ESTUDO DE ALGUMAS EQUAÇÕES

DE

CONGRUENCIA E INDETERMINADAS

ESTUDO DE ALGUMAS EQUAÇÕES

DE

CONGRUENCIA E INDETERMINADAS

POR

FRANCISCO MIRANDA DA COSTA LOBO

COIMBRA
IMPRENSA DA UNIVERSIDADE
1885

DISSERTAÇÃO DE CONCURSO

APRESENTADA Á

FACULDADE DE MATHEMATICA

DA

UNIVERSIDADE DE COIMBRA

DISSERTAÇÃO DE CONCURSO

APRESENTADA Á

FACULDADE DE MATHEMATICA

DA

UNIVERSIDADE DE COIMBRA

AO

ILLUSTRISSIMO E EXCELLENTISSIMO SENHOR

JOSÉ ESTEVÃO DE MORAES SARMENTO

Major promotor de justiça no 1.º cons. de guerra permanente na 1.ª div. mil.
Cavalleiro das ordens militares da Torre e Espada
e de S. Bento d'Aviz

Off. e D.

Francisco Miranda da Costa Lobo.

PREFACIO

O genero de questões que vamos apresentar como complemento do trabalho em que pretendemos desenvolver a theoria da resolução das equações indeterminadas, e como parte preparatoria, das equações de congruencia, faz parte do que ordinariamente se chama theoria dos numeros.

As regras que resolvem este genero de problemas dependem da 3.ª lei fundamental das mathematicas, apresentada por Wronski, e são essencialmente distinctas das que devem applicar-se nos casos ordinarios da algorithmia.

Era, portanto, necessaria uma nova notação algorithmica; foi Gauss que a introduziu, e foi dado o *nome de congruencia — á harmonia systematica entre a sommação e a graduação na geração dos numeros pelo seu concurso teleologico.*

Para melhor se comprehender o que Wronski designa por teleologia e por principio teleologico, notaremos a existencia em todas as sciencias d'uma realidade, que, apesar de satisfazer ás leis de universalidade que dominam o systema, comtudo parece seguir leis singulares.

É esta realidade, a que na lei da creação constitue a influencia reciproca dos elementos primordiaes, e que Wronski deno-

mina concurso final. *Teleologia* é a deducção dos factos que se referem a esta realidade. *Principio teleologico,* o principio de que deriva a effectividade dos factos que apresentam o accordo de que se trata.

Este principio deve portanto resultar do accordo dos 2 algorithmos primitivos oppostos, sommação e graduação, e tem a fórma

$$A + B x + C x^2 + \ldots + H x^h \equiv M \times N$$

que se torna considerando N como um numero indeterminado na congruencia geral

$$A + B x + C x^2 + \ldots + N x^n \equiv 0 \pmod{=M},$$

encontra-se egualmente na congruencia fundamental

$$x^m \equiv a \pmod{=M}.$$

Na D. I. vimos qual a maneira de achar os valores das differentes partes que entravam na construcção d'esta congruencia, e como a resolução das outras congruencias se operava em seguida.

Ainda vimos como se fazia depender a resolução das equações indeterminadas da resolução das equações de congruencia.

A resolução d'estas duas especies de equações effectua-se por meio das funcções alephs que Wronski introduziu nas mathematicas, e que n'este genero de problemas são funcções teleologicas.

É nas tres gerações (50), (51), (52) D. I. que consiste a lei teleologica, dando a construcção da congruencia fundamental de primeira ordem.

Na resolução das equações de congruencia e indeterminadas,

caracterisa o methodo teleologico a existencia, nas expressões generatrizes dos elementos que constituem as equações, das quantidades teleologicas k e h por meio das quaes se restringem os limites dos casos singulares em que podem apresentar-se as raizes das equações.

Ao que dissemos nos n.os 97, 98 e 99 D. I. só aqui juntaremos, que a não existencia nas fórmulas das quantidades k e h daria logar á necessidade d'uma serie de tentativas que na maior parte dos casos seria impraticavel; e para reconhecer o que dizemos basta attender á impossibilidade que haveria de obter a geração do modulo como se faz no n.º 83 D. I., e que é essencial para a determinação methodica das raizes das congruencias.

No trabalho que ora apresentamos e que se compõe de duas partes, equações de congruencia e equações indeterminadas, procuramos esclarecer, quanto nos foi possivel, por meio de algumas questões que n'ellas resolvemos, os methodos que muito summariamente tinham sido expostos na 3.ª e 4.ª parte da D. I.

Julgamos este trabalho de bastante necessidade para não deixar demasiadamente incompleto aquelle outro que tinhamos apresentado.

Com effeito, ha sempre muitas difficuldades que só apparecem quando se passa ás applicações, e factos que mesmo só então podem ser convenientemente explicados.

Por todos estes motivos parece-nos ter justificado a natureza do trabalho que apresentamos.

— D. I. é referencia á nossa Dissertação Inaugural.

EQUAÇÕES DE CONGRUENCIA

ESTUDO DE EQUAÇÕES CORRESPONDENTES AOS CASOS QUE SE APRESENTAM NA CONSTRUCÇÃO DAS CONGRUENCIAS

1. Seja a equação de congruencia

$$x^5 \equiv a \ (\text{mod.} = 31)$$

N'esta equação temos a calcular os residuos e raizes correspondentes. É um caso comprehendido no primeiro genero de problemas.

Fazendo as devidas substituições na fórmula que nos dá o residuo, temos

$$a = (-1)^{\omega+1} . [h\,(1^{k|1})^2 + (-1)^{k+1}]^5 \times \aleph \left[\frac{31}{(1^{k|1})^{10}}, \ \omega \right]^{(\omega-1)} + 31i.$$

Onde devem dar-se a k os valores comprehendidos entre 0 e 15, e a h os valores comprehendidos entre 0 e 30.

A expressão acima do residuo póde ainda apresentar-se d'este modo

$$a = \mathrm{A}\,(k, h) = (-1)^{5\,(k+1)} . \mathrm{A}\,(k, 0) . [h\,(1^{k|1})^2 + (-1)^{k|1}]^5 + 31i$$

..

sendo

$$A(k,0) = (-1)^{5(k+1)+\omega+1} \cdot \aleph\left[\frac{31}{(1^{k|1})^{10}}, \omega\right]^{(\omega-1)} + 31j.$$

Para

$$k=0 \quad \text{e} \quad k=1,$$

é

$$\aleph\left[\frac{N}{1}, 1\right]^{(1-1)} = 1,$$

$$A(0,0) = -1 + 31j$$

$$A(1,0) = 1 + 31j'$$

e por isso

$$a = A(0,h) = (h-1)^5 + 31i$$

$$a = A(1,h) = (h+1)^5 + 31i.$$

Quanto aos valores correspondentes de x, temos, attendendo á formula que nos dá as raizes das congruencias,

$$x = h + (-1)^{\pi+k} \cdot \aleph\left[\frac{31}{(1^{k|1})^2}, \pi\right]^{(\pi-1)} + Mi$$

e por isso

$$X(0,h) = (h-1) + 31i$$

$$X(1,h) = (h+1) + 31i.$$

Para um modulo qualquer

$$A(0,h) = (h-1)^m + Mj$$

$$A(1,h) = (h+1)^m + Mj$$

e

$$X(0,h) = (h-1)^m + Mi$$

$$X(1,h) = (h+1)^m + Mi.$$

Vê-se d'aqui que com os generos 0 e 1 obteriamos sempre os mesmos residuos e raizes correspondentes.

De resto já no n.º 121 da D. I. tinhamos visto a que correspondia darmos a k qualquer d'estes valores, 0 ou 1 (D. I., n.º 99).

É, portanto, necessario empregar um genero superior.

Façamos $k = 2$;

temos

$$A(2,0) = (-1)^\omega . \aleph\left[\frac{31}{1024}, \omega\right]^{(\omega-1)} + 31j.$$

Calculemos a funcção aleph, que entra n'esta expressão:

$$\frac{31}{1024} = 0 + \frac{31}{1024}, \; a_1 = 0, \; \aleph^{(1)} = 0$$

$$\frac{1024}{31} = 33 + \frac{1}{31}, \; a_2 = 33, \; \aleph^{(2)} = 1$$

$$\frac{31}{1} = 31 \qquad , \; a_3 = 31$$

logo $$A(2,0) = 1 + 31j$$

e $$a = A(2,h) = (4h-1)^5 + 31i$$

d'onde

$$A(2, 0) = -1, \quad A(2, 1) = 243, \quad A(2, 2) = 16807$$

....

Quanto aos valores de x temos

$$x = X(2, h) = h + (-1)^{\pi} . \aleph\left[\frac{31}{4}, \pi\right]^{(\pi-1)} + 31i$$

$$\frac{31}{4} = 7 + \frac{3}{4}, \; a_1 = 7, \; \aleph\left[\frac{31}{4}, 3\right]^{(1)} = 7$$

$$\frac{4}{3} = 1 + \frac{1}{3}, \; a_2 = 1, \; \aleph\left[\frac{31}{4}, 3\right]^{(2)} = 8$$

$$\frac{3}{1} = 3 \qquad , \; a_3 = 3$$

e

$$x = X(2, h) = (h - 8) + 31i$$

d'onde

$$X(2, 0) = -8, \quad X(2,1) = -7, \quad X(2,2) = -6, \ldots$$

A congruencia proposta é portanto satisfeita em geral do seguinte modo

$$(h - 8)^5 \equiv (4h - 1)^5 \;(\text{mod.} = 31)$$

e temos

$$(-8)^5 = -1, \; (-7)^5 \equiv 243, \ldots \;(\text{mod.} = 31).$$

Antes de mais nada vejamos como para outro qualquer valor

do modulo a fórmula geral que resolve a congruencia proposta não dá valores differentes dos já achados.

