\varepsilon\varphi+\beta+(2m+1)\theta\psi}{b^2-4ac} = \text{int.}$$

que tambem devem concordar entre si.

Determinado o valor de n d'esta maneira, será da fórma

$$\nu+(b^2-4ac)\,k$$

onde k é uma quantidade indeterminada, e teremos assim uma infinidade de soluções inteiras.

36. *Methodo de Gauss.* — Feita a sua transformação analoga á de Legendre: os valores das raizes da equação (8) são dados em funcção das raizes da transformada pelas formulas

$$x = \frac{p+cd-bc}{b^2-ac} \quad , \quad y = \frac{q+ac-bd}{b^2-ac}.$$

Em consequencia Gauss começa pelo estudo da representação de um numero M pela fórma

$$ap^2+2bpq+cq^2,$$

segundo os valores que pode ter o determinante d'esta expressão.

Notaremos só dois casos:

1.° Quando b^2-ac é um numero positivo não quadrado. Todas as representações de M são dadas pelas formulas

$$p = \frac{1}{m}(At+Bu) \quad , \quad q = \frac{1}{m}(Ct+Du)$$

onde A, B, C, D são numeros inteiros conhecidos, m é o menor divisor commum entre a, $2b$ e c; t e u numeros que satisfazem á equação

$$t^2-(b^2-ac)\,u^2 = m^2.$$

Como os valores de t e u podem ser tomados positivamente ou negativamente temos os quatro systemas:

$$\left.\begin{aligned} p &= \frac{1}{m}(At+Bu) \\ q &= \frac{1}{m}(Ct-Du) \end{aligned}\right\} \quad , \quad \left.\begin{aligned} p &= \frac{1}{m}(At-Bu) \\ q &= \frac{1}{m}(At+Du) \end{aligned}\right\}$$

$$\left.\begin{aligned} p &= \frac{1}{m}(-At+Bu) \\ q &= \frac{1}{m}(-Ct+Bu) \end{aligned}\right\} \quad , \quad \left.\begin{aligned} p &= -\frac{1}{m}(At+Bu) \\ q &= -\frac{1}{m}(Ct+Du) \end{aligned}\right\}$$

Vejamos quaes são os valores de t e u que dão para x e y valores inteiros.

O primeiro systema dá

$$x = \frac{At+Bu+mcd-mfe}{m(b^2-ac)} \quad , \quad y = \frac{et+Du+mae-mbd}{m(b^2-ac)}.$$

Os volores de t e u formam uma serie recurrente, e pode sempre achar-se para um dado valor M

$$t^{\mu} = t_0 + i\,M \quad , \quad t^{\mu+1} = t' + i_1\,M, \ldots .$$

$$u^{\mu} = u_0 + i'M \quad , \quad u^{\mu+1} = u' + i'_1\,M, \ldots .$$

Sendo pois $x^{(h)}$ $y^{(h)}$ numeros inteiros escolhendo convenientemente μ tambem serão inteiros os valores de $x^{h+\mu}$, $y^{h+2\mu}$; $x^{h+2\mu}$, $y^{h+2\mu}$; ... $x^{h+k\mu}$, $y^{h+k\mu}$.

Logo, se procurar-mos os valores de x, y desde x_0, y_0 até x^{n-1}, y^{n-1}, e nenhum for inteiro, não haverá raizes inteiras para

o primeiro systema

$$\left.\begin{aligned} p &= \frac{1}{m}(At + Bu) \\ q &= \frac{1}{m}(Ct + Du) \end{aligned}\right\} \ldots\ldots\ldots\ldots (32);$$

Se encontrarmos as raizes inteiras x^{ν}, y^{ν}; $x^{\nu'}$, $y^{\nu'}$, ... os valores inteiros dados pelas formulas (35) são os de x, y correspondentes aos acentos $\nu + k\mu$, $\nu' + k\mu$, k sendo um numero inteiro e positivo comprehendido nada.

Para os outros systemas havia a seguir-se o mesmo raciocinio.

2.° Quando $b^2 - ac = 0$; fazendo

$$\alpha x + \beta y = z \ldots\ldots\ldots\ldots\ldots (33)$$

teremos

$$x = \frac{\beta m z^2 + 2cz + \beta f}{a(\alpha e - \beta d)} \quad , \quad y = \frac{\alpha m z^2 + 2dz + \alpha f}{2(\alpha e - \beta d)}$$

valores que satisfazem a proposta, pondo de parte o caso em que é $\alpha e - \beta d = 0$ que depois consideraremos.

Vejamos quaes devam ser os valores de z para que os de x e y sejam inteiros.

A z só podem dar-se valores inteiros.

Substituindo em (33) por z todos os numeros inteiros desde 0 até $\pm 2(\alpha e - \beta d) - 1$, mais ou menos conforme for $\alpha e - \beta d$ positivo ou negativo: se nenhum der para x, y valores inteiros a proposta não admitte raizes inteiras. Supponhamos que satisfazem os valores δ, δ', ... Teremos todas as soluções tomando

$$z = 2(\alpha e - \beta d)k + \delta \quad , \quad z = 2(\alpha e - \beta d)k + \delta, \ldots; k = \text{int.}$$

Quando é $\alpha e - \beta d = 0$, a proposta tem a fórma

$$(m\alpha x + m\beta y + h)^2 - h^2 + mf.$$

E é portanto necessario que seja $h^2 - mf = k^2$

$$m\alpha x + m\beta y + h \pm k = 0$$

o que exige que seja $h \pm k$ divisivel por m.

Satisfeita esta condição immediatamente se encontrarão as raizes da equação dada.

EQUAÇÕES INDETERMINADAS DE GRÁO SUPERIOR AO SEGUNDO

Caso em que uma das incognitas não entra n'um gráo superior ao primeiro.

37. *Resolução d'Euler.* — Seja a equação

$$a + bx + cy + dx^2 + exy + fx^3 + gx^2y + hx^4 + hx^3y + \ldots = 0 \ldots (34).$$

Euler tira o valor de y e procura as condições a que deve satisfazer x, para que os termos que se apresentam no segundo membro sejam numeros inteiros.

Assim da equação

$$mxy = ax + by + c$$

tira-se

$$y = \frac{ax + c}{mx - b} \quad \text{ou} \quad y = \frac{mc + ab}{mx - b},$$

por onde se vê que $mx - b$ deve dividir $mc + ab$ que é um numero conhecido. Podendo-se em geral decompor $mc + ab$ pela fórma $mc + ab = fg$, teremos

$$mx - b = f \quad , \quad x = \frac{b + f}{m}.$$

E deduziremos em seguida os valores correspondentes de y.

38. *Resolução de Lagrange.* — De (34) tiramos

$$y = -\frac{a+bx+dx^2+fx^3+hx^4+\ldots}{c+ex+gx^2+\ldots}.$$

É necessario achar para x um valor tal que o numerador d'esta fracção seja divisivel pelo denominador.

Fazendo

$$a+bx+dx^2+\ldots = p \quad , \quad c+ex+gx^2+\ldots = q \ldots (35)$$

e eliminando x entre estas equações obteremos a equação final

$$A+Bp+Cq+Dp^2+Epq+Fq^2+Gp^3+\ldots = 0,$$

a qual, attendendo a que é $p = -qy$, se transforma em

$$A-Bqy+Cq+Dy^2q^2-Eq^2y+Fq^2+\ldots = 0.$$

Como q e y devem ser inteiros, segue-se que deve ser A divisivel por q.

Logo tomaremos para valores de q os divisores de A, e substituindo-os na segunda das equações (35) teremos outras tantas equações determinadas em x, das quaes achando as raizes inteiras e substituindo-as na primeira das citadas equações deduziremos os valores de p correspondentes.

Dos valores de p e q assim achados aproveitaremos aquelles de que o quociente é inteiro, fornecer-nos-hão os valores de y que, combinados com os valores de x a que correspondiam, serão as raizes da equação.

Resolução da equação mais geral entre duas variaveis.

39. *Theorema de Lagrange. — A resolução d'uma equação do segundo grão entre duas variaveis reduz-se á d'uma equação em que o termo constante é* ± 1.

Consideremos a equação

$$A_1 y^n + A_2 y^{n-1} z + A_2 y^{n-2} z^2 + \ldots + A_{n+1} z^n = \pm B.$$

Estando θ comprehendido entre $-\frac{1}{2}B$ e $+\frac{1}{2}B$, podemos fazer $y = \theta z + Bu$, e a equação acima transforma-se em

$$\pm 1 = \frac{(A_1 \theta^n + A_2 \theta^{n-1} + \ldots + A_{n+1})}{B} z^n +$$

$$+ (n A_1 \theta^{n-1} + (n-1) A_2 \theta^{n-2} + \ldots) z^{n-1} u +$$

$$+ \left(\frac{n(n-1)}{2} A_1 \theta^{n-2} + \frac{(n-1)(n-2)}{2} A_2 \theta^{n-3} + \ldots \right) B z^{n-2} u + \ldots.$$

Para que esta equação subsista é necessario que seja

$$\frac{A_1 \theta^n + A_2 \theta^{n-1} + \ldots + A_{n+1}}{B} = \text{int.}$$

Esta expressão determinar-nos-ha θ substituindo por esta quantidade os numeros comprehendidos entre $-\frac{B}{2}$ e $+\frac{B}{2}$.

Para cada valor obtido para θ teremos a resolver uma equação transformada

$$A'_1 z^n + A'_2 z^{n-1} u + A'_3 z^{n-2} u^2 + \ldots + A'_{n+1} u^n = \pm 1.$$

Cada systema de soluções d'esta ultima equação fornecer-nos-ha um systema para a proposta. E fica demonstrado o theorema.

40. *Resolução de Lagrange.* — Pela sua natureza vemos que

o problema se acha reduzido á determinação dos valores de z e u que tornam

$$A'_1 z^n + A'_2 z^{n-1} u + A'_3 z^{n-2} u^2 + \ldots + A'_{n+1} u^n$$

o menor numero inteiro.

Supponhamos para isso que

$$x - \alpha \ , \ x - \alpha' \ , \ x - \alpha'', \ldots$$

e $$(x - \beta)^2 + \gamma^2 \ , \ (x - \beta')^2 + \gamma'^2, \ldots$$

são os factores do primeiro e segundo gráo em que se decompõe a equação determinada

$$A'_1 x^n + A'_2 x^{n-1} + A'_3 x^{n-2} + \ldots + A'_{n+1} = 0$$

a proposta será

$$F(z,u) = A'_1 (z - \alpha u)(z - \alpha' u) \ldots [(z - \beta u)^2 + \gamma^2 u^2][(z - \beta' u)^2 + \gamma'^2 u^2] \ldots$$

Sejam p e q os valores que tornam esta funcção um minimo

$$F(p,q) = A'_1 (p - \alpha q)(p - \alpha' q) \ldots [(p - \beta q)^2 + \gamma^2 q^2][(p - \beta' q)^2 + \gamma'^2 q^2] \ldots$$

deve ser $$F(p,q) < F(z,u) \ldots\ldots\ldots\ldots (36).$$

Para que se verifique a condição (36) é necessario pelo menos que um dos factores de $F(p, q)$ seja menor do que o factor correspondente de $F(z, u)$.

Pode ser menor um factor real ou um factor imaginario.

Attendendo a estes dois casos vamos demonstrar o theorema seguinte:

A fracção $\frac{p}{q}$ *é sempre convergente para uma das quantidades* $\alpha, \alpha', \alpha'', \ldots; \beta, \beta', \beta'', \ldots$

Suppondo-se que é um dos factores reaes de $F(t, u)$ maior do que o correspondente de $F(p, q)$, teriamos

$$z - \alpha u > p - \alpha q:$$

$\frac{p}{q}$ seria uma fracção convergente para a raiz α.

Sendo um dos factores imaginarios de $F(z, u)$ maior do que o correspondente de $F(p, q)$, $(z-\beta u)^2+\gamma^2 u^2 > (p-\beta q)^2+\gamma^2\rho^2$, teriamos

$$z - \beta u > p - \beta q:$$

e seria $\frac{p}{q}$ uma fracção convergente para β.

Com effeito, tomemos $z = p_0$, $u = q_0$ e supponhamos $\frac{p_0}{q_0}$ a fracção antecedente a $\frac{p}{q}$: no primeiro caso é necessario que seja

$$\frac{p_0 - \alpha q_0}{p - \alpha q} < 1.$$

Se for

$$\frac{p_0 - \alpha q_0}{p - \alpha q} = -\delta \quad , \quad \alpha = \frac{p\delta + p_0}{q\delta + q_0},$$

sendo $\frac{p_0}{q_0}$ e $\frac{p}{q}$ duas fracções consecutivas convergentes para α, e δ o quociente completo correspondente á segunda.

