Said Sidki

INTRODUÇÃO À TEORIA DOS NÚMEROS

PREFÁCIO

Dos charmes da Teoria dos Números, muitos matemáticos cantaram. Da sua importância, basta-nos dizer que uma parte apreciável da árvore matemática brotou-se de problemas sobre os números inteiros.

Pretendemos com o presente trabalho apresentar certos aspectos da teoria, considerados elementares, e que são relacionados a esses problemas.

Supomos de pré-requisitos um bom primeiro curso de álgebra (por exemplo, do livro de autoria de Jacy Monteiro [15]), e os primeiros cursos universais de cálculo. Em certos pontos usamos os números complexos.

Nas referências, o leitor encontrará um farto material para estudos posteriores ou complementares.

Finalmente, extendemos os nossos agradecimentos a comissão organizadora do 10º Colóquio Brasileiro de Matemática que nos encarregou para dar este curso, e ao IMPA onde essas notas foram preparadas.

ÍNDICE

CAPÍTULO I

DIVISÃO

1.1. Divisibilidade

Definição 1. Sejam a, b inteiros. Dizemos que a divide b, denotado por $a|b$, se e somente se existe um inteiro c tal que $b = ac$. A notação $a\nmid b$ significa que a não divide b. Notamos que c é único quando $a \neq 0$; pois se c' é um outro inteiro satisfazendo $b = ac'$, então,

$$0 = ac - ac' = a(c - c'),$$

donde, pela lei do cancelamento, $c = c'$.

Teorema 2. Sejam a, b e c inteiros. Então, valem as seguintes implicações para β, σ inteiros quaisquer.

(1) $a|b,\ b > 0 \Longrightarrow a \leq b,$

(2) $ab = 1 \Longrightarrow a = \pm 1,$

(3) $a|b,\ a|b + c \Longrightarrow a|c,$ e
$a|b,\ a\nmid c \Longrightarrow a\nmid b + c,$

(4) $a|b,\ c \Longrightarrow a|\beta b + \sigma c$.

Demonstração. (1) Existe um inteiro c tal que $b = ac$. Suponhamos que $b < a$; então de

$$0 < b < a \quad e \quad 0 < c \ ,$$

obtemos

$$0 < bc < ac = b \ ,$$

e portanto,

$$0 < c < 1 \quad ;$$

um absurdo pelo Exercício 1, I.

(2) Tendo em vista que

$$ab = 1 \Longrightarrow (-a)(-b) = 1 \quad ,$$

podemos supor que a e b são ambos positivos. Da primeira parte deste teorema, obtem-se

$$0 < a \leq 1 \quad , \quad 0 < b \leq 1 \quad ,$$

e assim, pelo Teorema , $a = 1 = b$.

(3) e (4) (Exercício 6, I)

c. q. d.

Teorema 3. (Algoritmo da Divisão) Dados os inteiros a, b com $a \neq 0$, existe um par de inteiros q, r tal que

$$b = qa + r$$

com

$$0 \leq r < |a| \quad .$$

Além do mais, este par é o único satisfazendo essas condições.

Demonstração. Pelo Exercício 2,I, existe um inteiro d tal que $b - da > 0$. Seja

$$S = \{s | s = b - ia \quad \text{com} \quad s \geq 0\}.$$

Então S não é vazio, e portanto possui um elemento mínimo r; $r = b - qa$ para algum inteiro q. Afirmamos que $r < |a|$; pois no caso contrário teremos um absurdo a saber: $r-|a| \in S$ e $r - |a| < r$.

Seja q', r' um outro par satisfazendo as condições do teorema. Podemos supor que $0 < r \leq r' < |a|$; então , $0 \leq r' - r < |a|$.

Da igualdade

$$b = qa + r = q'a + r' \quad ,$$

obtemos

$$0 = b - b = (q - q')a + (r - r')$$

e

$$(q - q')a = r - r' \ ;$$

daí

$$a | r'-r \ .$$

Pela parte (1) do teorema anterior, vale

$$|a| \leq r' - r$$

ou

$$r' - r = 0.$$

O primeiro caso é impossível; então $r = r'$, e daí segue-se que $q = q'$. c.q.d.