Para isso supponhamos $k=3$

$$A(3,0)=(-1)^{\omega+1}\,.\,\aleph\left[\frac{31}{6^{10}},\,\omega\right]^{(\omega-1)}+31i.$$

Fazendo o calculo da funcção aleph, vê-se que é $\omega=5$

e $$\aleph\left[\frac{31}{6^{10}},\,5\right]^{(4)}=5$$

portanto

$$A(3,0)=5+31j$$

$$A(3,h)=5\,(36h+1)^5+31j$$

Para x temos

$$X(3,h)=h+(-1)^{\pi+3}\,.\,\aleph\left[\frac{31}{36},\,\pi\right]^{(\pi-1)}+31i.$$

N'este caso é $\pi=4$

e $$\aleph\left[\frac{31}{36},\,4\right]^{(3)}=6$$

por isso $$X(3,h)=(h-6)+31i$$

consequentemente a congruencia torna-se em

$$(h-6)^5\equiv 5\,(36h+1)^5\ (\text{mod.}=31)$$

..

ou

$$(h-6)^5 \equiv 5\ (5h+1)^5\ (\text{mod.} = 31)$$

que se transforma na congruencia já achada, mudando h em $h-2$.

2. Seja a equação de congruencia

$$x^5 \equiv 3\ (\text{mod.} = \text{M}).$$

Suppomos agora o caso em que são desconhecidos a base e o modulo.

N'este caso temos, attendendo á lei de geração do modulo,

$$\text{M} = \text{fact.}\left\{3\ (1^{k|1})^{10} - [h\ (1^{k|1})^2 + (-1)^{k|1}]^5\right\}.$$

Para $k = 2$

$$\text{M} = \text{fact.}\ [3 \cdot 1024 - (4h-1)^5].$$

Que dá para

$h = 0$, $\text{M} = \text{fact.}\ 3073 = 7 \times 439$

$h = 1$, $\text{M} = \text{fact.}\ 2829 = 3 \times 23 \times 41$

$h = 2$, $\text{M} = \text{fact.}\ 13735 = 5 \times 41 \times 67$.

....

Poderiamos immediatamente formar as congruencias correspondentes aos modulos assim achados; e applicando-lhe a lei de geração das raizes, conheceriamos estas.

Notaremos que as soluções, que se obtêm quando resolvemos a congruencia em que o modulo é composto, comprehendem as que correspondem aos modulos simples depois de reduzidas as primeiras segundo estes.

EQUAÇÕES DE CONGRUENCIA FUNDAMENTAES

SOBRE A EXISTENCIA DAS RAIZES REAES

3. Vejamos como reconhecer a existencia das raizes reaes nas equações de congruencia fundamentaes.

Fazendo $$H = h(1^{k|1})^2 + (-1)^{k+1} \ldots\ldots\ldots\ldots (1)$$

e porisso $$H^m = \Xi$$

temos

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

que póde transformar-se em

$$(-1)^{\pi} a + NH^m \equiv 0 \ (\text{mod.} = M) \ldots\ldots\ldots (2)$$

sendo o valor de Ξ dado pela formula (54), D. I.

Dando a i um valor tal que o segundo membro seja uma potencia do gráo m

$$\Xi = R^m$$

temos $$(-1)^{\pi} a + NR^m \equiv 0 \ (\text{mod.} = M) \ldots\ldots\ldots (3)$$

e teremos como congruencia de condição para a resultante da subtração de (2) e (3)

$$H^m - R^m \equiv 0 \ (\text{mod.} = M) \ldots\ldots\ldots (4).$$

Ora, quando m é impar, R tem um só valor real, e podemos substituir a (4) esta outra equação

$$(H-R)[H^{m-1}+A_2H^{m-2}+A_3H^{m-3}+\ldots+A_mH^0]\equiv 0(\text{mod.}=M)$$

ou

$$H^{m-1}+A_2H^{m-2}+A_3H^{m-3}+\ldots+A_mH^0\equiv 0\ (\text{mod.}=M)\ (5).$$

N'este caso existe, portanto, uma raiz real para a congruencia proposta: a existencia das outras raizes depende da existencia de raizes reaes na congruencia (5) com os valores das quaes estão ligadas as especies h pela relação (1).

No caso de m par ha dois valores reaes para R, duas raizes para a congruencia, e fica a existencia das outras dependente das da congruencia

$$H^{m-2}+B_4H^{m-4}+\ldots+B_mH^0\equiv 0\ (\text{mod.}=M).$$

4. Consideremos especialmente a equação de congruencia

$$x^m\equiv 1\ (\text{mod.}=M)$$

em que é

$$M=\text{fact.}\ [(1^{k|1})^{2m}-H^m]$$

ou

$$M=[(1^{k|1})^2-H].[(1^{k|1})^{2(m-1)}+H(1^{k|1})^{2(m-2)}+$$

$$+H^2(1^{k|1})^{2(m-3)}+\ldots+H^{m-1}]$$

e por isso

$$(1^{k|1})^2-H\equiv 0\ (\text{mod.}=M),$$

$$(1^{k|1})^{2(m-1)}+H(1^{k|1})^{2(m-2)}+\ldots+H^{m-1}\equiv 0(\text{mod.}=M)\ (6)$$

isto no caso de m impar.

Para m par, teremos

$$(1^{k|1})^4 - H^2 \equiv 0 \,(\text{mod.} = M)$$

$$(1^{k|1})^{2(m-2)} + H^2(1^{k|1})^{2(m-4)} + \ldots + H^{m-2} \equiv 0 \,(\text{mod.} = M) \,(7).$$

Introduzamos nas congruencias (6) e (7) o valor de H; teremos

$$(1^{k|1})^2 (1-h) + (-1)^k \equiv 0 \,(\text{mod.} = M)$$

d'onde

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

e assim teriamos já um valor para h.

Em seguida a resolução das equações de congruencia do gráo $m-1$ e $m-2$ indicar-nos-hia o numero de raizes reaes existentes.

5. Wronski apresenta porém um outro methodo, que, não nos conduzindo á certeza, póde comtudo dar-nos com a probabilidade que se exigir o numero de raizes reaes da congruencia fundamental.

Para apresentarmos o methodo de Wronski recordemos que para obter todas as raizes d'uma equação de congruencia basta dar a k um valor differente de 0, 1, e depois formar os residuos que entram na constituição da raiz dando a μ valores inteiros successivos.

Podiamos tambem dar a k valores successivos e obter com valores de μ ordinariamente differentes os valores das raizes.

Supponhamos agora que, tendo-se achado uma raiz para um determinado valor de k e μ, continuamos a obter a mesma raiz variando o valor de μ, a probabilidade de que as raizes sejam differentes irá diminuindo á medida que isto succeder para um maior numero de valores que tenhamos dado a μ, e poderemos augmentar a probabilidade tanto quanto quizermos.

De resto é facil verificar se a raiz que resulta para um dado valor de μ por exemplo $\mu = 1$ e um valor qualquer de k é a

mesma que tinhamos obtido dando a k um determinado valor, por exemplo $k=2$.

Para que a raiz fosse a mesma, seria necessario que o valor de T, correspondente ao novo valor de k, fosse o mesmo que tinhamos obtido para $k=2$.

Assim, suppondo r a raiz achada, correspondente a $\mu=1$, façamos

$$\alpha=[a(1^{k|1})^{2m}+\mathrm{M}j]^{\frac{1}{m}} \ldots\ldots\ldots\ldots\ldots (8)$$

teremos dando a Q a significação que lhe foi attribuida no n.º 71. D. I.

$$\alpha\,\mathrm{Q}-r\equiv 0\ (\mathrm{mod.}=\mathrm{M})$$

d'onde

$$\alpha=(-1)^{\pi-1}.r.\aleph\left[\frac{\mathrm{M}}{\mathrm{Q}},\ \pi\right]^{(\pi-1)}+\mathrm{M}i \ldots\ldots (9)$$

e portanto

$$\alpha^m=a(1^{k|1})^{2m}+\mathrm{M}j$$

pelo que, para ter logar a hypothese das raizes resultantes serem as mesmas, deve ser

$$\alpha^m\equiv \mathrm{T}\ (\mathrm{mod.}=\mathrm{M}).$$

RESOLUÇÃO GERAL DE CONGRUENCIAS FUNDAMENTAES

6. Considerando a fórmula (57) (D. I.), supponhamos o caso em que existe um só factor. N'este caso a formula reduz-se a

$$x=\left[a\left\{(-1)^{\pi+\rho}.\aleph\left[\frac{\mathrm{M}}{\mathrm{N}},\ \rho\right]^{(\rho-1)}\right\}^{\mu}+\mathrm{M}j\right]^{\frac{1}{m}}+$$

$$+\left\{(-1)^{\pi-1}.\aleph\left[\frac{\mathrm{M}}{(1^{k|1})^2},\ \pi\right]^{(\pi-1)}\right\}^{\mu}+\mathrm{M}i \ldots\ldots (10).$$

A maneira de determinar o valor de x para este caso é a mesma que para os outros.

Mais simplesmente a expressão acima escreve-se

$$x = [a\,P^{\mu} + Mj]^{\frac{1}{m}} . Q^{\mu} + Mi \ldots\ldots\ldots (11).$$

Por onde vemos que a resolução do problema reduz-se á formação progressiva das potencias P^{μ} e Q^{μ}.