Se for

$$\frac{p_0 - \alpha q_0}{p - \alpha q} = \delta \quad , \quad \alpha = \frac{p\delta - p_0}{q\delta - q_0}.$$

N'este caso, sendo $\delta > 2$, $\frac{p}{q}$ é uma fracção convergente para α; sendo < 2, $\frac{p}{q}$ não é uma fracção convergente para α mas tem um valor muito proximo d'esta raiz.

Continuando a raciocinar analogamente, resulta que em geral a fracção $\frac{p}{q}$, correspondente ao minimo da funcção proposta deve

estar comprehendida entre as fracções convergentes para uma das quantidades α, α', α'',... ou β, β', β'',....

Podiamos ainda notar que, se isto assim não succedesse, era necessario que se verificassem as condições seguintes:

Que $\frac{p_0 - \alpha q_0}{p - \alpha q}$, para uma determinada raiz α, fosse um valor comprehendido entre $+1$ e -1. Que todas as quantidades analogas

$$\frac{p_0 - \alpha' q}{p - \alpha' q} \quad , \quad \frac{p_0 - \alpha'' q_0}{p - \alpha'' q} \quad ,\ldots; \quad \frac{p_0 - \beta q_0}{p - \beta q} \quad , \quad \frac{p_0 - \beta' q_0}{p - \beta' q} ,\ldots.$$

relativamente ás outras raizes fossem menores do que 1.

Mas satisfeitas estas condições seria

$$\frac{F(p_0, q)_0}{F(p, q)} < 1$$

o que é contra a hypothese, logo fica demonstrado o theorema.

Em consequencia eis o caminho a seguir: — Desenvolver em fracção continua, successivamente cada uma das raizes reaes α, e egualmente cada uma das partes reaes β das raizes imaginarias.

Tomar em seguida por $\frac{p}{q}$ todas as fracções convergentes que resultam d'estas operações, e substituir os valores de p e q na proposta. Cada resultado no seu genero será um minimo, o menor é o procurado

Não terminaremos esta parte sem mencionar os trabalhos de grande importancia que sobre este assumpto foram publicados por José Ferreira Cangalhas, e Liouville.

Outros ha tambem dignos de menção. Ser-nos-hia impossivel referirmo-nos a todos. Notaremos porém que nenhum apresenta um methodo de resolução para equações completas de um gráo superior ao segundo.

SEGUNDA PARTE

CONSIDERAÇÕES GERAES

41. *Numeros congruos, modulo, congruencias.* — Quando a differença de dois numeros inteiros quaesquer é divisivel por um terceiro numero M que se suppõe sempre positivo, diz-se que os dois numeros são congruos segundo o numero M, a que se dá o nome de modulo.

A expressão analytica que representa esta operação é

$$A = B \pm \text{mult. } M$$

dá-se-lhe o nome de congruencia e segundo a notação de Gauss que primeiro comprehendeu a sua verdadeira importancia, e a quem principalmente são devidos os trabalhos apresentados n'esta parte, escreve-se debaixo da fórma

$$A \equiv B \,(\text{mod. } M).$$

A e B podem ser funcções racionaes e inteiras em que existam uma ou mais variaveis.

A B dá-se ainda o nome de residuo de A segundo o modulo M.

As equações, como se vê, são um caso particular das congruencias correspondentes a ser $M = 0$.

42. *Residuo minimo absoluto.* — Cada numero tem segundo o mesmo modulo uma infinidade de residuos, o mais pequeno chama-se residuo minimo.

Para cada numero existem dois residuos minimos, um positivo e outro negativo; o menor em valor absoluto é o residuo minimo absoluto. E como sendo um dos residuos minimos maior do que $\frac{M}{2}$ é o outro menor, conclue-se que:

Um numero tem sempre um residuo minimo absoluto menor do que $\frac{M}{2}$.

43. *Raizes das congruencias.* — Na resolução das congruencias trata-se de achar os valores de x que satisfazem á congruencia

$$f(x) \equiv 0 \pmod{M} \ldots\ldots\ldots\ldots (37)$$

em que $f(x)$ é um polynomio racional e inteiro e de que os coefficientes são numeros inteiros.

Como qualquer raiz x pode reduzir-se á fórma $x = a + iM$ segue-se que para cada raiz existe uma infinidade, equivalentes segundo o modulo M, e que podem deduzir-se d'uma qualquer, e por isso d'uma raiz menor do que M, que com certeza existe em qualquer dos systemas de raizes. Por isso o problema de resolução das congruencias reduz-se a determinar os valores de x menores que M, e é a estès valores que se dá o nome de raizes da congruencia (37).

44. *Uma congruencia pode sempre reduzir-se a ter os coefficientes menores do que* $\frac{M}{2}$. Com effeito, á congruencia (37) podemos substituir a congruencia equivalente

$$f(x) + MF(x) \equiv 0 \pmod{M}$$

e dar aos coefficientes de $F(x)$ valores convenientes para que todos os coefficientes da congruencia fiquem menores do que $\frac{M}{2}$.

45. *Classificação das equações de congruencia.* — As equações de congruencia classificam-se em relação ao numero de indeterminadas que encerram, e ao gráo mais elevado das potencias d'estas indeterminadas.

RESOLUÇÃO DAS CONGRUENCIAS DO PRIMEIRO GRÁO

Congruencias de primeira ordem.

46. *Resolução no caso em que o modulo é um numero primo.* — Ordinariamente faz-se a resolução das equações de congruencia por meio das equações indeterminadas.

A este methodo, que agora vamos seguir para a resolução das equações de congruencia, talvez se deva attribuir o pouco que se adiantou na sua resolução.

A fórma geral das congruencias de primeiro gráo e primeira ordem é

$$Ax + B \equiv A'x + B' \text{ (mod. M)}$$

que immediatamente se reduz á fórma mais simples

$$ax \equiv b \text{ (mod. M)} \ldots\ldots\ldots\ldots (38).$$

Esta expressão sabemos que significa: que o quociente da differença $ax - b$ por M é um numero inteiro, y por exemplo, e pode por isso dar-se-lhe a fórma d'uma equação indeterminada

$$ax - My = b$$

de que a resolução em numeros inteiros nos dará as raizes da congruencia proposta.

Só poderão obter-se os valores inteiros quando, supprimidos os factores communs, a e M forem numeros primos entre si.

Poderemos reduzir a e b aos seus residuos minimos segundo M sem com isso alterar os valores de x.

Attendendo ás formulas que resolvem as equações indeterminadas do primeiro grão a duas variaveis, a expressão dos valores de x que satisfazem á equação (38) é

$$x = (-1)^{\mu+1} b\, P_{\mu-1} + i\mathrm{M} \ldots\ldots\ldots (39)$$

representando μ o numero de quocientes que se obtem reduzindo $\frac{\mathrm{M}}{a}$ em fracção continua e $P_{\mu-1}$ o penultimo dos mediadores.

47. *Resolução no caso em que o modulo é um numero composto.* — Supponhamos

$$\mathrm{M} = p \cdot p_1 \cdot p_2 \ldots p_l.$$

Estabeleçamos a congruencia

$$ax \equiv b \,(\mathrm{mod.}\ p) \ldots\ldots\ldots\ldots\ldots (40).$$

Sendo θ uma raiz d'esta congruencia, os valores de x que satisfazem a proposta serão da fórma

$$x = \theta + px_1$$

e a congruencia (38) fazendo

$$\frac{a\theta - b}{p} = b_1$$

torna-se em

$$ax_1 \equiv b_1 \,(\mathrm{mod.}\ p_1 \cdot p_2 \ldots).$$

Estabeleceriamos agora a equação de congruencia

$$ax_1 \equiv b_1 \,(\mathrm{mod.}\ p_1)$$

e continuando a proceder analogamente vê-se que a resolução da congruencia em que o modulo é composto se reduz á das congruencias

$$ax \equiv b \pmod{p}$$

$$ax \equiv b_1 \pmod{p_1}$$

. . . . . .

$$ax \equiv b_{l-1} \pmod{p_1}$$

em que os modulos são numeros primos.

48. *As equações de congruencia do primeiro gráo e ordem só admittem uma raiz.* — Pela formula (39) vemos que a solução da congruencia (38) é dada pela da congruencia

$$x = (-1)^{\mu+1} b P_{\mu-1} \pmod{M} \quad \ldots\ldots\ldots (41)$$

ou $x = c \pmod{M}$

fazendo $(-1)^{\mu+1} b P_{\mu-1} = c.$

Como porém todos os numeros comprehendidos na fórma $c + iM$ são equivalentes segundo o modulo M, e existe entre elles um menor do que M, notando a definição que se deu de raizes d'uma congruencia, conhece-se a verdade do theorema.

49. *A resolução das equações de congruencia que estamos tratando reduz-se á d'uma equação de congruencia em que o segundo membro é egual a 1.* — Com effeito, suppondo na equação (38) $b = 1$ a expressão (41) reduz-se a

$$x = (-1)^{\mu+1} P_{\mu-1} \pmod{M}$$

por onde vemos que obteremos a raiz da equação geral multiplicando pelo segundo membro a raiz correspondente a termos supposto este segundo membro egual a 1.

50. Tendo de nos aproveitar adiante, vejamos a resolução do seguinte problema.

Achar a expressão dos valores de x que satisfazem as congruencias

$$x \equiv a \,(\text{mod. } M) \quad , \quad x \equiv b \,(\text{mod. } M_1) \quad , \quad x \equiv (\text{mod. } M_2), \ldots .$$

Da primeira tira-se

$$x = a + M\alpha$$

que, devendo satisfazer ás outras equações, dá

$$a + M\alpha = b \,(\text{mod. } M_1) \quad \text{ou} \quad M\alpha + (a - b) \equiv 0 \,(\text{mod. } M_1)$$

a qual pode escrever-se debaixo da fórma

$$\frac{M}{d}\alpha + \frac{a-b}{d} \equiv 0 \left(\text{mod. } \frac{M_1}{d}\right),$$

d maior divisor commum entre M e M_1, e sendo a sua raiz θ, será

$$\alpha = \theta + \frac{M_1}{d}\alpha_1$$

portanto

$$x = a + M\theta + \frac{MM_1}{d}\alpha_1 = a_1 + \frac{MM_1}{d}\alpha_1 \text{ pondo } a + M\theta = a_1.$$

Para este valor satisfazer á terceira equação era necessario que fosse

$$x = a_2 + \frac{MM_1M_2}{dd_1}\alpha_2.$$

E continuando assim successivamente, vê-se que no caso de não haver congruencia alguma impossivel o valor de x é

$$x = A + A'\alpha$$

sendo A' o menor multiplo commum de M, $M_1, \ldots$, e α uma indeterminada.

51. *Resolução d'um systema de equações de congruencia em numero egual ao das indeterminadas.* — Pelos methodos de eliminação entre equações lineares podemos sempre fazer depender a resolução do systema proposto da resolução d'um outro systema, em que as equações contêm uma só incognita, e que admittirão todas as soluções do systema proposto.

52. *Resolução das equações de congruencia de primeiro e de qualquer ordem.* — N'este caso o numero das raizes é illimitado.

Assim, suppondo que a congruencia dada é de ordem n

$$a_1x_1 + a_2x_2 + a_3x_3 + \ldots + a_nx_n \equiv a_{n+1} \text{ (mod. M)}$$

teremos

$$a_1x^1 \equiv a_{n+1} - a_1x_1 - a_2x_2 - a_3x_3 - \ldots - a_nx_n \text{ (mod. M)}$$

e sendo a_1 primo com M

$$x_1 = (-1)^{\mu+1}(a_{n+1} - a_1x_1 - a_2x_2 - a_3x_3 - \ldots - a_nx_n)P_{\mu-1} + i\text{M}.$$

CONGRUENCIAS FUNDAMENTAES DE PRIMEIRA ORDEM

53. *Congruencias fundamentaes. Sua resolução por tentativas.* — Dá-se o nome de congruencia fundamental de primeira ordem á congruencia binomia.

$$x^m \equiv a \text{ (mod. M)} \ldots\ldots\ldots\ldots (42)$$

onde sabemos que a pode sempre ser um numero menor do que M.

Como as raizes da equação (42) são numeros inferiores a M

que lhe satisfazem, vê-se que poderia empregar-se para as determinar um methodo de tentativas consistindo em formar as potencias m dos numeros inferiores a M e ver quaes d'estas potencias tinham o residuo a.

Não é methodo que possa empregar-se na pratica.

54. *Raizes primitivas.* — São assim chamadas as raizes que pelos residuos minimos das suas potencias successivas nos fornecem as raizes da equação. D'este modo, conhecida uma raiz primitiva, immediatamente ficam conhecidas todas as raizes.

A propriedade das raizes primitivas é não pertencerem a congruencias de que o gráo seja um submultiplo de m.

Se considerarmos a congruencia

$$x^{\varphi(M)} \equiv 1 \pmod{M}$$

em que $\varphi(M)$ designa todos os numeros primos com M e inferiores; são raizes primitivas os numeros que pertencem a $\varphi(M)$ segundo o modulo M. Só podem existir raizes primitivas nos casos de ser o modulo: um numero primo impar, o dobro d'uma potencia d'um numero primo impar ou egual a 4.