Algoritmo 4. O algoritmo para dividir b por a (digamos $b \geq a > 0$) baseia-se na aplicação repetida da subtração, e se procede da seguinte maneira:

(o) seja $b = b_1$,

(i) calcule $b_{i+1} = b_i - a$,

(ii) (a) se $b_{i+1} > 0$, então volte para (i) trocando i por $i + 1$,

(b) se $b_{i+1} \leq 0$, pare; o resultado é

$$b = \begin{cases} ia & , \text{ se } b_{i+1} = 0 \\ (i-1)a + bi, & \text{se } b_{i+1} < 0. \end{cases}$$

Por exemplo, sejam $b = 6$ e $a = 2$. Então, $b_1 = 6$, $b_2 = 4$, $b_3 = 2$, $b_4 = 0$, e daí $i + 1 = 4$ e $b = 3a$.

Outro exemplo. Sejam $b = 7$ e $a = 2$. Então, $b_1 = 7$, $b_2 = 5$, $b_3 = 3$, $b_4 = 1$, $b_5 = -1$, e daí $i + 1 = 5$ e $b = 3a + 1$.

1.2. Representação Posicional dos Inteiros

1.2.1. Genesis do Sistema Decimal. O nosso sistema decimal de numeração é conhecido como Hindu-Arabe e foi desenvolvido na sua forma final cerca de 500 DC pelos astronomos calculistas Hindus, entre os quais destacam-se Bhâskara I e Yinabhadra Gani. A aritmética Hindu foi adotada e divulgada no mun

islâmico cerca de 825 DC pelo matemático arabe Mohamad Ben Mussa Al Khawarismi.

No início do século XII, o monge inglês Adelard de Bath traduziu o livro de aritmética de Al Khawarismi para o latim sob o título de Algoritmi de Numero Indiorum ("Algarismo" e "Algoritmo" são corruptelas óbvias de "Al Khawarismi").

O sistema numérico usado na Europa não Hispânica até então, foi o Romano; os cálculos eram feitos com a ajuda do abacus. Houve um choque entre os dois sistemas, com que se criou dois campos de "guerra numérica", os "Abacistas" e os "Algoristas". Foi um conflito longo que terminou no século XVI com a supremacia do sistema Hindu-Arabe.

A título de comparação, daremos a seguir uma idéia rápida do sistema Romano.

Listamos primeiro os numerais romanos com as representações correspondentes.

ROMANO	I	V	X	L, ⊥ ou ↓	C	D ou ↁ	ↀ , Φ ou M	ↁↁ	ↀↁↁ
DECIMAL	1	5	10	50	100	500	1000	5000	10000

Os números foram representados aditivamente, e até subtrativamente:

II (2), III (3), IIII ou IV (4), ..., VIIII ou IX (9),etc.

A representação Romana de 1975 seria MCMLXXV.

Para somar os números CDLXXVII (477) e LXIX (69) procedeu-se da seguinte maneira:

C C C C L X X V I I
L X V I I I I
C C C C LLXXXVV IIIIII
C C C C C X X X X V I
D X X X X V I (546) .

O sistema Hindu-Arabe é decimal por ter dez algarismos (0, 1, 2, 3, 4, 5, 6, 7, 8, 9), e é posicional, no sentido de que o número se representa como uma sequência ordenada e finita de algarismos. O zero é o indicador da falta de certas potências de dez; um artifício que demorou muito para ser realizado.

O sistema posicional mais antigo conhecido na história é o sistema sexagesimal (de base 60) da Babilonia (cerca 1800 AC). O grande astronomo grego Ptolomeu (cerca 150 DC) usava-o no seu famoso livro Almagest. Vestígios da influência Babilônica são aparentes na divisão da hora em 60 minutos, do minuto em 60 segundos e da circunferência em 360 graus.

Nesta parte do mundo, os Mayas da América Central usavam (cerca 300 AC) um sistema posicional vigesimal (em base 20), e até tinham um símbolo para o zero.