Esta formação já vimos no n.° 74. (D. I.) que se fazia depender dos seus residuos em relação ao modulo M, e suppondo R_{μ}, S_{μ} os residuos de P^{μ} e Q^{μ}, é em geral

$$R_{\mu+\nu} \equiv R_{\mu} . R_{\nu}, \quad S_{\mu+\nu} \equiv S_{\mu} . S_{\nu} \ (\text{mod.} = M) \ldots (12)$$

e para o termo a P^{μ}, suppondo o seu residuo T_{μ}, temos

$$T_{\mu+1} \equiv T_{\mu} . R_1 + Mi \ldots\ldots\ldots\ldots (13).$$

7. O numero arbitrario j aproveita-se para a reducção dos residuos T_{μ} a numeros menores do que M, e a expressão de x torna-se em

$$x = [T_{\mu}]^{\frac{1}{m}} . Q^{\mu} + Mi \ldots\ldots\ldots\ldots (14).$$

8. Se ao formar os residuos progressivos T_{μ} chegarmos a resultados periodicos antes de obtermos algum que seja uma potencia exacta do gráo m, será necessario empregar outro genero k. Não obtendo com este e outros generos, que em seguida empregarmos, potencias exactas para os valores de T_{μ}, teremos uma nova infinidade d'estes valores, combinando os resultados obtidos para cada um dos valores que se deu a k; e então a fórmula a applicar é

$$x = \left((-1)^{\pi-1} \left[T_{1_{\mu_1}} . T_{2_{\mu_2}} \ldots T_{\rho_{\mu_\rho}} \right] \times \aleph \left[\frac{M}{a_{\rho-1}}, \pi \right]^{(\pi-1)} + Mj \right)^{\frac{1}{m}} \times$$

$$\times \left[Q_{\mu_1} . Q_{\mu_2} \ldots Q_{\mu_\rho} \right] + Mi \ldots\ldots\ldots (15)$$

ou mais simplesmente

$$x=\left[a\left\{(1^{k_1|1})^{2m.\mu_1}.(1^{k_2|1})^{2m.\mu_2}...(1^{k_\rho|1})^{2m.\mu_\rho}\right\}+\mathbf{M}j\right]^{\frac{1}{m}}\times$$

$$\times\left\{Q1^{\mu_1}.Q2^{\mu_2}...Q_\rho^{\mu_\rho}\right\}+\mathbf{M}i$$

que no caso d'um só factor se reduz a

$$x=\left[a(1^{k|1})^{2m.\mu}+\mathbf{M}j\right]^{\frac{1}{m}}\times\left\{(-1)^{\pi+1}.\aleph\left[\frac{\mathbf{M}}{(1^{k|1})^2},\pi\right]^{(\pi-1)}\right\}^{\mu}+\mathbf{M}i.$$

9. Conhecidas todas as raizes menos uma, a outra é dada por uma equação de congruencia de primeira ordem, que exprime uma relação entre as m raizes da proposta, e que é

$$x_1.x_2...x_m=a(-1)^m\ (\text{mod.}=\mathbf{M}).$$

10. No caso do gráo m ser um numero par é evidente que a cada raiz positiva corresponde uma outra negativa equivalente.

Em seguida vamos apresentar um caso, em que uma equação se resolve com a maior facilidade attendendo a este theorema.

11. Seja a equação de congruencia

$$x^4\equiv 1\ (\text{mod.}=17).$$

Para achar as raizes d'esta equação temos a fazer uso da fórmula (11).

Supponhamos $k=2$ e calculemos as quantidades que entram na expressão de x,

temos $\qquad (1^{2|1})^8=256\quad (1^{2|1})^2=4.$

Na funcção

$$\aleph\left[\frac{17}{4}, \pi\right]^{(\pi-1)} \text{ é } \pi = 2$$

e

$$\aleph\left[\frac{17}{4}, 2\right]^{(1)} = 4.$$

A expressão geral das raizes para o genero $k = 2$ é portanto

$$x = [(256)^{\mu} + 17j]^{\frac{1}{4}} . (4)^{\mu} + 17i.$$

Passemos ao calculo dos residuos progressivos.

$$(256)^{\mu} = R_{\mu} = T_{\mu} \quad (4)^{\mu} = S_{\mu}$$

$$T_0 = 1 \qquad S_0 = 1$$

$$T_1 = 256 \quad S_1 = 4$$

e

$$x = \pm 16$$

$$x = \pm 1$$

12. Considere-se a equação de congruencia

$$x^5 \equiv 193 \pmod{= 281}.$$

Formemos as expressões que entram na fórmula que dá as raizes da equação para o caso de $k = 2$.

Temos

$$(1^{k|1})^2 = 4 \quad (1^{k|1})^{2m} = 2^{10} = 1024$$

e calculando a funcção

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

n'este caso

$$\aleph\left[\frac{281}{4}, \pi\right]^{(\pi-1)}$$

encontra-se $\pi = 2$

e $$\aleph\left[\frac{281}{4}, 2\right]^{(1)} = 70$$

porisso

$$x = [193 \,.\, (1024)^{\mu} + 281j]^{\frac{1}{5}} \times (70)^{\mu} + 281i.$$

Vamos calcular os residuos progressivos da quantidade entre parenthesis, que representamos por T_{μ}, até encontrarmos valores para esta quantidade que deem para x um valor racional, e que, fornecendo-nos o valor de μ, nos sirvam para calcular as raizes que se procuram.

Quanto á quantidade j, que está entre parenthesis, servirá unicamente para reduzir os valores de T_{μ} a serem mais pequenos do que o modulo, n'este caso 281.

Ha porém a notar que, sendo muito distanciadas as potencias dos numeros inteiros consecutivos quando vão sendo bastante altas, resultando existir um pequeno numero menor do que o modulo quando este não é muito grande, convém calcular varios gráos de reducção da quantidade T_{μ} para mais facilmente encontrar os valores de μ, que tornam T_{μ} uma potencia exacta do gráo da equação dada.

Tanto por esta razão, como para simplificar o calculo dos residuos progressivos T_{μ}, reduzindo-o a sommas e subtracções, convém calcular os dez primeiros multiplos da quantidade R_1 e M, e em seguida estabelecer o calculo, como adeante se faz.

No caso proposto é

$$(1024)^{\mu} \equiv R_{\mu}, \quad (70)^{\mu} \equiv S_{\mu}, \quad 193 \,.\, (1024)^{\mu} \equiv T_{\mu}.$$

Para o calculo dos residuos progressivos T_{μ} temos ainda a fórmula (13).

Os dez primeiros multiplos de R_1 e de M. são

$R_1 = 1024$	$M = 281$
$2.R_1 = 2048$	$2.M = 562$
$3.R_1 = 3072$	$3.M = 843$
$4.R_1 = 4096$	$4.M = 1124$
$5.R_1 = 5120$	$5.M = 1405$
$6.R_1 = 6144$	$6.M = 1686$
$7.R_1 = 7168$	$7.M = 1967$
$8.R_1 = 8192$	$8.M = 2248$
$9.R_1 = 9216$	$9.M = 2529$
$10.R_1 = 10240$	$10.M = 2810$

Passemos ao calculo dos residuos T_μ

$R_1 = 1024$

3072 — $3\,R_1$

9216 — $90\,R_1$

1024

197632

1967 — $700\,M$

932 — $3\,M$

843

$T_1 = 89,-192$

9216 — $9\,R_1$

8192 — $80\,R_1$

91136

843 — $300\,M$

683

562 — $20\,M$

1216

1124 — $4\,M$

$T_2 = 92,-189$

E continuando a effectuar o calculo dos residuos progressivos T_μ obteriamos

$$T_1 = 89,-192, \quad T_2 = 92,-189$$

$$T_3 = 73,-208, \quad T_4 = 6,-275$$

$$T_5 = 243,-38, \quad T_6 = 147,-134$$

$$T_7 = 193,-88, \quad T_8 = 89,-192.$$

E como o valor de T_8 era o mesmo que tinhamos obtido para T_1, não temos a calcular mais valores de T, pois reproduzir-se-hiam periodicamente, e devemos dar um novo valor a k.

Dos valores achados temos o de T_5, $T_5 = 243$, que é uma potencia do 5.º gráo de 3 e por isso nos servirá para o calculo d'uma raiz racional da equação dada, a qual passamos a calcular.

É portanto $\mu = 5$, $\quad [T_5]^{\frac{1}{5}} = 3.$

Temos a fazer o calculo de S_5, n'este caso effectua-se immediatamente e resulta

$$S_5 = -222.$$

Estes valores substituidos na expressão de x dão

$$x = -3.222 + 281i$$

ou

$$x = -104 + 281i$$

ainda passando para a raiz positiva

$$x = 177 + 281i$$

Effectuando, como atraz notámos era conveniente, o calculo dos residuos por gráos successivos, obteriamos no calculo do residuo T_6 o numero 248832, que tambem é uma potencia exacta do 5.º gráo do numero 12; passando porém ao calculo da raiz correspondente, vê-se que não fornece nenhuma nova raiz, porque dá $x = 177$ que já foi obtida.