Não nos demoraremos n'esta parte apesar da sua importancia, resultando do que já dissemos que não existem methodos que nos possam dar em qualquer caso a solução completa d'estas equações.

Na algebra de Serret (vol. 2.°, pag. 47) encontra-se esta materia tratada com a maior clareza.

CONGRUENCIAS D'UM GRÁO QUALQUER

55. Relativamente a estas congruencias, para as quaes Wronski foi o primeiro que deu o methodo de resolução, existiam já theoremas importantes, alguns dos quaes aqui apresentaremos.

Uma congruencia não pode ter mais raizes do que unidades o gráo.

As raizes communs a muitas congruencias pertencem ao maior divisor commum dos seus primeiros membros.

Uma congruencia de que o modulo é primo pode sempre substituir-se por outra em que o coefficiente do primeiro termo é a unidade.

Dada uma congruencia em que o modulo é composto, achemos as raizes das congruencias em que tomemos para modulo cada um dos factores primos do modulo.

Designando por a as raizes correspondentes a um dos factores, por b, c, . . . as correspondentes aos outros, teremos as raizes da proposta achando os valores de x que satisfazem aos systemas da fórma

$$x \equiv a \,(\text{mod. } p) \quad , \quad x \equiv b \,(\text{mod. } p') \quad , \quad x \equiv c \,(\text{mod. } p'') \ldots$$

em que p, p', p'' . . . . são os factores primos de M.

TERCEIRA PARTE

CONSIDERAÇÕES GERAES

56. *A theoria dos numeros, e as equações de congruencia.* — A algebra divide-se em dois ramos fundamentaes. Um tem por objecto os modos individuaes da geração, e da comparação das quantidades numericas, outro os modos inversaes d'esta geração e comparação.

O primeiro é a *theoria*, o segundo a *technia*.

Cada um d'estes divide-se ainda em duas partes. Uma que tem por objecto os elementos necessarios das operações, outra a reunião d'estas operações elementares.

A primeira é a parte *elementar*, a segunda a *systematica*.

Cada uma tem duas divisões correspondentes a deverem as quantidades numericas ser consideradas debaixo do ponto de vista da sua geração, e comparação.

Na parte systematica da theoria ha, como dissemos, em vista reunir systematicamente os algorithmos elementares do que resultarão novas determinações e leis para a sua geração e comparação.

Imaginando que dois algorithmos primitivos concorrem para a geração d'uma quantidade, ou esta geração é dada indistinctamente por um ou outro d'estes algorithmos, ou esta geração é

operada pela influencia distincta d'um d'estes algorithmos sobre o outro.

Em geral é impossivel suppor que geram a mesma quantidade um ou outro dos algorithmos primitivos; não succede o mesmo com os algorithmos derivados.

Quando se dá o segundo modo de geração, como os algorithmos devem ser considerados distinctos, da sua reunião resulta uma diversidade systematica que pode manifestar-se das seguintes maneiras: — Pela influencia da sommação na geração das quantidades em que domina a graduação. Pela influencia da graduação na geração das quantidades em que domina a sommação. Ainda pela influencia reciproca da sommação e graduação na geração das quantidades em que domina um ou outro d'estes algorithmos.

O ultimo caso em que a influencia só pode dar-se sobre numeros gerados constitue a theoria dos numeros.

Em conclusão a theoria geral dos numeros tem em vista as leis particulares que devem dar-se para podermos considerar um numero como somma de numeros ou producto de factores; isto é, as leis que regem a possibilidade da existencia da relação

$$A + B = P \times Q \ldots\ldots\ldots\ldots\ldots (43).$$

Esta relação deve evidentemente estar sujeita a leis individuaes no caso de se exigir que se dê entre numeros inteiros.

Á relação (43) pode immediatamente dar-se a fórma de uma equação de congruencia.

57. *As equações de congruencia, e as equações indeterminadas.* — Na parte systematica da theoria algebrica tratam-se as equações de equivalencia dependentes da identidade systematica. Não é porém sobre os seus principios que repousa a resolução das equações indeterminadas. Fazem estas objecto d'uma parte da theoria dos numeros.

A sua resolução é dependente da resolução das equações de congruencia, as quaes correspondem a uma diversidade systematica que já vimos faz objecto da theoria dos numeros.

AS FUNCÇÕES ALEPHS

58. *Funcções alephs, sua construcção.* — Wronski deu o nome de funcções *alephs* ás funcções symetricas que resultam de elevar uma somma de n bases a uma potencia qualquer m, e egualar á unidade os coefficientes.

Sendo $a, b, c, \ldots, n$, as bases e $a+b+c+\ldots+n=\mathrm{N}$ Wronski designou-as por $\aleph\,[\mathrm{N}]^m$, o seu termo geral é

$$a^p b^q d^r, \ldots u^u \quad , \quad p+q+r+\ldots+u=m.$$

59. *Os mediadores e as funcções alephs.* — A resolução das equações indeterminadas e de congruencia vimos que dependiam das funcções a que se deu o nome de mediadores. Estas funcções só podem exprimir-se algebricamente por meio de certas bases dependentes dos quocientes da divisão de dois numeros.

Conhecidas as bases, a construcção immediata dos mediadores é

$$\mathrm{P}_\mu=\aleph\,[\mathrm{N}_\omega]^\mu.$$

Em consequencia os mediadores são funcções alephs dependentes de bases que só têm uma determinação arithmetica, e por isso não têm o caracter de universalidade das funcções algorithmicas.

60. *Construcção das funcções alephs de qualquer ordem, e em particular da segunda.* — Dados muitos systemas de bases.

$$a_1 \ , \ a_2 \ , \ a_3 \ , \ a_4 \ , \ \ldots.$$

$$b_1 \ , \ b_2 \ , \ b_3 \ , \ b_4 \ , \ \ldots.$$

$$c_1 \ , \ c_2 \ , \ c_3 \ , \ c_4 \ , \ \ldots.$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

as funcções *alephs* constroem-se do seguinte modo

$$\aleph^{(0)} = 1$$

$$\aleph^{(1)} = a_1 \aleph^{(0)}$$

$$\aleph^{(2)} = a_2 \aleph^{(1)} + b_1 \aleph^{(0)}$$

$$\aleph^{(3)} = a_3 \aleph^{(2)} + b_2 \aleph^{(1)} + c_1 \aleph^{(0)}$$

. . . . . .

Para as funcções *alephs* de segunda ordem, e em que as bases do segundo systema são eguaes á unidade teremos

$$\aleph^{(0)} = 1$$

$$\aleph^{(1)} = a_1 \aleph^{(0)}$$

$$\aleph^{(2)} = a_2 \aleph^{(1)} + \aleph^{(0)}$$

$$\aleph^{(3)} = a_3 \aleph^{(2)} + \aleph^{(1)}$$

. . . . . .

61. *Determinação das bases que entram no nosso caso nas funcções alephs.* — Sejam Q e R dois numeros que por divisões successivas dão os quocientes $a_1, a_2, \ldots a_\omega$ em que ω é o numero das divisões.

Para designar estas funcções *alephs* em que as bases resultam das divisões consecutivas em numero ω dos dois numeros Q e R, Wronski adopta a seguinte notação

$$\aleph \left[\frac{Q}{R}, \omega \right]^{(\mu)}$$

E por isso temos

$$\aleph\left[\frac{Q}{R}, \omega\right]^{(0)} = 1$$

$$\aleph\left[\frac{Q}{R}, \omega\right]^{(1)} = a_1 \aleph\left[\frac{Q}{R}, \omega\right]^{(0)}$$

$$\aleph\left[\frac{Q}{R}, \omega\right]^{(2)} = a_2 \aleph\left[\frac{Q}{R}, \omega\right]^{(1)} + \aleph\left[\frac{Q}{R}, \omega\right]^{(0)}$$

$$\aleph\left[\frac{Q}{R}, \omega\right]^{(3)} = a_3 \aleph\left[\frac{Q}{R}, \omega\right]^{(2)} + \aleph\left[\frac{Q}{R}, \omega\right]^{(1)}$$

.....

RESOLUÇÃO DAS CONGRUENCIAS DO PRIMEIRO GRÁO E PRIMEIRA ORDEM

62. Já vimos como estas equações se resolviam recorrendo ás equações indeterminadas; vamos ver como se póde effectuar esta resolução directamente.

Tomemos dois numeros M e N primos entre si, e reduzamos o seu quociente a fracção continua, calculando os mediadores P, Q, teremos a relação geral

$$P_{\mu-1} Q_\mu - P_\mu Q_{\mu-1} = (-1)^{\mu-1} \ldots\ldots\ldots (44).$$

Quando se toma $\mu = \omega$, sendo ω o numero dos quocientes é

$$P_\omega = M \quad , \quad Q_\omega = N$$

e a relação (44) torna-se em

$$P_{\omega-1} \cdot N - (-1)^{\omega-1} = M Q_{\omega-1}$$

que é identica com a congruencia

$$P_{\omega-1}.N-(-1)^{\omega-1}\equiv 0\ (\text{mod. } M)$$

ou $$(-1)^{\omega+1}P_{\omega-1}N-1\equiv 0\ (\text{mod. } M)$$

e ainda multiplicando por um numero qualquer O, teremos

$$(-1)^{\omega+1}P_{\omega-1}NO-O\equiv 0\ (\text{mod. } M).$$

Fazendo $$x=(-1)^{\omega+1}OP_{\omega-1}+iM\ldots\ldots\ldots(45)$$

fica $$Nx-O\equiv 0 \quad \text{ou} \quad Nx\equiv O\ (\text{mod. } M)\ldots\ldots(46)$$

por onde se vê que o valor (45) é a solução da equação de congruencia (46).

63. Em virtude do que dissemos nos n.^{os} 59 e 61 conclue-se que a fórma geral das raizes da congruencia

$$Nx\equiv O\ (\text{mod. } M)$$

é $$x=(-1)^{\omega+1}O\aleph\left[\frac{M}{N},\ \omega\right]^{(\omega-1)}+iM\ldots\ldots(47).$$

Torna-se conveniente introduzir na funcção aleph o numero ω porque tambem existe fóra.

A congruencia de condição que acima se estabeleceu toma a fórma

$$(-1)^{\omega+1}N.\aleph\left[\frac{M}{N},\ \omega\right]^{(\omega-1)}-1\equiv 0\ (\text{mod. } M)\ldots(48).$$

RESOLUÇÃO DAS CONGRUENCIAS FUNDAMENTAES

64. *As leis de Wronski para a resolução da congruencia fundamental.* — Como temos dito, Wronski foi quem descobriu as leis que seguem na sua determinação as quantidades a a, x e M que entram na construcção da congruencia fundamental

$$x^m \equiv a \,(\text{mod. M}) \ldots\ldots\ldots\ldots (49).$$

Wronski observando que para um dado expoente m e para um modulo M pode haver differentes raizes e differentes residuos não congruentes, introduz para o estabelecimento das leis, dois numeros k e h dos quaes depende esta multiplicidade de residuos e raizes; chamando a k o indice do *genero*, e a h o indice da *especie* de cada residuo determinado e da sua raiz correspondente.

As expressões que sem mais considerações apresenta Wronski como sendo as leis que seguem na sua determinação reciproca as quatro quantidades a, x, m e M são

$$a = (-1)^{\omega+1} \cdot \left\{h\,(1^{k|1})^2 + (-1)^{k|1}\right\}^m \cdot \aleph\left[\frac{\text{M}}{(1^{k|1})^2},\ \omega\right]^{(\omega-1)} + \text{M}j \quad (50)$$

$$x = h + (-1)^{\pi+k} \cdot \aleph\left[\frac{\text{M}}{(1^{k|1})^2},\ \pi\right]^{(\pi-1)} + \text{M}i \ldots\ldots\ldots\ldots (51)$$

$$\text{M} = \text{fact.}\left[a\,(1^{k|1})^{2m} - \left\{h\,.\,(1^{k|1})^2 + (-1)^{k+1}\right\}^m\right] \ldots\ldots\ldots (52)$$

(*Messianismo*, pag. 81).

Vamos ver primeiro por que considerações Bukaty (Déduction et démonstration de trois lois prìmordiales de la congruence des nombres) chegou ao estabelecimento d'estas leis, e depois mostraremos como tambem se podem obter, reduzindo ás equações do primeiro gráo a solução da equação fundamental.

65. *Deducção das leis* (50), (51), (52), *por Bukaty.* — Procurando-se a relação entre o modulo, a raiz e o residuo, é claro que antes de tudo é necessario determinar a composição do modulo M. Para essa composição os elementos mais simples são os que resultam de multiplicar consecutivamente os numeros 1, 2, 3,. . , o que constitue as factoriaes $1^{k|1}$ em que k é o numero dos foctores.