O leitor interessado em prosseguir este assunto deve consultar as referências [10] e [20].

1.2.2. Representação na Base a

Seja a um número natural maior que 1. Mostraremos a seguir um algoritmo para expressar os números inteiros na base a.

Teorema 5. Dado b um número natural, existem k, r_o, r_1, ..., r_k inteiros tais que

$$b = r_k a^k + r_{k-1} a^{k-1} + \ldots + r_1 a + r_o$$

com $k \geq 0$, $0 \leq r_i < a$ para $0 \leq i \leq k$ e $r_k \neq 0$.

Além do mais, esta representação de b é única.

Demonstração. (1) O algoritmo da divisão será usado repetidas vezes para obter a expressão desejada. O processo é o seguinte:

(o) seja $b = q_o$,

(i) calcule q_{i+1}, r_i : $q_i = q_{i+1} a + r_i$ com $0 \leq r_i < a$,

(ii) (a) se $q_i \geq a$, então volte para (i) trocando i por i + 1.

(b) se $q_i < a$, pare; o resultado é $b = r_i a^i + r_{i-1} a^{i-1} + \ldots + r_o$.

A afirmação feita sobre o resultado final baseia-se na observação,

$$b = q_o = q_1 a + r_o = (q_2 a + r_1)a + r_o =$$

$$= ((q_3 a + r_2)a + r_1)a + r_o = \text{etc...}$$

O processo descrito é destinado a parar, porque $q_o > q_1 > \ldots > q_i$.

(2) A unicidade da representação será demonstrada por indução sobre b. Se $b = 1$, então evidentemente $k = 0$ e $r_o = 1$. Suponhamos que o teorema é válido para todo inteiro c tal que $1 \leq c < b$, e sejam

$$r_k a^k + r_{k-1} a^{k-1} + \ldots + r_o$$

$$s_\ell a^\ell + s_{\ell-1} a^{\ell-1} + \ldots + s_o$$

duas representações de b satisfazendo as condições do teorema. Sejam também u e v os primeiros índices para os quais $r_u \neq 0 \neq s_v$. Então temos,

$$b = b' a^u = b'' a^v \quad ,$$

onde

$$b' = r_k a^{k-u} + r_{k-1} a^{k-1-u} + \ldots + r_u$$

$$b'' = s_\ell a^{\ell-v} + s_{\ell-1} a^{\ell-1-v} + \ldots + s_v \ .$$

Primeiro, vamos supor que um dos u, v é diferente de zero; digamos $u \geq v$. Então,

$$b'a^{u-v} = b'' ,$$

e portanto b'' possui as representações,

$$r_k a^{k-v} + r_{k-1} a^{k-1-v} + \ldots + r_u a^{u-v} ,$$

$$s_\ell a^{\ell-v} + s_{\ell-1} a^{\ell-1-v} + \ldots + s_v \quad .$$

Se $b'' < b$, então a hipótese da indução nos dará $k = \ell$, $u=v$ e $r_i = s_i$ para todo i: $u \leq i \leq k$, da qual se conclui facilmente que as duas representações de b são idênticas. A mesma conclusão será tirada se $v \geq u$.

Falta-nos considerar o caso $u = v = 0$. Neste caso ,

$$b = ab_1 + r_o = ab_2 + s_o ,$$

onde

$$b_1 = r_k a^{k-1} + r_{k-1} a^{k-2} + \ldots + r_1 ,$$

$$b_2 = s_\ell a^{\ell-1} + s_{\ell-1} a^{\ell-2} + \ldots + s_1 .$$

Temos,

$$a(b_1-b_2) = s_o-r_o ,$$

e portanto, $a|s_o-r_o$. Lembrando que $0 < s_o, r_o < a$, obtemos que $s_o - r_o = 0$; então, $s_o = r_o$ e $b_1 = b_2$. As duas representações de b_1 são idênticas, porque $b_1 < b$; daí chegamos ao fim da demonstração.

c.q.d.