Fazendo $k = 3$

temos

$$(1^{k|1})^{2m} = (1^{3|1})^{10} = 60466176 \quad (1^{3|1})^2 = 36$$

e a expressão de x, attendendo a que é

$$\pi = 4, \aleph \left[\frac{281}{36}, 4 \right]^{(3)} = 39,$$

é $$x = [193.(60466176)^\mu + 281.i]^{\frac{1}{5}} (-39)^\mu + 281j.$$

Temos $R_\mu \equiv (60466176)^\mu$ $S_\mu \equiv (-39)^\mu$

$$T_\mu \equiv 193.(60466176)^\mu$$

e obteriamos $R_1 = 60466176$

$T_1 = 99, -182$ $T_2 = 215, -66$ $T_3 = 120, -161$

$T_4 = 146, -135$ $T_5 = 187, -94$ $T_6 = 123, -158$

$T_7 = 248, -33$ $T_8 = 2, -279$ $T_9 = 68, -213$

$T_{10} = 64, -217$ $T_{11} = 209, -72$ $T_{12} = 166, -115$

$T_{13} = 24, -257$ $T_{14} = 254, -27$ $T_{15} = 251, -30$

$T_{16} = 104, -177$ $T_{17} = 164, -117$ $T_{18} = 237, -44$

$T_{19} = 190, -91$ $T_{20} = 278, -3$ $T_{21} = 179, -102$

$T_{22} = 185, -96$ $T_{23} = 108, -173$ $T_{24} = 19, -262$

$T_{25} = 84, -197$ $T_{26} = 46, -235$ $T_{27} = 159, -122$

$T_{28} = 67, -214$ $T_{29} = 30, -251$ $T_{30} = 177, -104$

$T_{31} = 117, -164$ $T_{32} = 44, -237$ $T_{33} = 91, -190$

$T_{34} = 3, -278$ $T_{35} = 102, -179$ $T_{36} = 135, -146$

$T_{37} = 94, -187$ $T_{38} = 105, -176$ $T_{39} = 198, -83$

$T_{40} = 53, -248$ $T_{41} = 279, -2$ $T_{42} = 213, -68$

$T_{43} = 217, -64$ $T_{44} = 72, -209$ $T_{45} = 200, -81$

$T_{46} = 56, -225$ $T_{47} = 218, -63$ $T_{48} = 106, -175$

$T_{49} = 232, -49$ $T_{50} = 20, -261$ $T_{51} = 118, -163$

$T_{52} = 78, -203$ $T_{53} = 123, -158.$

E apezar de ainda não termos obtido residuo algum que fosse uma potencia exacta do 5.º gráo, tinhamos a terminar o calculo dos residuos para $k = 3$, visto que appareceu $T_{53} = T_6$.

Seguia-se fazer $k = 4$; antes d'isso vejamos se os residuos obtidos poderão ser aproveitados de maneira a darem-nos mais alguma raiz real para a equação proposta, se é que a tem.

Ora é claro que os residuos T_μ que temos calculado tanto

podem comparar-se com as potencias dos numeros inteiros, como com os residuos d'estas segundo o modulo, e portanto podemos ter um grande numero de valores de comparação calculando residuos das potencias dos numeros inteiros. Assim evitar-se-ha a difficuldade resultante do pequeno numero de potencias inteiras do gráo da equação dada e inferiores ao modulo.

Em seguida está um quadro com os residuos das quintas potencias segundo o modulo 281 desde 1 até 42.

$1^5 \equiv 1$, $2^5 \equiv 32$, $3^5 \equiv 243$, $4^5 \equiv 181$, $5^5 \equiv 34$, $6^5 \equiv 189$

$7^5 \equiv 228$, $8^5 \equiv 172$, $9^5 \equiv 39$, $10^5 \equiv 245$, $11^5 \equiv 38$, $12^5 \equiv 147$

$13^5 \equiv 92$, $14^5 \equiv 271$, $15^5 \equiv 113$, $16^5 \equiv 165$, $17^5 \equiv 245$, $18^5 \equiv 124$

$19^5 \equiv 208$, $20^5 \equiv 253$, $21^5 \equiv 47$, $22^5 \equiv 92$, $23^5 \equiv 38$, $24^5 \equiv 208$

$25^5 \equiv 32$, $26^5 \equiv 134$, $27^5 \equiv 204$, $28^5 \equiv 242$, $29^5 \equiv 116$, $30^5 \equiv 244$

$31^5 \equiv 28$, $32^5 \equiv 222$, $33^5 \equiv 242$, $34^5 \equiv 253$, $35^5 \equiv 142$, $36^5 \equiv 34$

$37^5 \equiv 182$, $38^5 \equiv 193$, $39^5 \equiv 157$, $40^5 \equiv 228$, $41^5 \equiv 182$, $42^5 \equiv 99$

Se compararmos os residuos obtidos com os de T_μ para $k=2$ e $k=3$ vê-se que coincidem os seguintes.

Dos valores de T_μ para $k=2$

T_5 com o residuo de 3^5

$-T_2$ » » » » 6^5

$-T_5$ » » » » 11^5

T_6 » » » » 12^5

T_2 » » » » 13^5

T_2 » » » » 22^5

$-T_5$ » » » » 23^5

$-T_6$ » » » » 26^5

T_7 » » » » 38^5

Dos valores de T_μ para $k=3$

$-T_1$ com o residuo de 41^5

T_1 » » » » 42^5

O residuo T_5 para $k=2$ já atraz o consideramos e deu-nos a raiz $x=177$.

O residuo $T_2=(-6)^5$ a que corresponde $S_2=123$ dá

$$x=-6\times 123+281i$$

ou $x=-176+281i$, raiz positiva $x=105+281i$.

O residuo $T_5=(-11)^5$, a que corresponde $S_5=-222$, dá

$$x=-11\times -222+281i$$

$$x=194+281i.$$

O residuo $T_6=(12)^5$ a que corresponde $S_6=85$ dá a mesma raiz que tinhamos obtido para $T_5=243$.

Egualmente $T_2=(13)^5$, dá a mesma raiz que $T_5=(-11)^5$: $T_2=(22)^5$ a mesma raiz que $T_5=243$.

O residuo $T^5=(-23)^5$, a que corresponde $S_5=-222$, dá

$$x=-23\times -222+281i,$$

ou $$x=48+281i.$$

Como se vê já obtivemos 4 raizes para a equação proposta 177, 105, 194 e 48, porisso estamos no caso de poder calcular

immediatamente a 5.ª raiz attendendo ao theorema do n.º 9.

A equação que nos deve dar a 5.ª raiz é

$$177 \times 105 \times 194 \times 48 \times x \equiv 193 \pmod{=281}$$

ou

$$116\,x \equiv 193 \pmod{=281}$$

que resolvida pelas formulas que dão as raizes da equação de congruencia do primeiro gráo e ordem, temos

$$x = (-1)^{\omega+1} . 193 . \aleph\left[\frac{281}{116}, \omega\right]^{(\omega-1)} + \mathbf{M}i$$

onde é $\omega = 8$, e

$$\aleph\left[\frac{281}{116}, 8\right]^{(7)} = 109$$

e portanto

$$x = -243 + 281\,i,$$

ou a raiz positiva

$$x = 38 + 281\,i.$$

Se calculassemos as raizes correspondentes aos outros valores de T_μ coincidentes com os residuos das potencias do 5.º gráo dos numeros inteiros recahiriamos em valores já obtidos.

EQUAÇÕES DE CONGRUENCIA DE PRIMEIRA ORDEM E D'UM GRÁO QUALQUER

13. Consideremos a equação de congruencia

$$5 + 11\,x + 4\,x^2 + 7\,x^3 \equiv 0 \pmod{=\mathrm{M}}.$$

Tinhamos primeiramente a achar os valores de M e em seguida os valores correspondentes das raizes.

..

Ora pela fórmula do n.º 78 (D. I.) que nos dá o valor de M, temos

$$M = \text{fact.}\,[5\,(1^{k|1})^6 + 11\,(1^{k|1})^4 . H + 4\,(1^{k|1})^2 . H^2 + 7\,H^3]$$

sendo $$H = h . (1^{k|1})^2 + (-1)^{k+1}$$

Dando a k e h os valores que quizermos, deduziremos os correspondentes para H, e em seguida os que dão M satisfazendo á congruencia proposta.

O mais simples é fazer

$$k = 2, \quad h = 0$$

vem $$H = -1$$

e $$M = \text{fact.}\ 153 = 3 \times 3 \times 17$$

Para $$k = 2, \quad h = 1$$

tinhamos $$H = 3$$

e $$M = 1181$$

Os valores de x são dados pela expressão

$$x = h + (-1)^{\pi+k} . \aleph \left[\frac{M}{(1^{k|1})^2}, \pi \right]^{(\pi-1)} + Mi \ldots . (16)$$

onde substituindo por M, 1181 e por k e h os valores que correspondem

$$k = 2, \quad h = 1,$$

resulta

$$x = 1 + (-1)^{\pi} . \aleph \left[\frac{1181}{4}, \pi \right]^{(\pi-1)} + 1181 . i$$

e como é

$$\pi = 2, \aleph \left[\frac{1181}{4}, 2 \right]^{(1)} = 295$$

temos $$x = 296 + 1181 i.$$

E analogamente obteriamos as raizes que quizessemos.

14. Vamos em seguida considerar um caso em que não é dado o modulo.

N'este caso torna-se necessario determinar o genero k e a especie h que geram o modulo dado. Uma vez conhecidas aquellas quantidades immediatamente o ficam as raizes pela expressão (16).

As raizes sempre devem poder determinar-se methodicamente desde o momento em que a equação dada tenha raizes reaes, e vimos no n.° 19 (D. I.) como se fazia essa determinação.

Seja a equação

$$3x^4 + 7x^3 + 4x^2 + 5x + 2 \equiv 0 \ (\text{mod.} = 89).$$

Attendendo á lei de geração do modulo temos a satisfazer á equação

$$89 = \text{fact.} [2 . (1^{k|1})^8 + 5 . (1^{k|1})^6 . H + 4 (1^{k|1})^4 . H^2 +$$

$$+ 7 (1^{k|1})^2 . H^3 + 3 . H^4].$$

Com os valores de k e h que satisfizerem a esta equação é que determinaremos os valores das raizes.

Ora dando a k um valor qualquer temos a certeza, que desde o momento em que haja raizes reaes ha de encontrar-se sempre um valor para h, que com o valor de k, satisfaça aquella equação.

Façamos $k=2$

fica

$$89 = \text{fact.}\,[512+320.H+64.H^2+28.H^3+3.H^4]\ldots(17)$$

e $$H=4h-1.$$

Vamos dar a h valores successivos até encontrar algum que satisfaça a (17).