Vejamos como exprimir M em funcção de $1^{k|1}$. Para isso notemos que para termos os differentes residuos de $\frac{M}{1^{k|1}}$ basta tomar para k, no caso do modulo ser um numero primo, metade depois de diminuido d'uma unidade ou geralmente metade do seu mais pequeno factor primo depois de egualmente diminuido; no denominador substituiremos o quadrado da factorial para não termos residuos de signaes contrarios.

Posto isto, como sabemos que nas fracções integrantes de $\frac{M}{(1^{k|1})^2}$ transformada em fracção continua, as differenças dos numeradores é sempre 1; teremos, achando a differença das duas ultimas fracções integrantes

$$(1^{k|1})^2 . \aleph\left[\frac{M}{(1^{k|1})^2}, \omega\right]^{(\omega-1)} - 1 = iM$$

ou

$$(1^{k|1})^2 . \aleph\left[\frac{M}{(1^{k|1})^2}, \pi\right]^{(\pi-1)} \equiv 1 \pmod{M}$$

e egualmente

$$(1^{k|1})^{2m} . \aleph\left[\frac{M}{(1^{k|1})^{2m}}, \omega\right]^{(\omega-1)} \equiv 1 \pmod{M}$$

que combinadas nos dão a congruencia final

$$\left\{\aleph\left[\frac{M}{(1^{k|1})^2}, \omega\right]^{\omega-1}\right\}^m \equiv \aleph\left[\frac{M}{(1^{k|1})^{2m}}, \omega\right]^{(\omega-1)} \pmod{M}$$

e por isso

$$x = \aleph\left[\frac{M}{(1^{k|1})^2},\ \pi\right]^{(\pi-1)} + Mi$$

$$a = \aleph\left[\frac{M}{(1^{k|1})^{2m}},\ \omega\right]^{(\omega-1)} + Mj.$$

O expoente k constitue o *genero* da congruencia, e a cada genero do residuo e da raiz pode juntar-se o seu complemento o que constitue a *especie* h, a qual portanto varia entre 0 e M.

É a combinação d'estes dois elementos que reduz ao minimo as operações a executar.

Nas expressões que atraz deduzimos para x e a havia ainda que attender aos signaes que dependem do indice e do genero, em razão d'esta circumstancia e de podermos completar a raiz do genero k até ao modulo M, teremos para x a seguinte expressão que é a lei (51)

$$x = h + (-1)^{\pi+k} \cdot \aleph\left[\frac{M}{(1^{k|1})^2},\ \pi\right]^{(\pi-1)} + Mi.$$

Em virtude da influencia da especie h para que a expressão do residuo possa satisfazer com toda a generalidade, acha-se facilmente que deve ser a da lei (50)

$$a = (-1)^{\omega+1}\left\{h(1^{k|1})^2 + (-1)^{k+1}\right\}^m \cdot \aleph\left[\frac{M}{(1^{k|1})^{2m}},\ \omega\right]^{(\omega-1)}.$$

Quanto ao modulo como é

$$(1^{k|1})^{2m} \cdot \aleph\left[\frac{M}{(1^{k|1})^{2m}},\ \pi\right]^{(\pi-1)} \equiv 1 \pmod{M}$$

deve ser

$$(-1)^{\pi+1} \cdot \left\{h(1^{k|1})^2 + (-1)^{k+1}\right\}^m \cdot (1^{k|1})^{2m} \cdot \aleph\left[\frac{M}{(1^{k|1})^{2m}},\ \pi\right]^{(\pi-1)}$$

$$\equiv \left\{h(1^{k|1})^2 + (-1)^{k+1}\right\}^m \pmod{M}$$

e por isso

$$\mathrm{M}i = a\,(1^{k|1})^{2m} - \left\{ h\,(1^{k|1})^2 + (-1)^{k+1} \right\}^m$$

d'onde resulta a lei (52)

$$\mathrm{M} = \text{fact.} \left\{ a\,(1^{k|1})^{2m} - \left[h\,(1^{k|1})^2 + (-1)^{k+1} \right]^m \right\}$$

66. *Deducção das leis que regem a congruencia fundamental, reduzindo-a á congruencia de primeira ordem.* — Supponhamos P um numero primo com M; a congruencia fundamental decompõe-se nas duas

$$\mathrm{P}x \equiv 1 \pmod{\mathrm{M}} \quad , \quad \mathrm{P}^m a \equiv 1 \pmod{\mathrm{M}}$$

d'onde

$$x = (-1)^{\pi+1} \cdot \aleph \left[\frac{\mathrm{M}}{\mathrm{P}},\ \pi \right]^{(\pi-1)} + \mathrm{M}i$$

$$a = (-1)^{\omega+1} \cdot \aleph \left[\frac{\mathrm{M}}{\mathrm{P}^m},\ \omega \right]^{(\omega-1)} + \mathrm{M}j$$

Mudando x em $x - h$, a primeira congruencia torna-se em

$$\mathrm{P}x \equiv \mathrm{P}h + 1 \quad \text{ou} \quad \frac{\mathrm{P}x}{\mathrm{P}h+1} \equiv 1 \pmod{\mathrm{M}}$$

e o valor de x em

$$x = h + (-1)^{\pi+1} \cdot \aleph \left[\frac{\mathrm{M}}{\mathrm{P}},\ \pi \right]^{(\pi-1)} + \mathrm{M}i.$$

Como a segunda equação se transformava em

$$\frac{\mathrm{P}^m}{(\mathrm{P}h+1)^m} \equiv 1 \pmod{\mathrm{M}} \ldots\ldots\ldots\ldots (53)$$

segue-se que o valor de a é

$$a = (-1)^{\omega+1} (\mathrm{P}h+1)^m \aleph \left[\frac{\mathrm{M}}{\mathrm{P}},\ \omega \right]^{(\omega-1)} + \mathrm{M}j.$$

Para cada valor de P teremos uma serie de expressões dando a h os valores desde $h=0$ até $h=\mathrm{M}$.

Quanto ao valor de M, tiramos de (53)

$$\mathrm{M}=\frac{1}{i}\left[\mathrm{P}^m a-(\mathrm{P}h+1)^m\right].$$

Fazendo agora $\mathrm{P}=(1^{k|1})^2$ immediatamente se transformam as expressões que acabamos de deduzir nas leis de Wronski.

67. *Verificação das leis* (50), (51) e (52). — Substituindo na terceira lei o valor de a dado pela primeira e fazendo

$$\Xi=\left[h\,(1^{k|1})^2+(-1)^{k+1}\right]^m$$

resulta

$$\mathrm{M}=(-1)^{\omega+1}\,.\,\Xi\,.\,\aleph\left[\frac{\mathrm{M}}{(1^{k|1})^{2m}},\ \omega\right]^{(\omega-1)}.\,(1^{k|1})^{2m}-\Xi+\mathrm{M}j$$

logo

$$(-1)^{\omega+1}(1^{k|1})^{2m}\,.\,\aleph\left[\frac{\mathrm{M}}{(1^{k|1})^{2m}},\ \omega\right]^{(\omega-1)}+1\equiv 0\ (\mathrm{mod.\ M}).$$

Esta congruencia analoga á congruencia condicional (48) das funcções *alephs teleologicas* serve de verificação ás leis indicadas.

68. As leis teleologicas mostram-nos os problemas que ha a tractar, e que se resumem em dois.

Dado um modulo e um gráo determinado achar todos os residuos e raizes correspondentes.

Dado o residuo e o gráo achar o modulo.

A construcção de x sendo independente de m mostra que as raizes calculadas servem geralmente nos seus generos e respectivas especies, para as congruencias de todos os gráos.

69. *Condições de possibilidade da congruencia fundamental.*

Seja a congruencia

$$x^m\equiv a\ (\mathrm{mod.}\ p)$$

em que p é um numero primo. Esta congruencia será ou não possivel segundo a for ou não residuo em relação a p.

Se considerarmos a congruencia

$$x^{m(p-1)} \equiv a^{p-1} \pmod{p}$$

sabemos que tem logar quando x e a são congruos com p: mas sendo α o maior divisor commum entre $p-1$ e m podemos pôr

$$[(x^{(p-1)})^{\beta}]^{\alpha} \equiv \left(q^{\frac{p-1}{\alpha}}\right)^{\alpha} \pmod{p},$$

e como é sempre

$$[x^{(p-1)}]^{\beta} \equiv 1 \pmod{p}$$

segue-se que tem egualmente logar a congruencia

$$\left(a^{\frac{p-1}{\alpha}}\right)^{\alpha} - (1)^{\alpha} \equiv 0 \pmod{p}$$

que envolve a existencia da congruencia

$$\left(a^{\frac{p-1}{\alpha}} - 1\right) . \aleph \left[a^{\frac{p-1}{\alpha}} + 1\right]^{(\alpha-1)} \equiv 0 \pmod{p}.$$

Esta ultima divide-se nas duas

$$a^{\frac{p-1}{\alpha}} - 1 \equiv 0 \pmod{p} \quad , \quad \aleph \left[a^{\frac{p-1}{\alpha}} + 1\right]^{(\alpha-1)} \equiv 0 \pmod{p},$$

e vemos que para ter logar a congruencia dada é necessario que seja

$$\aleph \left[a^{\frac{p-1}{\alpha}} + 1\right]^{(\alpha-1)} \equiv 0 \pmod{p}.$$

Attenta a dependencia que existe entre as congruencias de que os modulos são numeros compostos e aquellas em que são numeros primos, segue-se que está, a questão tractada qualquer que seja o modulo.

70. *Determinação das raizes.* — Vejamos o caminho a seguir para a determinação directa das raizes x.

Da primeira lei tira-se

$$x = h + (-1)^{\pi+k} \cdot \aleph\left[\frac{M}{(1^{k|1})^1}, \pi\right]^{(\pi-1)} + Mi.$$

Fazendo $$N = \aleph\left[\frac{M}{(1^{k|1})^{2m}}, \omega\right]^{(\omega-1)}$$

a geração do residuo torna-se em

$$a = (-1)^{\omega+1} N \cdot \Xi + Mj$$

ou $$(-1)^{\omega} a + N \cdot \Xi \equiv 0 \pmod{M}$$

que é a fórma das congruencias do primeiro gráo e por isso

$$\Xi = (-1)^{\omega+\rho} \cdot a \cdot \aleph\left[\frac{M}{N}, \rho\right]^{(\rho-1)} + Mj \ldots\ldots (54)$$

expressão que nos fará conhecer Ξ para um dado valor de k.

Se o valor resultante for uma potencia do gráo m

$$\Xi = R_1^m + Mj$$

attendendo ao valor de Ξ, teremos

$$R_1 \equiv [h\,(1^{k|1})^2 +] \pmod{M}$$

congruencia do primeiro gráo em h, d'onde deduzimos

$$h = (-1)^{\pi+1} \cdot [R_1 + (-1)^k] \cdot \aleph\left[\frac{M}{(1^{k|1})^2}, \pi\right]^{(\pi-1)} + Mj$$

e $$x = (-1)^{\pi+1} \cdot R_1 \cdot \aleph\left[\frac{M}{(1^{k|1})^2}, \pi\right]^{(\pi-1)} + Mi \ldots (55),$$

Porém, se dando a j um valor conveniente a expressão (54) não nos der para Ξ uma potencia m, em todo o caso o valor achado será o residuo exacto d'uma potencia do gráo m em relação ao modulo M e teremos

$$R_1^m \equiv \Xi \,(\text{mod. } M).$$

Congruencia que tem de ser tratada analogamente.

Obtendo-se para R_1 um valor que seja uma potencia do gráo m

$$R_1 = R_2^m + M i$$

teremos em virtude de (58)

$$R_1 = (-1)^{\pi+1} \cdot R_2 \aleph \left[\frac{M}{(1^{k|1})^2}, \pi \right]^{(\pi-1)} + M i$$

e $$x = R_2 \left\{ (-1)^{\pi+1} \cdot \aleph \left[\frac{M}{(1^{k|1})^2}, \pi \right]^{(\pi-1)} \right\}^2 + M i.$$

Se ainda R_1 não fosse uma potencia exacta do gráo m continuariamos do mesmo modo até chegarmos a um residuo R_μ^m que o fosse, e a expressão da raiz seria

$$x = R_\mu \left\{ (-1)^{\pi+1} \cdot \aleph \left[\frac{M}{(1^{k|1})^1}, \pi \right]^{(\pi-1)} \right\}^\mu + M i.$$

E attendendo a que a expressão geradora de R_μ era

$$R_\mu = a \left\{ (-1)^{\omega+\rho} \cdot \aleph \left[\frac{M}{N}, \rho \right]^{(\rho-1)} \right\}^\mu + M j$$

teremos

$$x = \left\{ a \left((-1)^{\omega+\rho} \cdot \aleph \left[\frac{M}{N}, \rho \right]^{(\rho-1)} \right)^{\mu} + Mj \right\}^{\frac{1}{m}} \times$$

$$\times \left\{ (-1)^{\pi+1} \cdot \left[\frac{M}{(1^{k|1})^2}, \pi \right]^{(\pi-1)} \right\}^{\mu} + Mi.$$

Esta expressão pode ainda tomar outra fórma, conveniente pela simplificação que introduz.