A representação na base a de b, para $b \leq 0$ é a seguinte:

$$0 \quad \text{se} \quad b = 0,$$

$$-(a^k r_k + a^{k-1} r_{k-1} + \ldots + r_o), \text{ ou simplesmente}$$

$$-r_k r_{k-1} \cdots r_o \text{ , se } b < 0 \text{ , onde}$$

$$(-b) = a^k r_k + a^{k-1} r_{k-1} + \ldots + r_o \text{ .}$$

Exemplo 6. Representaremos o número decimal b = 125 nas bases a = 2, 12.

(i) Sejam a = 2 e 0, 1 os algarismos (mantemos os seus significados usuais: 0 + 0 = 0, 0 + 1 = 1, 1.0 = 0 , 1.1 = 1,etc...). Seguindo o algoritmo da demonstração do teorema anterior temos,

$$125 = 62.2 + 1$$
$$62 = 31.2 + 0$$
$$31 = 15.2 + 1$$
$$15 = 7.2 + 1$$
$$7 = 3.2 + 1$$
$$3 = 1.2 + 1$$
$$1 = 0.2 + 1.$$

Então, $125 = 62.2 + 1 = (31.2 + 0)2 + 1 = \ldots = 1.2^6 + 1.2^5 + 1.2^4 + 1.2^3 + 1.2^2 + 0.2 + 1$, ou simplesmente 1111101.

(ii) Seja a = 12 e sejam 0, 1, 2, 3, ..., 9 , $\alpha(=10)$, $\beta(=11)$ os algarismos. Então,

$$125 = \alpha.12 + 5,$$

ou simplesmente $\alpha 5$.

É bem conhecido que quando o último algarismo na expansão decimal de um número a é um múltiplo de dois, ou cinco, então o mesmo é certo para a. Apresentaremos a seguir alguns critérios deste gênero.

Teorema 7. Seja b um número natural e seja $r_k 10^k + r_{k-1}10^{k-1} + \ldots + r_o$ a sua expansão decimal. Então,

(1) para $\ell \leq k$,

$$2^\ell | b \Longleftrightarrow 2^\ell | r_{\ell-1}10^{\ell-1} + \ldots + r_1 10 + r_o \ ,$$

(2) para $\ell \leq k$,

$$5^\ell | b \Longleftrightarrow 5^\ell | r_{\ell-1}10^{\ell-1} + \ldots + r_1 10 + r_o \ ,$$

(3) para $i \leq 2$,

$$3^i | b \Longleftrightarrow 3^i | r_o + r_1 + \ldots + r_k \ ,$$

(4) $11 | b \Longleftrightarrow 11 | r_o - r_1 + r_2 - r_3 + \ldots$.

Demonstração. (1) $c = r_k 10^k + \ldots + r_\ell 10^\ell$ é divisível por 2^ℓ, tendo em vista que $k \geq \ell$. Então, $2^\ell | b \Longleftrightarrow 2^\ell | b-c$; daí a conclusão desejada.

(2) A demonstração é igual a de (1), só que trocamos 2 por 5.

(3) Notamos aqui que para $i \geq 0$,

$$10^i = (9 + 1)^i = 9^i + \binom{i}{1}9^{i-1} + \ldots + \binom{i}{i-1}9 + 1$$
$$= (9^{i-1} + \binom{i}{1}9^{i-2} + \ldots + \binom{i}{i-1})9 + 1$$
$$= s_i 9 + 1.$$

Substituindo essas expressões para as diversas potências de 10 na expansão de b, obtemos,

$$b = (r_k s_k + r_{k-1}s_{k-1} + \ldots + r_1)9 +$$
$$+ (r_k + r_{k-1} + \ldots + r_o).$$

Assim chegamos a

$$3^i | b \iff 3^i | r_k + r_{k-1} + \ldots + r_o$$

para $i = 1, 2$.

(4) A demonstração desta parte é inteiramente análoga à de (3); em vez de 10, escrevemos (11 - 1).

c.q.d.