Para $h=0$

vem $H=-1,$

e a quantidade entre parenthesis torna-se em 231 que não tem para factor 89,

para $h=1$

vem $H=3$

e para a quantidade entre parenthesis 3047, que tambem não tem 89 como factor,

ainda para $h=2$

vem $H=7$

e resulta para a quantidade entre parenthesis

$$22695=5\times3\times17\times89$$

Por onde vemos que os numeros 2 e 2 são d'aquelles d'entre

os que podem ter o genero k e a especie h, que geram o modulo 89.

A raiz que corresponde é

$$x = 2 + (-1)^{\pi} \aleph\left[\frac{89}{4}, \pi\right]^{(\pi-1)} + 89\,i$$

onde é $$\pi = 2$$

e $$\aleph\left[\frac{89}{4}, 2\right]^{(1)} = 22,$$

logo $$x = 24 + 89\,i.$$

Em seguida para obtermos o valor das outras raizes tinhamos que continuar a dar a h valores successivos até encontrarmos novos valores que com o de k gerassem o modulo dado.

Ainda para realisar estas operações Wronski dá um methodo que as reduz a sommas e subtracções.

Como temos dito o genero k é completamente arbitrario, e para obtermos todas as raizes da congruencia basta em consequencia dar-lhe um, e combinar com elle os das especies h.

No emtanto ha conveniencia em variar os valores de k, porque variando a distancia dos valores de h que tem de ser combinados com o de k para gerar o modulo, com a distancia das raizes, póde ser necessario dar um grande numero de valores a h antes de chegarmos ao que aproveita, quando temos continuado a usar do mesmo genero; pelo contrario variando os generos k devemos obter as raizes com pequenos valores de h.

É d'estas simplificações, consequencias immediatas do methodo que se está applicando, que resulta uma das suas grandes vantagens.

Vejamos a applicação ao nosso caso do methodo apresentado por Wronski para o calculo da funcção F (k, h), que nos dá os valores de k e h quando satisfaz á relação (17).

A regra de Wronski serve para calcular os coefficientes de $F(k, h \pm 1)$ conhecidos os de $F(k, h)$.

Sendo

$$F(k, h) = A_0 W_0 + A_1 W_1 + A_2 W_2 + \ldots + A_m W_m \quad (18)$$

e

$$F(k, h \pm 1) = B_0 W_0 + B_1 W_1 + B_2 W_2 + \ldots + B_m W_m \quad (19)$$

vê-se immediatamente pelo n.º 79 (D. I.) que os valores de B_0, $B_1, \ldots B_m$ são dados em funcção dos coefficientes A_0, $A_1, \ldots A_m$ pelas relações

$$\left.\begin{aligned} B_0 &= A_0 \pm A_1 + A_2 \pm A_3 + \ldots (\pm 1)^m A_m \\ B_1 &= A_1 \pm 2A_2 + 3A_3 \pm 4A_4 + \ldots (\pm 1)^{m-1} \cdot \frac{m}{1} \cdot A_m \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ B_m &= A_m \end{aligned}\right\} (20).$$

Partindo pois de $F(2,2)$ ultima que tinhamos calculado tinhamos para as quantidades W, de que a expressão geral é

$$W_\rho = (1^{k|1})^{2(m-\rho)} . H^\rho,$$

n'este caso de $h = 2$

$$W_\rho = [(-1)^{k+1} + 2(1^{k|1})^2] . (1^{k|1})^{2(m-\rho)};$$

d'onde fazendo $k = 2$, resulta

$$W_\rho = 7 . 4^{(m-\rho)} = 7 . 4^{(4-\rho)}$$

que dá $W_0 = 1792, \quad W_1 = 448$

$W_2 = 112, \quad W_3 = 28$

$W_4 = 7.$

E como era

$$A_0 = 2, \quad A_1 = 5, \quad A_2 = 4, \quad A_3 = 7, \quad A_4 = 3$$

teremos para coefficientes da funcção F (2,3)

$$B_0 = 2 + 5 + 4 + 7 + 3 = 21$$

$$B_1 = 2 + 2.4 + 3.7 + 4.3 = 43$$

$$B_2 = 4 + 3.7 + 6.3 = 43$$

$$B_3 = 7 + 4.3 = 19$$

$$B_4 = 3.$$

Formando agora os dez primeiros multiplos das funcções W_ρ, que nos servirão para o calculo de F (2,3) e em geral de F $(2, h)$, obteremos com simples sommas e subtracções os valores das funcções variadas.

Calcularemos muito facilmente F (2,3) como em seguida se faz segundo a formula (19)

$$\begin{array}{r} 1\,W_0 = \quad 1792 \\ 20\,W_0 = 3584 \\ 3\,W_1 = \quad 344 \\ 40\,W_1 = 1792 \\ 3\,W_2 = \quad 112 \\ 40\,W_2 = \quad 448 \\ 9\,W_3 = \quad 252 \\ 10\,W_3 = \quad 28 \\ 3\,W_4 = \quad 21 \\ \hline 31041 = 9 \times 3449. \end{array}$$

Em logar porém de continuarmos no calculo das funcções $\mathbf{F}(2, h)$ passaremos a variar o valor de k attendendo as razões que acima expozemos.

Para $k=3, h=0$ temos

$$W_\rho = 36^{(4-\rho)}$$

e

$$W_0 = 1679616, \quad W_1 = 46656$$

$$W_2 = 1296, \quad W_3 = 34$$

$$W_4 = 1,$$

e para M resulta o valor

$$M = 3597937$$

que não é divisivel por 89.

Para $h=1$ o calculo dos coefficientes da funcção variada dá

$$A_0 = 21, \quad A_1 = 43,$$

$$A_2 = 43, \quad A_3 = 18,$$

$$A_4 = 3,$$

e $$M = 37334521 = 89 \times 419489.$$

Temos portanto uma nova raiz para a equação proposta correspondente ao genero $k=3$, especie $h=1$; substituindo estes valores na expressão da raiz resulta

$$x = 1 + (-1)^{\pi+3} \cdot \aleph \left[\frac{89}{36}, \pi \right]^{(\pi-1)} + 89\,i$$

onde é $\pi = 4$, $\aleph^{(3)} = 42$, e

$$x = 1 - 42 + 89\,i$$

ou

$$x = 48 + 89\,i.$$

Dispensamo-nos de continuar no calculo das raizes, que se effectuava analogamente, convindo em seguida dar um novo valor a k.

RESOLUCÃO GERAL DE CONGRUENCIAS FUNDAMENTAES DE SEGUNDA ORDEM

15. Para effectuar a resolução das congruencias fundamentaes de segunda ordem

$$z^n - ay^n \equiv 0 \pmod{=\mathrm{M}}$$

temos, segundo se deduziu no n.° 77, D. I., que formar a expressão

$$\alpha = (-1)^{\omega+1} . \aleph \left[\frac{\mathrm{M}}{a}, \omega \right]^{(\omega-1)} + \mathrm{M}\,i \ldots\ldots (21)$$

e em seguida resolver a congruencia

$$x^n \equiv \alpha \pmod{=\mathrm{M}} \ldots\ldots\ldots\ldots (22)$$

determinar os residuos da congruencia

$$(1^{k|1})^2 \equiv f(k) \pmod{=\mathrm{M}} \ldots\ldots\ldots (23)$$

e comparal-os com as raizes de (22); aquelles valores de k para

os quaes houver resultados eguaes são os que devem ser introduzidos nas expressões das raizes

$$z = h + (-1)^{\pi+k} . \aleph \left[\frac{\mathbf{M}}{(1^{k|1})^2}, \pi \right]^{(\pi-1)} + \mathbf{M}i_1$$

$$y = h\,(1^{k|1})^2 + (-1)^{k+1} + \mathbf{M}i_2.$$

16. Do que fica dito no numero antecedente deprehende-se a necessidade de formar os quadrados das factoriaes $(1^{k|1})$ para achar os seus residuos segundo o modulo, o que traz o inconveniente de effectuar calculos com numeros muito grandes; póde porém evitar-se, e ao mesmo tempo que vamos ver o meio, trataremos mais especialmente a maneira de obter os valores de k, quando não se obtem facilmente uma raiz da equação (22) que seja identica a um residuo de (23).

Por causa d'esta ultima difficuldade é que convem ter os quadrados das factoriaes $(1^{k|1})$, para obter os valores de $f(k)$ que servem para achar os de k.

Para evitar numeros muito grandes convem calcular logo os residuos de $(1^{k|1})$ segundo o modulo M, e formar depois os quadrados. Ou podemos formar as expressões

$$(1^{k|1}) = x \quad \alpha = (1^{k|1})^{2n}$$

e resolver a congruencia

$$x^{2n} \equiv \alpha \pmod{= \mathbf{M}}$$

de que depois compararemos os residuos com os da factorial $1^{k|1}$, para determinarmos os valores de k que havemos de substituir nas expressões das raizes.

17. Seja a equação de congruencia

$$z^5 - y^5 \equiv 0 \pmod{= 11}.$$

Calculando a funcção $\aleph\left[\frac{M}{a}, \omega\right]^{(\omega-1)}$

n'este caso $\aleph\left[\frac{11}{1}, \omega\right]^{(\omega-1)}$

que entra em (21), vê-se que é $\omega = 1$,

$$\aleph\left[\frac{11}{1}, 1\right]^{(0)} = 1$$

portanto $\alpha = 1 + 11i,$

e a congruencia (22) torna-se em

$$x^5 \equiv 1 \pmod{=11}.$$

Esta equação para $k = 2$ dá $T_1 = 1$, e $x = 3$, notando que com este genero já não se podia obter mais nenhuma raiz; e como 3 é um residuo de

$$(1^{k|1})^2 = f(k) \pmod{=11}$$

para $k = 2$, vamos substituir por k este valor nas expressões das raizes, temos

$$z = h + (-1)^{\pi} . \aleph\left[\frac{11}{4}, \pi\right]^{(\pi-1)} + 11i_1$$

$$y = 4h - 1 + 11i_2$$

e como é $\pi = 3$

$$\aleph\left[\frac{11}{4}, 3\right]^{(2)} = 3,$$

resulta

$$z = (h-3) \quad + \mathrm{M}\, i_1$$

$$y = (4h-1) + \mathrm{M}\, i_2,$$

onde fica h arbitrario determinando os differentes valores que podem ter as raizes.