Com effeito, sendo

$$N = \aleph \left[\frac{M}{(1^{k|1})^2}, \omega \right]^{(\omega-1)}$$

é raiz da congruencia elementar

$$N (1^{k|1})^{2m} \equiv (-1)^{\omega+1} \pmod{M}$$

que resolvida em ordem a $(1^{k|1})^{2m}$, dá

$$(1^{k|1})^{2m} = (-1)^{\omega+\rho} \cdot \aleph \left[\frac{M}{N}, \rho \right] + Mj$$

e portanto

$$x = \left[a (1^{k|1})^{2m} \cdot \mu \right]^{\frac{1}{m}} \cdot \left\{ (-1)^{\omega+1} \cdot \aleph \left[\frac{M}{(1^{k|1})^2}, \omega \right]^{(\omega-1)} \right\}^{\mu} + Mi.$$

71. Vejamos agora como de facto a expressão acima nos offerece a solução completa do problema.

Elevando a potencia m, resulta

$$x^m = \left[a (1^{k|1})^{2m} \cdot \mu + Mj \right] \left\{ (-1)^{\omega+1} \cdot \aleph \left[\frac{M}{(1^{k|1})^2}, \omega \right]^{(\omega-1)} \right\}^{\mu.m} \quad (56)$$

ou

$$x^m \equiv a \left\{(-1)^{\omega+1} \cdot (1^{k|1})^2 \cdot \aleph\left[\frac{M}{(1^{k|1})^2}, \omega\right]^{(\omega-1)}\right\}^{m \cdot \mu}$$

e como temos a congruencia fundamental

$$(-1)^{\omega+1} \cdot (1^{k|1})^2 \cdot \aleph\left[\frac{M}{(1^{k|1})^2}, \omega\right]^{(\omega-1)} \equiv 1 \pmod{M}$$

fica $x^m \equiv a \cdot 1^{m \cdot \mu}$ ou $x^m \equiv a \pmod{M}$

que prova o que tinhamos dito.

Pelo methodo que se empregou para resolver a congruencia fundamental, vê-se que ha uma difficuldade a resolver.

Tendo de calcular-se os residuos successivos Ξ_1, Ξ_2, ... para um genero k, pode succeder que antes de chegarmos a um que seja uma potencia exacta do gráo m se reproduza um residuo já achado e por isso se reproduzam todos periodicamente, não se obtendo aquelle que deve empregar-se.

N'este caso recorreremos a outro genero k, e procederemos identicamente até empregarmos um genero que levante a difficuldade. D'esta maneira passaremos por todos os residuos possiveis, entre os quaes se encontram as potencias exactas do gráo m, e resolver-se-ha o problema.

No caso de serem k_1, k_2, ... os differentes generos, formemos as exppessões

$$N_\nu = \aleph\left[\frac{M}{(1^{k_\nu|1})^{2m}}, \omega_\nu\right]^{(\omega_\nu-1)}, \quad P_\nu = (-1)^{\pi_\nu+\rho_\nu} \cdot \aleph\left[\frac{M}{N_\nu}, \rho_\nu\right]^{(\rho_\nu-1)}$$

e $$Q_\nu = (-1)^{\pi_\nu+1} \cdot \aleph\left[\frac{M}{(1^{k_\nu|1})^2}, \pi_\nu\right]^{(\pi_\nu-1)}$$

o valor geral de x é

$$x = [a(P_1^{\mu_1} \cdot P_2^{\mu_2} \ldots .) + Mj]^{\frac{1}{m}} \cdot [Q_1^{\mu_1} \cdot Q_2^{\mu_2} \ldots .] + Mi \ldots . (57).$$

D'esta expressão é (55) um caso particular correspondente a ter ν um só valor.

72. Esta expressão de x satisfaz ao problema como vamos ver.

Attendendo ao valor que achamos para $(1^{k|1})^{2m}$, vemos que é egual ao de P, isto é,

$$P_\nu = (1^{k_\nu|1})^{2m}$$

e portanto teremos

$$x = \left\{a\left[(1^{k_1|1})^{2m\,.\,\mu_1}(1^{k_2|1})^{2m\,.\,\mu_2}\ldots\right]+Mi\right\}^{\frac{1}{m}}\times\left[Q_1 1^{\mu_1}.Q_2 1^{\mu_2}\ldots\right]+Mi.$$

Elevando este valor á potencia m

$$x^m = a\,(1^{k_1|1})^{2m\,.\,\mu_1}\,(1^{k_2|1})^{2m\,.\,\mu_2}\ldots\times$$

$$\times\left\{(-1)^{(\pi_1+1)\mu_1}(-1)^{(\pi_2+1)\mu_2}\ldots\aleph\left[\frac{M}{(1^{k_1|1})^2},\ \pi_1\right]^{(\pi_1-1)\mu_1}\times\right.$$

$$\left.\times\aleph\left[\frac{M}{(1^{k_2|1})^2},\ \pi_2\right]^{(\pi_2-1)\mu_2}\ldots\right\}^m+Mi$$

logo $$x^m = a\,(1)^{m\,.\,\mu}\ldots+Mi.$$

Este valor substituido em $x^m - a$ dá

$$x^m - a = a\,(1^{m\,.\,\mu_1}\,.\,1^{m\,.\,\mu_2}\ldots-1)+Mi' = 0+Mi$$

e mostra que satisfaz.

73. Para que os valores de x sejam quantidades racionaes é necessario que na expressão (56) a quantidade do que está entre parentheses seja uma potencia exacta do gráo m, e por isso que seja

$$z^m = a\,[(1^{k|1})^{2\mu}]^m+Mi$$

ou em geral

$$z^m = a\,[(1^{k_1|1})^{2\mu_1}\,.\,(1^{k_2|1})^{2\mu_2}\,.\,.\,.]^m + \mathrm{M}i$$

sendo z um numero inteiro.

Mas para satisfazermos a esta condição, egualando a y a quantidade que está entre parentheses obtem-se a congruencia de segunda ordem

$$z^m = ay^m \text{ (mod. M)}$$

que se resolve pelas de primeira ordem.

Por consequencia não podem determinar-se á priori as condições para que sejam inteiras as soluções.

Em todo o caso ha a certeza de que esta condição é satisfeita, e não é difficil a verificação á posteriori.

74. *Resolução directa e methodica.* — Fazendo $\mathrm{T}_\mu = a\mathrm{P}^\mu + \mathrm{M}i$, isto é, chamando T_μ ao residuo segundo M de P_μ, usar-se-ha da quantidade i unicamente para tornar T_μ e R_μ menores do que M. A expressão de x torna-se em

$$x = [\mathrm{T}_\mu]^{\frac{1}{m}}\left\{(-1)^{\pi+1}\,.\,\aleph\left[\frac{\mathrm{M}}{(1^{k|1})^2},\ \pi\right]^{(\pi-1)\mu} + \mathrm{M}i\right.$$

$$\left(x = (-1)^{\pi+1}\,.\left[\mathrm{T}_{1_{\mu_1}}\,.\,\mathrm{T}_{2_{\mu_2}}\,.\,.\,.\,\mathrm{T}_{\rho_{\mu_\rho}}\right]\times\right.$$

$$\left.\times\,\aleph\left[\frac{\mathrm{M}}{a^\rho - 1},\ \pi\right]^{(\pi-1)} + \mathrm{M}j\right)^{\frac{1}{m}}\,.\left[\mathrm{Q}_{\mu_1}\,\mathrm{Q}_{\mu_2}\,.\,.\,\mathrm{Q}_{\mu_\rho}\right] + \mathrm{M}i$$

que se reduz á antecedente fazendo $\rho = 1$.

Resta-nos ver o meio methodico de formar as quantidades P, Q ou T, Q.

Sendo $\mathrm{P}^\mu \equiv \mathrm{R}_\mu \text{ (mod. M)}$, $\mathrm{Q}_\mu \equiv \mathrm{S}_\mu \text{ (mod. M)}$

teremos $\mathrm{R}_{\mu-\nu} \equiv \mathrm{R}_\mu\,.\,\mathrm{R}_\nu$, $\mathrm{S}_{\mu+\nu} \equiv \mathrm{S}_\mu\,.\,\mathrm{S}_\nu \text{ (mod. M)}$.

Para T_ν teremos em geral

$$a^2 P^{\mu+\nu} \equiv T_\mu . T_\nu \pmod{M}$$

ou $$a T_{\mu+\nu} \equiv T_\mu . T_\nu \pmod{M},$$

e por isso

$$T_{\mu+\nu} = (-1)^{\pi+1} . T_\mu . T_\nu . \aleph\left[\frac{M}{a}, \pi\right]^{(\pi-1)} + M i.$$

Quanto á formação dos residuos progressivos, teremos

$$T_{\mu+1} = a P^{\mu+1} = (a P^\mu) P = T_\mu . P = T_\mu . R_1 + M i$$

de modo que basta multiplicar o residuo antecedente por P, ou pelo seu residuo minimo.

Em se obtendo um residuo T_μ que seja uma potencia exacta do grão m, teremos o valor de μ que tem de servir para calcular o segundo factor ou o seu residuo minimo; isto effectua-se do mesmo modo calculando os residuos successivos até μ.

35. *Methodo geral de exclusão para a resolução das congruencias fundamentaes.* — Formando as expressões

$$N = \aleph\left[\frac{M}{(1^{k|1})^{2m}}, \omega\right]^{(\omega-1)} . \Xi = [h (1^{k|1})^2 + (-1)^{k+1}]^m$$

pela geração do residuo, temos

$$\Xi = -\frac{a + M i}{N (-1)^\omega}.$$

Chamando a' um residuo do mesmo genero k em relação a M': teremos

$$\Xi = -\frac{a' + M' j}{N' (-1)^{\omega'}}.$$

D'onde resulta

$$a\,N'(-1)^{\omega'} - a'\,N(-1)^{\omega} \equiv M'N(-1)^{\omega} j - MN'(-1)^{\omega'} i$$

e por meio da congruencia a que se reduz, tira-se

$$i \equiv [aN' - a'N(-1)^{\omega-\omega'}] \cdot \aleph\left[\frac{M'N}{M \cdot N'}, \sigma\right]^{(\sigma-1)} + M'Nj \ldots (58).$$

Vê-se portanto que para resolver por tentativas a congruencia fundamental de primeira ordem, teremos a substituir por i em $x^m \equiv a + Mi$ os numeros inteiros dados por (58), no caso em que a' não é o residuo que em relação a M' corresponde ao genero k.

RESOLUÇÃO DAS CONGRUENCIAS FUNDAMENTAES DO GRÁO n E DE SEGUNDA ORDEM

76. Seja a congruencia

$$z^n - ay^n \equiv 0 \pmod{M}.$$

Pondo $z \equiv xy$ fica

$$x^n y^n - ay^n \equiv 0 \pmod{M}$$

ou

$$x^n - a \equiv 0 \pmod{M}.$$

D'este modo a congruencia proposta acha-se reduzida á congruencia fundamental binomia de primeira ordem, suppondo y um numero arbitrario não congruo com M, teremos

$$M \equiv \text{fact.} \left\{a\,(1^{k|1})^{2n} - [h\,(1^{k|1})^2 + (-1)^{k+1}]^n\right\}$$

$$y \equiv azb$$

$$z \equiv y\left\{h + (-1)^{\pi+k} \cdot \aleph\left[\frac{M}{(1^{k|1})^2}, \pi\right]^{(\pi-1)} + Mj\right\}.$$

A solução que procuramos é a que nos dá valores imdependentes para z e y.

Ora, como já fizemos

$$N = (-1)^{\pi+1} \cdot \aleph \left[\frac{M}{(1^{k|1})^{2m}}, \omega \right]^{(\omega-1)}$$

a expressão do residuo é

$$a = N\,[h\,(1^{k|1})^2 + (-1)^{k+1}]^m$$

a qual substituida na expresão do modulo dá

$$M = \text{fact.} \left\{ [N\,(1^{k|1})^{2m} - 1] \cdot [h\,(1^{k|1})^2 + (-1)^{k+1}]^m \right\}$$

que se reduz a

$$M = \text{fact.}\,[N\,(1^{k|1})^{2m} - 1]$$

attenta a existencia da quantidade h no segundo factor.