18. Para as equações de congruencia da fórma

$$z^m - y^m \equiv 0 \pmod{=1}$$

resulta

$$\alpha = 1 + i$$

$$x = 1 + i,$$

e

$$z = h + i_1$$

$$y = (4h-1) + i_2$$

o que mostra, como era evidente, que a equação proposta é satisfeita por quaesquer valores inteiros das variaveis.

RESOLUÇÃO GERAL D'UMA CONGRUENCIA DE TERCEIRA ORDEM

19. Vamos resolver a equação de congruencia de 3.ª ordem que Wronski apresenta (Messianisme 1.° pag. 199)

$$\left.\begin{array}{l} 1+2x_1+\ 7x_1+17x_1\ x_2 \\ +3x_2+11x_2+19x_1\ x_3 \\ +5x_3+13x_3+23x_2x_3 \end{array}\right\} \equiv 0 \pmod{=61}.$$

A expressão generatriz do modulo é

$$M=\text{fact.}\left\{\begin{array}{l} (1^{k_1|1})^4.(1^{k_2|1})^4.(1^{k_3|1})^4+ \\ +2(1^{k_1|1})^2.(1^{k_2|1})^4.(1^{k_3|1})^4.H_1+\ 7\ (1^{k_2|1})^4.(1^{k_3|1})^4.H_1{}^2 \\ +3\,(1^{k_1|1})^4.(1^{k_2|1})^2.(1^{k|_31})^4.H_2+11.(1^{k_1|1})^4.(1^{k_3|1})^4.H_2{}^2 \\ +5\,(1^{k_1|1})^4.(1^{k_2|1})^4.(1^{k_3|1})^2.H_3+13\ (1^{k_1|1})^4.(1^{k_2|1})^4.H_3{}^2 \\ +\ (1^{k_1|1})^2.(1^{k_2|1}).(1^{k_3|1})^2.[17.(1^{k_3|1})^2.H_1.H_2+ \\ \qquad +19(1^{k_2|1})^2.H_1.H_3+23.(1^{k_1|1})^2.H_2.H_3] \end{array}\right\}$$

e temos a ver quaes são os valores combinados de k_μ, h_μ, que satisfazem a esta equação, os quaes devem ser depois introduzidos nas formulas (62) D. I., e darão as raizes da proposta.

Para isso, segundo o que se viu no n.° 83, formam-se as equa-

ções de congruencia correspondentes ás equações (64) D. I.,

$$S_1 + (1^{k_1|1})^4.(1^{k_2|1})^4.(1^{k_3|1})^4 + 2\,(1^{k_1|1})^2.(1^{k_2|1})^4.(1^{k_3|1})^4.H_1 +$$

$$+ 7.(1^{k_2|1})^4.(1^{k_3|1})^4.H_1^2 \equiv 0 \pmod{=M}$$

$$S_2 + 3\,(1^{k_1|1})^4.(1^{k_2|1})^2.(^{k_3|1})^4.H_2 +$$

$$+ 11.(1^{k_1|1})^4.(1^{k_3|1})^4.H_2^2 \equiv 0 \pmod{=M}$$

$$S_3 + 5.(1^{k_1|1})^4.(1^{k_2|1})^4.(1^{k_3|1})^2.H_3 +$$

$$+ 13.(1^{k_1|1})^4.(1^{k_2|1})^4.H_3^2 \equiv 0 \pmod{=M}$$

$$S_4 + (1^{k_1|1})^2.(1^{k_2|1})^2.(1^{k_3|1})^2 \times$$

$$\times [17.(1^{k_3|1})^2.H_1.H_2 + 19.(1^{k_2|1})^2.H_1.H_3 +$$

$$+ 23.(1^{k_1|1})^2.H_2.H_3] \equiv 0 \pmod{=M}$$

sendo $S_1 + S_2 + S_3 + S_4 \equiv 0 \pmod{=M}$,

e onde $H_\mu{}^n$ é da fórma

$$H_\mu{}^n = [h_\mu\,(1^{k_\mu|1})^2 + (-1)^{k_\mu+1}]^n$$

d'onde se tira

$$H_1 = [h_1\,(1^{k_1|1})^2 + (-1)^{k_1+1}]$$

$$H_1^2 = [h_1\,(1^{k_1|1})^2 + (-1)^{k_1+1}]^2$$

$$H_2 = [h_2 (1^{k_2|1})^2 + (-1)^{k_2+1}]$$

$$H_2^2 = [h_2 (1^{k_2|1})^2 + (-1)^{k_2+1}]^2$$

$$H_3 = [h_3 (1^{k_3|1})^2 + (-1)^{k_3+1}]$$

$$H_3^2 = [h_3 (1^{k_3|1})^2 + (-1)^{k_3+1}]^2.$$

Teriamos, para

$$h_1 = 0, \quad h_2 = 0, \quad h_3 = 0$$

$$H_1 = (-1)^{k_1+1}, \quad H_2 = (-1)^{k_2+1}, \quad H_3 = (-1)^{k_3+1},$$

$$H_1^2 = (-1)^{2(k_1+1)}, \quad H_2^2 = (-1)^{2(k_2+1)}, \quad H_3^2 = (-1)^{2(k_3+1)},$$

para $h_1 = 1, \quad h_2 = 1, \quad h_3 = 1.$

$$H_1 = [(1^{k_1|1})^2 + (-1)^{k_1+1}], \quad H_1^2 = [(1^{k_1|1})^2 + (-1)^{k_1+1}]^2$$

$$H_2 = [(1^{k_2|1})^2 + (-1)^{k_2+1}], \quad H_2^2 = [(1^{k_2|1}) + (-1)^{k_2+1}]^2$$

$$H_3 = [(1^{k_3|1})^2 + (-1)^{k_3+1}], \quad H_3^2 = [(1^{k_3|1}) + (-1)^{k_3+1}]^2$$

etc.

E effectuadas as operações expostas no n.º 83 D. I. para o calculo dos valores k_μ, h_μ encontra-se como gerando o modulo,

$$h_1 = 0, \quad h_2 = 1, \quad h_3 = 0$$

e

$$k_1 = 2, \quad k_2 = 2, \quad k_3 = 3.$$

Estes valores substituidos nas expressões (62) D. I. das raizes dão

$$x_1 = 15 + 61i$$

$$x_2 = 16 + 61i$$

$$x_3 = 39 + 61i.$$

EQUAÇÕES INDETERMINADAS

RESOLUÇÃO GERAL DE ALGUMAS EQUAÇÕES INDETERMINADAS

20. A importancia das equações da fórma

$$z^n - B q^n = A p^n \quad \ldots\ldots\ldots\ldots (24)$$

e

$$z^n - B q^n = A \quad \ldots\ldots\ldots\ldots (25)$$

obriga-nos a tratar mais especialmente estes casos a que nos referimos nos n.os 92, 93 e 94 (D. I).

21. A equação $z^n - B q^n = A p^n$

de que se mostrou o modo de determinar as raizes no n.º 92, D. I., póde ainda ser resolvida mais facilmente.

Com effeito attendendo a que os valores de z, q e p são

$$z = h_1 + (-1)^{\pi_1 + k_1} . N\left[\frac{M}{(1^{k_1}|1)^2}, \pi_1\right]^{(\pi_1 - 1)} + A i_1$$

$$q = h_1 (1^{k_1}|1)^2 - (-1)^{k_1} + A i_2$$

e

$$z = h_2 + (-1)^{\pi_2+k_2} \cdot \aleph\left[\frac{M}{(1^{k_2}|1)^2},\ \pi_2\right]^{(\pi_2-1)} + Bj_1$$

$$p = h_2 (1_1^{k_2}|1)^2 - (-1)^{k_2} + Bj_2$$

substituiremos na equação (72) D. I.,

$$K = h_1 + \aleph_1 \quad L = h_1 (1^{k_1}|1)^2 - (-1)^{k_1}$$

$$K_1 = h_2 + \aleph_2 \quad L_1 = h_2 (1^{k_2}|1)^2 - (-1)^{k_2},$$

e teremos para valor de q no caso de $m = 0$

$$q^n = \frac{[(\alpha+1)(h_1+\aleph_1) - \alpha(h_2+\aleph_2)]^n - A[h_2 (1^{k_2}|1)^2 - (-1)^{k_2}]^n}{B} \quad (26)$$

sendo os valores correspondentes de z e p

$$z = (\alpha+1)(h_1+\aleph_1) - \alpha(h_2+\aleph_2)$$

$$p = h_2 (1^{k_2}|1)^2 - (-1)^{k_2}.$$

Resta determinar h_1 e h_2 de modo a tornarem o segundo membro de (26) uma potencia exacta do gráo n: notando que aquellas quantidades têm $\frac{1}{2}$ A e $\frac{1}{2}$ B para limite absoluto.

Desenvolvamos q^n segundo as potencias de h_1, ficarão os coeffi-

cientes compostos com h_2 e será

$$q^n = A_0 + A_1 h_1 + A_2 h_1^2 + A_3 h_1^3 + \ldots + A_n h^n.$$

Calculemos os valores dos coefficientes temos

$$A_0 = \frac{[(\alpha+1).\aleph_1 - \alpha(h_2+\aleph_2)]^n - M[h_2(1^{k_2|1}) - (-1)^{k_2}]^n}{B} =$$

$$= \frac{[(\alpha_1+1)[(\aleph_1-\aleph_2)-h_2]+(h_2+\aleph_2)]^n - E}{B}$$

$$= \frac{[(\alpha+1).F+(h_2+\aleph_2)]^n - E}{B}$$

tendo feito

$$M[h_2(1^{k_2|1})^2 - (-1)^{k_2}]^n = E$$

$$[(\aleph_1-\aleph_2)-h_2] = F,$$

e desenvolvendo a potencia n que entra no valor de A_0 resulta

$$A_0 = \frac{1}{B}\left\{[h_2+\aleph_2]^n + n[h_2+\aleph_2]^{n-1}.(\alpha+1).F + \right.$$

$$\left. + \frac{n^{2|-1}}{1^{2}1}.[h^2+\aleph_2]^{n-1}.(\alpha+1)^2.F^2 + \ldots + (\alpha+1)^n.F^n - E\right\}.$$

Façamos

$$\frac{[h_2+\aleph_2]^n-E}{B}=G$$

$$(\alpha+1).F+(h_2+\aleph_2)=I$$

ter-se-ha

$$A_0=G+\frac{\alpha+1}{B}.F.[I^{n-1}+(h_2+\aleph_2).I^{n-2}+$$

$$+(h_2+\aleph_2)^2.I^{n-3}+\ldots+(h_2+\aleph_2)^{n-1}]$$

$$=G+F.K.L$$

fazendo

$$\frac{\alpha+1}{B}=(-1)^{\pi+1}.\aleph\left[\frac{A}{B},\pi\right]^{\pi-1}=K$$

$$I^{n-1}+(h_2+\aleph_2).I^{n-2}+(h_2+\aleph_2)^2.I^{n-3}+\ldots+(h_2+\aleph_2)^{n-1}=L,$$

e notaremos que são inteiras as quantidades G, F, K, L.

$$A_1=\frac{n}{1}.I^{n-1}.K$$

$$A_2=\frac{n^{2|-1}}{1^{2|1}}.I^{n-2}.K.(\alpha+1)$$

.....

$$A_l = \frac{n^{l|-1}}{1^{l|1}} . I^{n-l} . K (\alpha + 1)^{l-1}$$

. . . . . .

$$A_n = K . (\alpha + 1)^{n-1}.$$

Conhecidos assim os coefficientes do desenvolvimento de q^n calcularemos para esta quantidade os valores correspondentes aos que formos dando a h_2.

Temos pois conhecido para todos os valores de h_2, e um determinado de h_1

$$F (h_1) = A_0 + A_1 . h_1 + A_2 . h_1^2 + \ldots + A_n . h_1^n,$$

e obteriamos o valor de

$$F (h_1 \pm 1) = B_0 + B_1 . h_1 + B_2 . h_1^2 + \ldots + B_n . h_1^n$$

calculando os coefficientes d'esta funcção pelas expressões (20).

O calculo das raizes z e p effectuar-se-hia immediatamente com os elementos conhecidos.

22. Supponhamos a equação indeterminada

$$z^n - B q^n = A.$$

No n.º 93 D. I., vimos como se determinavam as raizes d'esta equação, dependendo essa determinação de tornar racional

$$\left[A_0 + A_1 h + A_2 h + \ldots + A_n h^n\right]^{\frac{1}{n}}$$

que segundo a egualdade (73) é egual a q.

A existencia de limites que h não póde exceder dá logar a que d'este modo fique simplificado o problema, apesar de ainda depender da resolução d'uma equação indeterminada.

Succede além d'isso que ha um caso em que póde simplificar-se a resolução da equação proposta.

Com effeito suppondo que se deu ao numerador da expressão de y^n no n.° 93 D. I. a fórma

$$[(\alpha+1)(K-K_1)+AB.m+K_1]^n-A$$

vê-se immediatamente que todo o numerador mesmo a parte K_1^n-A é divisivel por B: se além d'isso o quociente d'esta divisão for uma potencia do grão n, vejamos o que succede.

Seja a aquelle quociente, operando de modo que seja nulla a differença entre os dois valores de z que se combinaram resultará

$$q=L+Ai=a$$

sendo $$K-K_1=0$$

a equação que determina o valor de h com que hão de obter-se os valores de K e L.

Quando for conhecido um systema de valores para z e q correspondentes a $m=0$, vamos ver como podem obter-se novos valores para estas quantidades aproveitando as fórmulas de pag. 119, D. I.

$$z=K+\alpha(K-K_1)+ABm$$

$$q=L+Ai$$

Sejam Z e Q os valores obtidos, será

$$z = Z + AB\,m$$

$$q = Q + A\,i.$$

Substituindo estas expressões na proposta, para cada valor de m, i será determinado pela egualdade

$$(Z + A.B.m)^n - B\,(Q + A\,i)^n = A$$

d'onde

$$(Q + A\,i)^n = \frac{(Z + A.B.m)^n - A}{B}$$

e estamos reduzidos a procurar valores para m que tornem o segundo membro d'esta egualdade uma potencia do gráo n para termos os valores i, e porisso de q: e com o valor de m achado teremos o correspondente para z.

23. A equação proposta (25) póde ainda ser resolvida como um caso particular da equação de 3.ª ordem (24), e pelo methodo apresentado no n.º (21).

Designando por $(\aleph_2)$ a quantidade correspondente a $\aleph_2$, e que é

$$(\aleph_2) = \left[T_n\right]^n . \left[(-1)^{\pi-1} . \aleph\left[\frac{B}{(1^{k|1})^2}, \pi\right]^{(\pi-1)}\right]^\mu + Bj$$

teremos

$$q^n = \frac{[(\alpha + 1)\,(h + \aleph_1) - \alpha\,(\aleph_2)]^n - A}{B}$$

$$z = (\alpha + 1).(h + \aleph_1) - \alpha\,(\aleph_2).$$

Entra agora em q^n só uma especie h que determinaremos de modo que o segundo membro seja uma potencia inteira do gráo n; e conhecidos os valores de q e z para um determinado valor de h por exemplo $h=0$ immediatamente conheceremos os que correspondem a outros valores da maneira que está indicada.

24. Seja a equação

$$z^3 - 5\,y^3 = 11\,u^3.$$

Temos a resolver primeiramente a equação

$$z^3 - 5\,y^3 \equiv 0 \pmod{=11}.$$

É $$\alpha = -2 + 11j = 9 - 11j,$$

e $$x^6 \equiv 9 \pmod{=11}$$

tem para raiz $$x = 9,$$

resultando $$k = 2:$$

pelo que as expressões das raizes são

$$z = (h_1 - 3) + 11i, \quad h_1 + \aleph_1 = h_1 - 3$$

$$y = (4h_1 - 1) + 11i.$$

Em seguida temos a congruencia

$$z^3 - 11\,u^3 \equiv 0 \pmod{=5}$$

de que as raizes são dadas pelas expressões respectivas fazendo $k = 3$ e vem

$$z = (h_2 + 1) + 5j_1 \quad h_2 + \aleph_2 = h_2 + 1$$

$$u = (36\,h_2 + 1) + 5j_2.$$

Ora n'este caso é

$$\alpha + 1 = -10$$

logo

$$y^3 = \frac{[10\,(3 - h_1) + 11\,(h_2 + 1)]^3 - 11\,.\,[36\,h_2 + 1]^3}{5}$$

$$= \frac{[41 - 10\,h_1 + 11\,h_2]^3 - 11\,.\,[36\,h_2 + 1]^3}{5},$$

$$z = 41 - 10\,.\,h_1 + 11\,.\,h_2,$$

$$u = 36\,.\,h_2 + 1,$$

onde h_1 e h_2 tem para limites absolutos 6 e 3.

Desenvolvamos y^3 para effectuar o calculo dos valores de h_1 e h_2, e para isso formemos as quantidades auxiliares que entram na composição dos coefficientes; temos

$$\mathrm{I} = -10\,.\,[-4\,h_2] + (h_2 + 1) = 41 + 11\,h_2$$

$$\mathrm{G} = \frac{(h_2 + 1)^3 - 11\,.\,[36\,h_2 + 1]^3}{5}$$

$$\mathrm{K} = -2$$

$$\mathrm{L} = (41 + 11\,.\,h_2)^2 + (h_2 + 1)\,(41 + 11\,.\,h_2) + (h_2 + 1)^2,$$

e para valores dos coefficientes

$$A_0 = G + 2.[h_2 + 4].L$$

$$A_1 = -6(41 + 11.h_2)^2$$

$$A_2 = 60.(41 + 11.h_2)$$

$$A_3 = -200.$$

Portanto a expressão de y^3 é

$$y^3 = G + 2(h_2 + 4).L - 6(41 + 11.h_2)^2 +$$

$$+ 60.(41 + 11.h_2)\,h_1^2 - 200\,h_1^3.$$

Os coefficientes relativos aos differentes valores que temos a dar a h_2 são

$(A_0)_0 = -\ 9782\,(A_1)_0 = -10086\,(A_2)_0 = 2460\,(A_3)_0 = -200$

$(A_0)_1 = -\ 83315\,(A_1)_1 = -16224\,(A_2)_1 = 3120\,(A_3)_1 = -200$

$(A_0)_{-1} = \ 99725\,(A_1)_{-1} = -\ 5400\,(A_2)_{-1} = 1800\,(A_3)_{-1} = -200$

$(A_0)_2 = -\ 805828\,(A_1)_2 = -23814\,(A_2)_2 = 3780\,(A_3)_2 = -200$

$(A_0)_{-2} = \ 831120\,(A_1)_{-2} = -\ 2166\,(A_2)_{-2} = 1140\,(A_3)_{-2} = -200$

$(A_0)_{-3} = -2768019\,(A_1)_3 = -32856\,(A_2)_3 = 1440\,(A_3)_3 = -200$

$(A_0)_{-3} = \ 2695205\,(A_1)_{-3} = -\ 384\,(A_2)_{-3} = \ 480\,(A_3)_{-3} = -200$

effectuando o calculo das funcções $F(h_1)_{h_2}$ obtem-se

$F(0)_0 = 9782$ $F(1)_0 = 1956$ $F(-1)_0 = 22528$

$F(2)_0 = 4150$ $F(-2)_0 = 41394$

$F(3)_0 = 3766$ $F(-3)_0 = 67580$

$F(4)_0 = -4002$ $F(-4)_0 = 102286$

$F(5)_0 = -4148$ $F(-5)_0 = 146712$

$F(6)_0 = 5374$ $F(-6)_0 = 202058$

etc.,

sendo o methodo mais rapido para calcular estas funcções o que em seguida se indica, por exemplo para calcular $F(1)_3$ e $F(-1)_3$, $F(2)_3$ e $F(-2)_3$, etc.