E se suppozermos a congruencia mais geral

$$z^n - Ny^m \equiv 0 \pmod{M},$$

fazendo $Ny^m = a$ reduz-se á congruencia fundamental

$$z^m - a \equiv 0 \pmod{M}.$$

Em razão do valor de a será

$$y = h\,(1^{k|1})^2 + (-1)^{k+1},$$

z será dado pela expressão

$$z = h + (-1)^{\pi+k} \cdot \aleph \left[\frac{M}{(1^{k|1})^2}, \pi \right]^{(\pi-1)} + Mj.$$

77. Vejamos como effectuar a resolução.

Supponhamos $x = (1^{k|1})^2$ e $x^n = (1^{k|1})^{2n} = \alpha$

*

em virtude da expressão que dá o modulo, temos

$$a\alpha - 1 \equiv 0 \text{ (mod. M)}$$

d'onde

$$\alpha = (-1)^{\omega+1} \cdot \aleph\left[\frac{M}{a}, \omega\right]^{(\omega-1)} + Mi$$

e poderemos formar a expressão

$$x^n \equiv \alpha \text{ (mod. M)}.$$

Calculando para os generos successivos os residuos dados por $(1^{k|1})^2 \equiv f(k)$ (mod. M) chegaremos a egualdades da fórma $x=f(k)$, que nos darão os generos de que depende a formação de z e y.

No caso de não se obter egualdade alguma, concluia-se que a congruencia não era possivel com o coefficiente que tinha.

CONGRUENCIAS DE PRIMEIRA ORDEM E DE GRÁO *m*

78. *Resolução das congruencias de primeira ordem e de grão* m. Seja a congruencia

$$A_0 + A_1x + A_2x^2 + \ldots + A_mx^m \equiv 0 \text{ (mod. M)} \ldots (59)$$

o methodo de a resolver consiste em reduzil-a ás congruencias de primeira ordem.

Ora, na congruencia fundamental binomia de primeira ordem $x^n \equiv a$ (mod. M), é

$$a = (-1)^{\omega+1}[h(1^{k|1})^2 + (-1)^{k+1}]^n \cdot \aleph\left[\frac{M}{(1^{k|1})^{2n}}, \omega\right]^{(\omega-1)} + Mi$$

$$= N_n H^n + Mi$$

fazendo

$$(-1)^{\omega+1}.\aleph\left[\frac{M}{(1^{k|1})^{2n}},\ \omega\right]^{(\omega-1)}=N_n,\ [h(1^{k|1})^2+(-1)^{k+1}]^n=H^n$$

portanto

$$x^n\equiv N_n H^n \pmod{M}.$$

Substituindo na equação (59), vem

$$A_1+A_1 N_1 H+A_2 N_2 H^2+\ldots+A_m N_m H^m\equiv 0 \pmod{M}$$

multiplicando por $(1^{k|1})^{2m}$ eliminamos N e fica

$$A_0(1^{k|1})^{2m}+A_1(1^{k|1})^{2(m-1)}.H+\ldots+A_n(1^{k|1})^{2(m-n)}.H^n+\ldots+$$
$$+A_m H^m\equiv 0 \pmod{M}$$

em que, no primeiro membro já não existe M, e por isso determina esta quantidade.

$$M=\text{fact.}\,[A_0(1^{k|1})^{2m}+A_1(1^{k|1})^{2(m-1)}H+$$
$$+A_2(1^{k|1})^{2(m-2)}.H^2+\ldots+A_m H^m]$$

sendo ainda o valor de x

$$x=h+(-1)^{\pi+k}.\aleph\left[\frac{M}{(1^{k|1})^2},\ \pi\right]^{(\pi-1)}+Mj.$$

79. *Determinação methodica das raizes.* — Estabelecendo

$$W_\rho=(1^{k|1})^{2(m-\rho)}H^\rho$$

temos

$$M=\text{fact.}\,[A_0 W_0+A_1 W_1+A_2 W_2+\ldots+A_m W_m]$$

e como a quantidade entre parentheses é uma funcção de k e h, podemos pôr

$$F(k, h) = A_0 . W_0 + A_1 . W_1 + A_2 . W_2 + \ldots + A_m . W_m$$

por isso

$$\frac{dF(k,h)}{dh} = A_1 . W_1 + \frac{2}{1} A_2 . W_2 +$$

$$+ \frac{3^{2|-1}}{1^{2|1}} . A_3 . W_2 + \ldots + \frac{m^{m-1|-1}}{1^{m-1|1}} . A_m W_{m-1}$$

e em geral

$$\frac{d^\mu F(k,h)}{d^{\mu|1} . dh^\mu} = A_\mu . W_0 + \frac{\mu+1}{1} . A_{\mu+1} . W_1 + \frac{(\mu+2)^{2|-1}}{1^{2|1}} A_{\mu+2} . W_2 + \ldots$$

$$+ \frac{m^{m-\mu|-1}}{1^{(m-\mu)|1}} . A_m . W^{m-\mu}.$$

Portanto

$$F(k, h \pm 1) = [A_0 \pm A_1 + A_2 \pm \ldots (\pm 1)^m A_m] W_0 +$$

$$+ \left[A_1 \pm 2A_2 + \ldots (\pm 1)^{m-1} \frac{m}{1} A_m \right] W_1 \ldots + A_m . W_m$$

$$= B_0 W_0 + B_1 W_1 + B_2 W_2 + \ldots + B_m W_m.$$

Partindo pois d'um valor primitivo de h, poderemos com um valor dado k, calcular para todos os valores de h a quantidade $F(k, h)$ que é a funcção generatriz de M, e d'este modo achar os elementos k, h, que geram o modulo dado.

A expressão que nos dá x mostra-nos que qualquer que seja o valor de k sempre haverá um de h com o qual combinado resultará o valor de x.

Reconheceremos a probabilidade de que seja impossivel a congruencia, se dando a k valores cada vez maiores não chegarmos a uma funcção variada propria para gerar o modulo.

Não é necessario dar a k mais d'um valor: não insistiremos sobre a vantagem de lhe dar differentes valores, para se reconhecer basta notar os calculos numericos que evitam este modo de proceder.

80. *Resolução pelo abaixamento de gráo.* — Depois de termos calculado uma raiz da congruencia podemos aproveitar-nos d'ella para abaixar o gráo.

Com effeito, supponhamos que se achou uma raiz a da congruencia (59),

$$x = a + \mathrm{M}i,$$

dividindo o primeiro membro por

$$x - a \equiv 0 \pmod{\mathrm{M}}$$

temos

$$(x-a)[\mathrm{A'}_0 + \mathrm{A'}_1 x + \mathrm{A'}_2 x^2 + \ldots + \mathrm{A'}_{m-1} x^{m-1}] - \mathrm{R} \equiv \pmod{\mathrm{M}},$$

e como $x = a$ reduz esta equação a

$$-\mathrm{R} \equiv 0 \pmod{\mathrm{M}}$$

deve R ser um numero congruo com M.

Em consequencia a expressão acima torna-se em

$$(x-a)\,(\mathrm{A'}_0 + \mathrm{A'}_1 x + \mathrm{A'}_2 x^2 + \ldots + \mathrm{A'}_{m-1} x^{m-1}) \equiv 0 \pmod{\mathrm{M}}$$

que se decompõe nas duas

$$x - a \equiv 0 \pmod{\mathrm{M}}$$

$$\mathrm{A'}_0 + \mathrm{A'}_1 x + \mathrm{A'}_2 x^2 + \ldots + \mathrm{A'}_{m-1} x^{m-1} \equiv 0 \pmod{\mathrm{M}}$$

de harmonia com o que dissemos.

81. *Resolução por meio de transformações algebricas.* — Con-

sideremos a equação do segundo grão

$$x^2 + Ax + B \equiv 0 \pmod{M}$$

e façamos

$$x \equiv z + \alpha \pmod{M}$$

fica

$$z^2 + (2\alpha + A)z + (\alpha^2 + A\alpha + B) \equiv 0 \pmod{M} \ldots (60).$$

Como α é uma quantidade qualquer, podemos determinal-a pela condição

$$2\alpha + A \equiv 0 \pmod{M}$$

que dá

$$\alpha = (-1)^{\omega} . A . \aleph \left[\frac{M}{2}, \omega \right]^{(\omega-1)} + Mi:$$

este valor introduzido na congruencia (60) dá

$$z^2 + (\alpha^2 + A\alpha + B) \equiv 0 \pmod{M}$$

congruencia fundamental de primeira ordem que immediatamente se pode resolver.

Consideremos a congruencia de terceiro grão

$$x^3 + Ax^2 + Bx + C \equiv 0 \pmod{M} \ldots\ldots (61)$$

fazendo

$$x \equiv (z + \alpha) \pmod{M}$$

vem

$$z^3 + (3\alpha + A)z^2 + (3\alpha^2 + 2A\alpha + B)z + (\alpha^3 + A\alpha^2 + B\alpha + C) \equiv 0 \pmod{M}.$$

Estabelecendo as congruencias de condição

$$3\alpha + A \equiv 0 \pmod{M} \quad , \quad 3\alpha^2 + 2A\alpha + B \equiv 0 \pmod{M}$$

a congruencia (61) reduz-se á fundamental de primeira ordem

$$z^3 + (\alpha^3 + A\alpha^2 + B\alpha + C) \equiv 0 \pmod{M}.$$

N'este caso é porém necessario que o valor de α dado pela primeira congruencia de condição satisfaça á segunda.

Havia a fazer considerações analogas sendo qualquer o gráo da congruencia.

CONGRUENCIAS DE QUALQUER ORDEM E GRÁO

82. *Resolução da congruencia de qualquer ordem e gráo.* — Vamos apresentar a deducção das formulas para este caso geral.

Seja a congruencia

$$\left.\begin{aligned}
&(0)+(1_1)x_1+(\ 1_2\ )x_1^2+(\ 1_3\ )x_1^3+\ldots.\\
&+(2_1)x_2+(1_1\,2_1)x_1x_2+(1_2\,2_1)x_1^2x_2+\ldots.\\
&+(3_1)x_3+(\ 2_2\ )x_2^2+(1_1\,2_2)x_1x_2^2+\ldots.\\
&+\ldots..+(1_1\,3_1)x_1x_3+(\ 2_3\ )x_2^3+\ldots.\\
&+(2_1\,3_1)x_2x_3+(1_2\,3_1)x_1^2x_3+\ldots.\\
&+(\ 3_2\ )x_3^2+(1_1\,3_2)x_1x_3^2+\ldots.\\
&+\ldots\ldots\ldots+(2_2\,3_1)x_2^2x_3+\ldots.\\
&+(2_1\,3_2)x_2x_3^2+\ldots.\\
&+(\ 3_3\ )x_3^3+\ldots.\\
&+(1_1\,2_1\,3_1)x_1x_2x_3+\ldots\\
&\ldots\ldots\ldots\ldots\ldots
\end{aligned}\right\}\equiv 0\ (\text{mod. M}).$$

Estabeleçamos as congruencias

$$x_1^n\equiv a_1\ (\text{mod. M})$$

$$x_2^n\equiv a_2\ (\text{mod. M})$$

$$x_3^n\equiv a_3\ (\text{mod. M})$$

$$\ldots\ldots\ldots\ldots$$

Fazendo

$$(-1)^{\omega_\mu+1} \cdot \aleph\left[\frac{M}{(1^{k_\mu|1})^{2n}}, \omega\right]^{(\omega-1)} = M_{n_\mu}$$

$$\left[h_\mu (1^{k_\mu|1})^2 + (-1)^{k_\mu+1}\right]^n = H_\mu^n$$

será em virtude da lei da geração dos residuos

$$a_1 = N_{n_1} H_1^n + M i_1$$
$$a_2 = N_{n_2} H_2^n + M i_2$$
$$a_3 = N_{n_3} H_3^n + M i_3$$
$$\ldots\ldots\ldots\ldots\ldots$$

e por isso

$$x_1^n = N_{n_1} H_1^n + M i_1$$
$$x_2^n = N_{n_2} H_2^n + M i_1$$
$$x_3^n = N_{n_3} H_3^n + M i_2$$
$$\ldots\ldots\ldots\ldots\ldots$$

Estes valores substituidos na congruencia geral, dão

$$\begin{aligned}
&(0)+(1_1)N_{1_1}.H_1+(1_2)N_{2_1}.H_1^2+(1_3)N_{3_1}.H_1^3+\ldots\\
&+(2_1)N_{1_2}H_2+(1_12_1)N_{1_1}.N_{1_2}H_1.H_2+(1_22_1)N_{2_1}N_{1_2}H_1^2H_2+\ldots\\
&+(3_1)N_{1_3}H_3+(2_2)N_{2_2}H_2^2+(1_12_2)N_{1_1}N_{2_2}H_1H_2^2+\ldots\\
&+\ldots\ldots+(1_13_1)N_{1_1}N_{1_3}H_1H_3+(2_3)N_3H_2^3+\ldots\\
&+(2_13_1)N_{1_2}N_{1_3}H_3+(1_23_1)N_{2_1}N_{1_3}H_1^2H_3+\ldots\\
&+(3_2)N_{2_3}H_3^2+(1_13_2)N_{1_1}N_{2_3}H_1H_3^2+\ldots\\
&+\ldots\ldots\ldots\ldots+(2_23_1)N_{2_2}N_{1_3}H_2^2H_3+\ldots\\
&+\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

$$\equiv 0 \text{ (mod. M)}.$$

Multiplicando pelo producto de factoriaes de que a expressão é $(1^{k_\mu|1})^{2n}$ e notando que é

$$(1^{k_\mu|1})^{2n} . N_{n_\mu} \equiv 1 \text{ (mod. M)}$$

a congruencia atraz transforma-se em

$$\begin{aligned}
&(0)\,(1^{k_1|1})^{2(m_1-0)}\,(1^{k_2|1})^{2(m_2-0)}\,(1^{k_3|1})^{2(m_3-0)}\ldots\ldots\ldots\ldots\ldots+\\
&\quad+(1_1)\,(1^{k_1|1})^{2(m_1-1)}.H_1.(1^{k_2|1})^{2(m_2-0)}.(1^{k_3|1})^{2(m_3-0)}\ldots\ldots+\\
&\quad+(1_2)\,(1^{k_1|1})^{2(m_1-2)}.H_1^2.(1^{k_2|1})^{2(m_2-0)}.(1^{k_3|1})^{2(m_3-0)}\ldots\ldots+\\
&\quad+(2_1)\,(1^{k_1|1})^{2(m_1-0)}.(1^{k_2|1})^{2(m_2-1)}.H_2.(1^{k_3|1})^{2(m_3-0)}\ldots\ldots+\\
&\quad+(1_1 2_1)(1^{k_1|1})^{2(m_1-1)}.H_1.(1^{k_2|1})^{2(m_2-1)}.H_2.(1^{k_3|1})^{2(m_3-0)}\ldots+\\
&\quad+(3_1)\,(1^{k_1|1})^{2(m_1-0)}.(1^{k_2|1})^{2(m_2-0)}.(1^{k_3|1})^{2(m_3-1)}.H_3\ldots\ldots+\\
&\quad+(2_2)\,(1^{k_1|1})^{2(m_1-0)}.(1^{k_2|1})^{2(m_2-2)}.H_2^2.(1^{k_3|1})^{2(m_3-0)}\ldots\ldots+\\
&\quad+\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

$$\equiv 0 \text{ (mod. M)}.$$

Por consequencia, fazendo

$$W_{n_{\rho_p}} = (1^{k_n|1})^{2(m_n-\rho_p)}\,(H_n)^{\rho_p}$$

teremos

$$\begin{aligned}
M = \text{fact.}\,[(0)\,.\,&W_{1_0}.W_{2_0}.W_{3_0}\ldots+\\
+(1_1)\,W_{1_1}.W_{2_0}.W_{3_1}\ldots+&(\;1_2\;).W_{1_2}.W_{2_0}.W_{3_0}\ldots+\ldots\\
+(2_1)\,W_{1_0}.W_{2_1}.W_{3_0}\ldots+&(1_1 2_1).W_{1_1}.W_{2_1}.W_{3_0}\ldots+\ldots\\
+(3_1)\,W_{1_0}.W_{2_0}.W_{3_1}\ldots+&(\;2_2\;).W_{1_0}.W_{2_2}.W_{3_0}\ldots+\ldots\\
+\ldots\ldots\ldots\ldots\ldots\ldots+&(1_1 3_1).W_{1_1}.W_{2_0}.W_{3_1}\ldots+\ldots\\
+&(2_1 3_1).W_{1_0}.W_{2_1}.W_{3_1}\ldots+\ldots\\
+&(\;3_2\;).W_{1_0}.W_{2_0}.W_{3_2}\ldots+\ldots\\
\ldots&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots]
\end{aligned}$$

Conhecida assim a geração do modulo M, as raizes da congruencia terão para valores

$$\left.\begin{aligned} x_1 &= h_1 + (-1)^{\pi_1+k_1} \cdot \aleph\left[\frac{M}{(1^{k_1|1})^2},\ \pi_1\right]^{(\pi_1-1)} + M i_1 \\ x_2 &= h_2 + (-1)^{\pi_2+k_2} \cdot \aleph\left[\frac{M}{(1^{k_2|1})^2},\ \pi_2\right]^{(\pi_2-1)} + M i_2 \\ x_3 &= h_3 + (-1)^{\pi_3+k_3} \cdot \aleph\left[\frac{M}{(1^{k_3|1})^2},\ \pi_3\right]^{(\pi_3-1)} + M i_3 \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \end{aligned}\right\} \ldots (62)$$

83. *Determinação methodica das raizes.* — Notando que analogamente ao que atraz dissemos, pode suppor-se o modulo como uma funcção de k e H, teremos

$$M = \text{fact.}\,[F(k_1, k_2, k_3, \ldots; H_1, H_2, H_3, \ldots)]$$

que equivale á congruencia

$$F(k_1, k_2, k_3, \ldots; H_1, H_2, H_3, \ldots) \equiv 0 \ (\text{mod. } M).$$

No caso de ser a congruencia dada d'uma ordem qualquer μ, e $m_1, m_2, m_3, \ldots m_\mu$, os gráos das variaveis, temos

$$F(k_1, k_2, k_3 \ldots k_\mu; H_1, H_2, H_3 \ldots H_\mu) \equiv 0 \ (\text{mod. } M)$$

e como no primeiro menbro d'esta congruencia ha termos em que só ha H_1 ou $H_2, \ldots$ e que denotaremos por $F^{(1)}, F^{(2)}, \ldots$.

$F^{(n)}$, outro em $H_1 . H_2 \ldots H_{\mu-1} . H_\mu$ que denotaremos por $F^{(\mu+1)}$;

se imaginarmos $\mu+1$ quantidades satisfazendo á condição

$$S_1+S_2+\ldots S_{\mu+1}\equiv 0 \pmod{M} \ldots\ldots (63)$$

podemos decompor a congruencia acima em $\mu+1$ outras, a saber

$$\left.\begin{array}{l} S_1+F^{(1)}(k_1, k_2, k_3, \ldots k_\mu, H_1)\equiv 0 \pmod{M} \\ S_2+F^{(2)}(k_1, k_2, k_3, \ldots k_\mu, H_2)\equiv 0 \pmod{M} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ S_\mu+F^{(\mu)}(k_1, k_2\ k_3, \ldots k_\mu, H_\mu)\equiv 0 \pmod{M} \end{array}\right\} \ldots (64)$$

$$S^{\mu+1}+F^{(\mu+1)}(k_1, k_2, k_3, \ldots k_\mu, H_1\, H_2 \ldots H_\mu)\equiv 0 \pmod{M} \ldots (65).$$

Pelo methodo já atraz exposto podemos deduzir das μ primeiras equações os valores de $S_1, S_2, \ldots S_\mu$; eliminando por meio dos valores assim obtidos $H_1, H_2, \ldots H_\mu$ de (64), resultará a congruencia

$$F^{(\mu+2)}(k_1, k_2, k_3, \ldots k_\mu; S_1, S_2, \ldots S_{\mu+1})\equiv 0 \pmod{M},$$

eliminando ainda $S_{\mu+1}$ pela congruencia (63), fica

$$F^{(\mu+2)}(k_1, k_2, k_3, \ldots k_\mu; S_1, S_2, \ldots S_\mu)\equiv 0 \pmod{M} \ldots (66).$$

Portanto determinados pelas congruencia (64) os valores de $S_1, S_2, \ldots S_\mu$ correspondentes a differentes especies $h_1, h_2, \ldots$ os systemas de valores que satisfizerem a (66) indicar-nos-hão aquelles dos valores de h que devemos aproveitar para achar as raizes $x_1, x_2, \ldots x_\mu$.

84. As cousas podem muitas vezes conduzir-se com mais simplicidade.

Com effeito, sabendo-se achar os valores de $F^{(1)}$, $F^{(2)}$, ..., por meio d'estas congruencias teremos os valores de H_1, H_2, ...; substituidos na congruencia (64), achar-se-ha $S_{\mu+1}$. Verificando em seguida os systemas de valores de S_1, S_2, ... $S_{\mu+1}$ que satisfazem a congruencia de condição, teremos pelos correspondentes de h os systemas que nos hão de determinar as raizes x_1, x_2, ... x_μ, substituindo além d'isso nas expressões achadas valores arbitrarios para k.

QUARTA PARTE

EQUAÇÕES INDETERMINADAS DE QUALQUER GRÁO E ORDEM

85. *A resolução das equações indeterminadas de uma ordem qualquer reduz-se á de equações indeterminadas em que a ordem é inferior de uma unidade.* — Estudadas como se acham as equações de congruencia, facil é ver que a resolução das equações indeterminadas está só dependente da transformação algebrica que as reduz ás equações de congruencia, tomando-se em consideração o factor do modulo.

Consideremos a equação geral

$$\left.\begin{array}{l}(0)+(1_1)x_1+(1_2)x_1^2+(1_3)x_1^3+\ldots.\\ +(2_1)x_2+(1_1 2_1)x_1x_2+(1_2 2_1)x_1^2x_2+\ldots.\\ +(3_1)x_3+(2_2)x_2^2+(1_1 2_2)x_1x_2^2+\ldots.\\ +\ldots\ldots+(1_1 3_1)x_1x_3+(2_3)x_2^3+\ldots.\\ +(2_1 3_1)x_2x_3+(1_2 3_1)x_1^2x_3+\ldots.\\ +(3_2)x_3^2+(1_1 3_2)x_1x_3^2+\ldots.\\ +\ldots\ldots\ldots+(2_2 3_1)x_2^2x_3+\ldots.\\ +(2_1 3_2)x_2x_3^2+\ldots.\\ +(3_3)x_3^3+\ldots.\\ +(1_1 2_1 3_1)x_1x_2x_3+\ldots\\ \ldots\ldots\ldots\ldots\ldots\end{array}\right\}=0\ldots\ldots(67)$$

No caso d'esta equação ser completa tem um termo em que existe o producto $x_1 . x_2 \ldots x_\mu$. Wronski chama a este termo *dominante*.

Em consequencia (67) póde escrever-se debaixo da fórma

$$F(x_1, x_2, x_3 \ldots x_\mu) + (x_1 . x_2 . x_3 \ldots x_\mu) = 0 \ldots . (68)$$

que immediatamente se reduz á congruencia

$$F(x_1, x_2, x_3, \ldots x_\mu) \equiv 0 \pmod{M} \ldots \ldots . (69).$$

Como já se sabem resolver as congruencias de qualquer gráo e ordem, tiraremos de (69) os valores de x_1, $x_2, \ldots x_\mu$: terão as expressões

$$x_2 = X_1 + Mj, \; x_2 = X_2 + Mj_2, \ldots x_\mu = X_\mu + Mj_\mu \ldots (70).$$

Estes, porém, não são os valores que satisfazem á equação indeterminada proposta; pois, em quanto que na congruencia transformada é arbitrario o factor do modulo M, na equação indeterminada tem um certo valor $(x_1 . x_2 . x_3 \ldots x_\mu)$.

Por isso, para que os valores satisfaçam á proposta (67) é necessario escolher convenientemente, $j_1, j_2, \ldots j_\mu$.

Introduzidos na proposta estes valores de $x_1, x_2, x_3, \ldots$ resultará uma equação indeterminada entre $j_1, j_2, \ldots$

$$\varphi(j_1, j_2, j_3, \ldots) = 0$$

da mesma ordem e gráo que a humitiva. Pelo que parece nada se ter adiantado.

Estes numeros $j_1, j_2, j_3, \ldots$, são porém completamente indeterminados, sendo só obrigados a satisfazer á congruencia.

Notando que os valores indicados de $x_1, x_2, x_3 \ldots$ das raizes da congruencia, tornam a equação divisivel por M, vemos que formam uma primeira determinação das raizes da equação.

Podemos por isso suppor, que o valor que tomou uma das raizes dando a j um certo valor é o que lhe corresponde na equação,

comtanto que determinemos quaes devem ser conseguintemente os valores para as outras indeterminadas.

O mais simples é fazer $j_1 = 0$. Em consequencia a equação indeterminada anterior ficará da ordem $\mu - 1$. E vê-se como é possivel effectuar a resolução do problema.

86. Procedendo analogamente com a equação que resulta para determinar os valores das outras quantidades $j_2, j_3, \ldots$, chegariamos a uma equação da ordem $\mu - 2$. E assim continuariamos até chegar a uma equação de primeira ordem: obtendo-se sempre valores de $x_1, x_2, x_3, \ldots$ cada vez mais determinados.

87. *Reducção immediata a uma equação em que a ordem é inferior de muitas unidades á da proposta.* — Transformemos a proposta em differentes congruencias, tomando para modulos coefficientes diversos do termo dominante, e combinemos as raizes correspondentes de modo que possam identificar-se por meio de valores convenientes das arbitrarias j. D'este modo a proposta será ao mesmo tempo divisivel por todos os coefficientes que formam os modulos d'estas congruencias.