$$
\begin{array}{rrrrr}
(A_0)_3 = & -2768019 & , & = & -2768019 \text{ etc.} \\
(A_1)_3 = & -32856 & , \; 2(A_1)_3 = & -65712 & \\
(A_3)_3 = & -200 & , \; 8(A_3)_3 = & -1600 & \\
\hline
 & -2801075 & , & & 2835331 \\
(A_2)_3 = & 1440 & , \; 4(A_2)_3 = & 5760 & \\
\hline
F(1)_3 = & -2799635 & , \; F(2)_3 = & -2829571 & \\
 & 34496 & & 73072 & \\
\hline
F(-1)_3 & -2733523 & , \; F(-2)_3 = & -2694947. &
\end{array}
$$

Feito o calculo veriamos que nenhuma das funcções obtidas era uma potencia exacta do 3.º gráo pelo que tinhamos a concluir: — *Que o cubo d'um numero inteiro não póde ser decomposto na somma dos productos que se obtêm multiplicando dois cubos de quaesquer numeros inteiros, um por 5 e outro por 11.*

25. Seja a equação

$$z^3 - 2u^3 = 127.$$

Tem de resolver-se as duas equações de congruencia

$$z^3 - 2u^3 \equiv 0 \pmod{=127} \ldots\ldots\ldots (27)$$

e

$$z^3 - 127 \equiv 0 \pmod{=2} \ldots\ldots\ldots (28).$$

Para a resolução de (27) temos

$$\alpha = 64$$

e que resolver $x^3 \equiv 64 \pmod{=11}$

de que é raiz $x = 4.$

Ora da equação

$$(1^{k|1})^2 \equiv f(k) \pmod{=M}$$

é n'este caso 4 um residuo para $k = 2.$

É portanto

$$z = (h - 32) + 127 i_1$$

$$u = (4h - 1) + 127 i_2.$$

A equação de congruencia (28) tem para raiz

$$z = 1 + 2j.$$

O valor de α_1 é

$$\alpha_1 = -2.63 - 1 = -126 - 1.$$

E teremos para o caso de $m = 0$, attendendo a que é

$$h + \aleph_1 = h - 32 \quad \text{e} \quad (\aleph_2) = 1,$$

$$y^3 = \frac{[-126(h-32)+127.]^3 - 127}{2} =$$

$$= \frac{(4159 - 126.h)^3 - 127}{2}.$$

E como calculando esta expressão viamos, que não se encontrava valor algum de h para o qual se tornasse no cubo d'um numero inteiro, concluiriamos — *Que, a somma do dobro do cubo d'um numero inteiro qualquer com* 127, *não póde ser um cubo exacto.*

26. Seja a equação

$$z = 2x^3 - 5y^2 \ldots\ldots\ldots\ldots (29).$$

Trata-se de ver se ha numeros que possam ser representados pela differença entre o dobro do cubo e cinco vezes o quadrado d'um numero inteiro.

Resolvamos a equação de congruencia

$$2x^3 - 5y^2 \equiv 0 \pmod{=1}.$$

É, segundo a fórmula que nos dá o modulo n.° 82, D. I.,

$$M = \text{fact.}\,[(1_3).W_{1_3}.W_{2_0} + (2_2).W_{1_0}.W_{2_2}]$$

sendo $W_{1_3} = (H_1)^3$, $W_{2_0} = (1^{k_2|1})^4$

$W_{1_0} = (1^{k_1|1})^6$, $W_{2_2} = (H_2)^2$,

logo

$$M = \text{fact.}\,[2.(1^{k_2|1})^4.H_1^3 - 5.(1^{k_1|1})^6.H_2^2]$$

a que satisfazem quaesquer valores de k e h, e temos

$$x = \alpha + i_1 \quad y = \alpha + i_2$$

expressões em que α é um numero inteiro qualquer.

Analogamente resolve-se a congruencia

$$2x^3 - z \equiv 0 \pmod{=5};$$

é $$M = \text{fact.}\,[2.(1^{k_2|1})^2.H_1^3 - (1^{k_1|1})^6.H_2]$$

e teremos pelas expressões (64) e 65) D. I.,

$$S_1 + 2.(1^{k_2|1})^2.H_1^3 \equiv 0 \pmod{=5}$$

$$S_2 - (1^{k_1|1})^6.H_2 \equiv 0 \pmod{=5}$$

$$S_1 + S_2 \equiv 0 \pmod{=5},$$

$$H_1 = h_1(1^{k_1|1})^2 + (-1)^{k_1+1}, \quad H_2 = h_2(1^{k_2|1})^2 + (-1)^{k_2+1},$$

pelo que resultam para k e h os valores

$$k_1 = k_2 = 2, \quad h_1 = 0, \quad h_2 = 1$$

e para as raizes

$$x = 1 + 5j'_1, \quad z = 2 + 5j''_2.$$

A congruencia

$$5y^2 + z \equiv 0 \pmod{=2}$$

dá $$M = \text{fact.}\,[5.(1^{k_2|1})^2.H_1{}^2 + (1^{k_1|1})^4.H_2]$$

expressão que é satisfeita por $k_1 = k_2 = 2$ e quaesquer valores de h: portanto é

$$y = h + 2i'_1 \quad z = -h + 2i'_2$$

sendo h um inteiro qualquer.

Combinando agora conforme ao modo que se indicou no n.º 85 D. I. os 2 valores obtidos para cada uma das raizes por meio das 3 equações de congruencia, temos os seguintes resultados

$$x = 1 + 5j_1$$

$$y = h + 2j_2$$

$$z = -(5h + 8) + 10j_3$$

e como podemos dar a uma das quantidades $j_1\ j_2\ j_3$ um valor qualquer comtanto que determinemos as outras; seja $j_1 = 0$,

..

e substituamos os valores de x, y, z na equação proposta, resulta

$$-(5h+8)+10j_3=2-5h^2-20j_2^2-20hj_2\ldots\ (30)$$

d'onde

$$4j_2^2+4hj_2+h_2-h-2\equiv 0\ (\text{mod.}=2).$$

O valor de k que torna a expressão generatriz do modulo d'esta congruencia divisivel por 2 é

$$k=2,$$

e porisso é

$$j_2=h_1+(-1)^{\pi}.\aleph\left[\frac{2}{4},\ \pi\right]^{(\pi-1)}+2i$$

ou $$j_2=h_1.$$

Substituindo na equação (30) este valor de j_2 teremos immediatamente o de j_3

$$j_3=\frac{2+h(1-h)-4h_1(h_1-h)}{2}\ldots\ldots\ (31)$$

e como $h\ (1-h)$ é sempre um numero par qualquer que seja o valor inteiro dado a h, segue-se, que poderemos em (31) dar a h e h_1 todos os valores inteiros resultando os de j_3 que se procuravam.

Os valores das incognitas que satisfazem a (29) são portanto

$$x=1$$

$$y=h+2h_1$$

$$z=-(5h+8)+10j_3$$

em que j_3 é dado pela fórmula (31).

D'onde se conclue — *Que os numeros inteiros da fórma* $-(5h+8)+10j_3$ *são dados pela expressão* (29), *sendo* x *da fórma* 1, y *da fórma* $h+2h_1$, *e tendo em vista a fórmula* (31).

27. Vejamos se o numero 107 póde ser dado por uma expressão da fórma $3x^2+7xy+y^2$: isto é trata-se de ver se é possivel satisfazer em numeros inteiros á equação

$$107=3x^2+7xy+y^2.$$

Resolvamos a equação de congruencia

$$7xy+y^2\equiv 107 \pmod{=3},$$

temos

$$M=\text{fact.}[-107.(1^{k_1|1})^4.(1^{k_2|1})^2+7.(1^{k_1|1})^2.H_1.H_2+$$

$$+(1^{k_2|1})^2H_1^2].$$

E formando as expressões (64) e (65) D. I., encontrariamos que

$$k_1=k_2=2,\quad h_1=0,\quad h_2=3$$

satisfazem a esta relação. Substituindo em consequencia estes valores nas expressões das raizes teremos estas

$$x=2+3i_1$$

$$y=-1+3i_2.$$

Substituamos estes valores na equação proposta; o resultado

que se obtem depois de fazer $i_1 = 0$, o que podemos segundo se disse no n.° 85 D. I., é

$$i_2^2 + 4i_2 - 12 = 0$$

a que satisfaz

$$i_2 = 2.$$

Concluimos portanto — *Que o numero* 107 *póde ser decomposto na somma* $3x^2 + 7xy + y^2$, *sendo* $x = 2$, $y = 5$.

FIM.

INDICE

1885 C. LOBO - DISSERTAÇÃO DE CONCURSO MATHEMATICA