Estas raizes terão assim gráos successivamente mais elevados de determinação. Poderemos determinar completamente tantas raizes quantos forem os systemas de equações, e porisso egualmente outros tantos numeros indeterminados j. Estes valores determinados, substituidos na equação em j, reduzil-a-hão a uma ordem inferior de um numero correspondente de unidades.

88. Se for N o termo independente, temos

$$f(x_1, x_2, x_3, \ldots) + N = 0$$

ou

$$f(x_1, x_2, x_3, \ldots) \equiv 0 \pmod{N}$$

d'onde

$$x_1 = X'_1 + N i_1 \ldots, \quad x_2 = X'_2 + N i_2, \ldots.$$

em que são $X'_1, X'_2, \ldots$ quantidades conhecidas, $i_1, i_2, \ldots$ quantidades indeterminadas.

Considerados em si, estes valores são uma primeira determinação das raizes da proposta.

Porém se escolhendo convenientemente os valores de i obtivermos que sejam eguaes os valores correspondentes das raizes tiradas das differentes congruencias, substituidos na equação proposta, esta será divisivel por M e N. Formarão pois uma segunda determinação das raizes da equação.

89. Vejamos como effectuar a combinação de que fallamos.

Sendo duas raizes dos dois systemas

$$\alpha_1 = A + Mi \quad , \quad \alpha_2 = B + Ni_1,$$

para serem eguaes deve ser

$$A - B + Mi - Ni_1 = 0.$$

Resultam portanto para determinar i e i_1 as congruencias

$$Mi + (A - B) \equiv 0 \pmod{N}$$

$$Ni_1 - (A - B) \equiv 0 \pmod{M}$$

d'onde

$$i = (-1)^{\omega} (A - B) . \aleph \left[\frac{N}{M}, \omega \right]^{(\omega-1)} + Np$$

$$i_1 = (-1)^{\pi} (A - B) . \aleph \left[\frac{M}{N}, \pi \right]^{(\pi-1)} + Mq$$

em que p e q são novas arbitrarias.

Em consequencia, temos

$$\alpha_1 = A + (-1)^{\omega} (A - B) . \aleph \left[\frac{N}{M}, \omega \right]^{(\omega-1)} + NMp$$

$$\alpha_2 = B - (-1)^{\pi} (A - B) . \aleph \left[\frac{M}{N}, \pi \right]^{(\pi-1)} + MNq$$

$$\alpha_1 - \alpha_2 = (A - B)\left(1 + (-1)^{\omega}.M.\aleph\left[\frac{N}{M}, \omega\right]^{(\omega-1)}\right.$$

$$\left. + (-1)^{\pi}N.\left[\frac{M}{N}, \pi\right]^{(\pi-1)}\right) + MNp - MNq$$

mas, como é

$$(-1)^{\omega}.N.\aleph\left[\frac{N}{M}, \omega\right]^{(\omega-1)} + 1 \equiv 0 \text{ (mod. M)}$$

será

$$\alpha_1 - \alpha_2 = MNp - MNq.$$

Porisso tomando

$$p = q \quad , \quad \alpha_1 = \alpha_2$$

as raizes serão

$$x_1 = X_1 + (-1)^{\omega}(X_1 - X'_1)\,M.\aleph\left[\frac{N}{M}, \omega\right]^{(\omega-1)} + MNp_1$$

$$x_2 = X_2 + (-1)^{\omega}(X_2 - X'_2)\,M.\aleph\left[\frac{N}{M}, \omega\right]^{(\omega-1)} + MNp_2$$

. . . . . .

Agora n'estas expressões poderemos dar a duas arbitrarias quaesquer p os valores que quizermos, nada por exemplo, e ficarão determinadas duas raizes, comtanto que depois determinemos as outras arbitrarias pela condição de que todas as raizes substituidas na equação lhe satisfaçam.

90. Depois de substituidos estes valores das raizes na proposta ficar-nos-ha a equação

$$\varphi(p_1, p_2, p_3, \ldots) = 0$$

d'ordem $\mu - 1$, para determinar, $p_1, p_2, \ldots$.

D'esta maneira temos introduzido $\mu - 1$ arbitrarias o que não podia deixar de succeder, determinando a equação dada uma quantidade

*

QUINTA PARTE

91. N'esta ultima parte, como dissemos no prefacio, temo-nos proposto relacionar as materias expostas nas outras.

Bastaria a simples inspecção dos resultados obtidos na primeira e segunda parte para nos poupar quaesquer considerações.

N'este ponto não nos referimos á comparação da terceira e quarta parte relativas á resolução das equações de congruencias.

De mais a terceira e quarta completam-se, aquella dando os fundamentos para a resolução das equações indeterminadas que se faz na quarta, e esta apresentando-nos a resolução final dos problemas a tratar na theoria dos numeros.

Lançando uma rapida vista retrospectiva, vemos o seguinte:

Que na primeira parte se indicaram methodos; para a resolução completa e methodica das equações do primeiro e segundo gráo, no segundo caso só para quando houver duas variaveis; e para a resolução das equações a duas variaveis de gráos superiores ao segundo, não havendo já n'este caso um processo methodico para se resolver o problema.

Conforme Lagrange fez primeiro a resolução das equações indeterminadas, procura-se sempre fazer depender essa resolução do desenvolvimento em fracção continua d'uma expressão.

Falta porém para os casos geraes ver o meio de poder determinar methodicamente as raizes, e ainda, não o havendo, achar meio de reconhecer que se têm encontrado todas, para evitar uma serie indefinida de tentativas infructiferas.

No periodo anterior acabamos de dizer que — falta para os casos geraes, etc., — mas em verdade ainda a propria resolução das equações indeterminadas do segundo gráo é feita por tentativas, e vamos reconhecer isso.

92. Antes, porém, vejamos como se resolve pelos methodos teleologicos a congruencia de terceira ordem e gráo qualquer

$$z^n - Bq^n = Ap^n \ldots\ldots\ldots\ldots\ldots (71)$$

a qual para $n = 2$ se torna em

$$z^2 - Bq^2 = Ap^2.$$

É esta a equação de que apresentamos a resolução feita por Lagrange no n.° 26, e á qual se reduz a resolução das equações indeterminadas completas a duas variaveis.

A equação (71) dá a congruencia

$$z^n - Bq^n \equiv 0 \pmod{A}$$

que já sabemos resolver, e resulta

$$z = K + Ai_1 \quad , \quad q = L + Ai_2.$$

Depois temos

$$z^n - Ap^n \equiv 0 \pmod{B}$$

e porisso

$$z = K_1 + Bj_1 \quad , \quad p = L_1 + Bj_2.$$

Combinando os valores de z segundo a regra dada, teremos

$$z = K + (-1)^{\omega}(K - K_1)\,A \,.\, \aleph\left[\frac{B}{A},\ \omega\right]^{(\omega-1)} + ABn$$

$$z = K_1 + (-1)^{\pi}(K - K_1)\,B \,.\, \aleph\left[\frac{A}{B},\ \pi\right]^{(\pi-1)} + ABn$$

e fazendo auxiliarmente

$$(-1)^{\omega}.A.\aleph\left[\frac{B}{A},\omega\right]^{(\omega-1)}=(-1)^{\pi+1}B.\aleph\left[\frac{A}{B},\pi\right]^{(\pi-1)}-1=\alpha$$

fica

$$z=K+\alpha(K-K_1)+ABn\quad,\quad q=L+Ai\quad,\quad p=Q+Bj$$

em que n póde ter o valor que quizermos, nada por exemplo, e resta determinar i e j.

Introduzindo estes valores na proposta, vem

$$[K+\alpha(K-K_1)+ABn]^n-B(L+Ai)^n=A(L_1+Bj)^n\ldots(72).$$

E teriamos uma equação de primeira ordem a resolver.

93. Póde porém evitar-se a resolução da equação (72). Com effeito, sendo a proposta de segunda ordem

$$z^n-Bq^n=A$$

seria

$$z^n\equiv A\ (\text{mod. } B)$$

d'onde

$$z=K_1+Bi.$$

A segunda determinação de z era

$$z=K+\alpha(K-K_1)+ABn$$

e o valor de q

$$q=L+Ai.$$

Só havia a indeterminada i, a qual se acha pela equação

$$[K+\alpha(K-K_1)+ABn]^n-B(L+Ai)^n=A.$$

E como temos immediatamente

$$y^n = (P + Mi)^n = \frac{[K + \alpha(K - K_1) + ABn]^n - A}{B}$$

o ultimo membro d'esta egualdade terá a fórma

$$y^n = A_0 + A_1 h + A_2 h + \ldots + A_n h^n \ldots \quad \ldots (73)$$

em que os coefficientes são inteiros.

Resta só achar os valores de h que tornam o segundo membro d'esta egualdade uma potencia do gráo m, para termos os valores de y; darão ao mesmo tempo os valores correspondentes de z. Se para nenhum valor de h poder ser resolvida (73), é porque a proposta não admittiu soluções inteiras.

94. Quanto á equação (72) que obtivemos para a resolução das congruencias de terceira ordem, notando que contém h e h', poderemos por uma determinação conveniente d'estes numeros h e h' attender á determinação dos valores de i e j que n'ella entravam. E conforme ao que vimos no numero antecedente, resolver a equação de segunda ordem sem a reduzir a uma outra de primeira ordem.

95. Refiramo-nos porém de novo ás equações indeterminadas do segundo gráo e á sua resolução por Lagrange.

No n.° 26 vemos que a resolução fica dependente da equação

$$z = nq - Aq'$$

e porisso só por tentativas é que póde completar-se a resolução do problema.

De resto não era dada a solução completa das congruencias que era necessario estabelecer.

96. Temos demais visto na quarta parte que a resolução

das equações indeterminadas de todas as ordens se funda na resolução de equações instrumentaes, que no caso das equações indeterminadas de terceira ordem são duas, uma de segunda ordem e outra de primeira.

A resolução das equações de congruencia acha-se completamente feita para qualquer ordem na terceira parte.

97. Vejamos a final em que consiste essencialmente o methodo teleologico.

Consiste em não se procurar obter directamente as quantidades como se faz nas questões algebricas da algorithmia, em que se dá a lei da continuidade.

Em vez d'isso procuram-se quantidades que, variando continuamente, nos façam conhecer as raizes.

Estas quantidades são aqui o genero k e a especie h, que nos servem para determinar methodicamente os valores desconhecidos que só satisfazem a leis de singularidade.

Escolhendo arbitrariamente um d'aquelles elementos, poderemos ir estreitando, quanto quizermos, os limites entre os quaes deve ser tomado o outro elemento para obtermos as soluções do problema.

D'este modo evitam-se as tentativas caracteristicas dos methodos usados na theoria dos numeros.

98. Desde que se fizessem desapparecer das formulas os elementos auxiliares k e h de modo a ficarem-nos reduzidas a simples formulas algebricas, não teriamos por onde nos guiar e seria necessario empregar uma serie indefinida de tentativas, ficando-nos ordinariamente a incerteza de ter resolvido o problema.

Em conclusão. — *Os methodos teleologicos reduzem-se a construir uma lei auxiliar de continuidade para ligar factos discontinuos.*

99. Antes de acabarmos, e como justificação do que dissemos no numero antecedente, vejamos o que succederia na resolução das congruencias compostas, senão tivessemos empregado os elementos auxiliares k e h.

Fazendo eguaes a nada ou um as quantidades k_1, k_2, k_3,... teriamos

$$k_\nu = 0 \quad , \quad H_\nu = h_\nu - 1 \quad , \quad x_\nu = h_\nu - 1$$

ou $$k_\nu = 2 \quad , \quad H_\nu = h_\nu + 1 \quad , \quad x_{1\nu} = h_\nu + 1$$

portanto

$$x = H_1 \quad , \quad x_1 = H_2 \quad , \quad x_3 = H_3, \ldots .$$

Estes valores introduzidos na expressão do modulo reduzem-na á equação dada, e portanto não teremos meio de obter os modulos senão procurando-os com os valores das raizes.

Consequentemente estes valores poderiam ser determinados por tentativas, substituindo successivamente por cada raiz todos os numeros inteiros.

100. Deficiente, como não póde deixar de ser, este nosso trabalho, fica principalmente com uma lacuna importante.

Referimo-nos á demonstração por meio de applicações das vantagens do uso do methodo teleologico. Unico que de resto na maior parte dos casos póde resolver os problemas.

Esperamos preenchel-a o mais brevemente possivel, tanto quanto as nossas forças, demasiadamente fracas, o permittirem.

FIM.

INDICE

ERRATAS

Pag. 8, linh. 7, onde se lê inversaes — leia-se universaes.
Pag. 112, linh. 21, onde se lê humitiva — leia-se primitiva.

1885 C. LOBO-DISSERTAÇÃO INAUGURAL MATHEMATICA