1.3. Máximo Divisor Comum - Mínimo Múltiplo Comum

1.3.1. Existência e Forma

O propósito desta secção é de estudar formalmente as noções de máximo divisor comum (m.d.c.) e do mínimo múltiplo comum (m.m.c.) de quaisquer dois inteiros não nulos; o lei

tor sem dúvida, conheceu essas noções na infância.

Definição 8. (i) Sejam a, b inteiros não simultaneamente nulos. Um número natural d chama-se o máximo divisor comum (m.d.c.) de a e b, denotado por (a,b), se e somente se

(1) $d|a, b$,

(2) c inteiro, $c|a,b \Longrightarrow c|d$.

(ii) Sejam a, b inteiros não nulos. Um número natural c chama-se o mínimo múltiplo comum (m.m.c.) de a e b, denotado por [a,b], se e somente se

(1) $a,b|c$,

(2) f inteiro, $a,b|f \Longrightarrow c|f$.

Observação 9. A segunda parte da definição do m.d.c. garante a unicidade de d; porque se d' é um outro, então por (2) $d|d'$ e $d'|d$ e portanto $d = d'$. Fazemos o mesmo comentário a respeito do m.m.c..

Teorema 10. Sejam a, b inteiros não simultaneamente nulos. Então existe d, o máximo divisor comum de a e b. Além do mais, d é uma combinação linear de a e b; isto é, existem inteiros α, β tais que $d = \alpha a + \beta b$.

Demonstração. Consideremos $I = \{a\alpha + \beta b | \alpha, \beta \in Z\}$. Eis alguns elementos de I: $a(= 1a + 0.b)$, $-a(= -1a + 0.b)$, $\pm b$, $a + b(=1.a + 1.b)$.

I é um subconjunto não trivial de Z com as seguintes propriedades notáveis,

(1) I é fechado para a soma:

$$(\alpha_1 a + \beta_1 b) + (\alpha_2 a + \beta_2 b) = (\alpha_1+\alpha_2)a + (\beta_1+\beta_2)b \ ,$$

(2) dado $c \in Z$ e $f\ (=\alpha a + \beta b) \in I$, então $cf \in I$: $cf = c(\alpha a + \beta b) = (c\alpha)a + (c\beta)b$; em síntese, I é um ideal de Z.

I contém inteiros; pois a, -a, b e -b ε I. Então I^+, a parte positiva de I, não é vazia. Assim, pelo axioma da boa ordem, existe $d \in I^+$ que é o menor elemento de I^+. d já tem a forma certa:

$$d = \alpha' a + \beta' b \quad \text{para alguns inteiros } \alpha', \beta' \ .$$

Todo elemento de I, e em particular a e b, é um múltiplo de d: pelo algoritmo da divisão, existem inteiros q, r tais que

$$a = qd + r, \quad 0 \leq r < d \ ;$$

pela propriedade (2) de I, $(-q)d \in I$, e pela propriedade (1), tendo em vista que $a, (-q)d \in I$, obtem-se $a-qd(=r) \in I$; dado a minimalidade de d, r = 0. Finalmente, se $c \in Z$ e $c|a$, b, então como $d = \alpha' a + \beta' b$, $c|d$.

c.q.d.

Comentário 11. O ideal I foi construído a partir de todas as combinações lineares de a e b; o que se expressa diferentemente dizendo que I foi gerado por a e b. A demonstração revelou a possibilidade de substituir os dois geradores por d, um só gerador.

Perguntamos: "Que tal se I fosse gerado por três, ou quatro, etc... elementos? Será que é sempre possível arranjar um só gerador para I?". Para colocar a resposta numa forma exata, seria conveniente dar a seguinte definição:

Seja R um anel comutativo com identidade, e seja I um ideal de R. I chama-se ideal principal, se existir $a \in R$ tal que

$$I = Ra = \{ra | r \in R\} .$$

Se todos os ideais de R são principais então R chama-se um anel principal.

A resposta a pergunta é um resultado importante.

Teorema 12. Z é um anel principal.

Demonstração. (Exercício 17, I ; modifique a demonstração do teorema anterior).

2.3.2. O Algoritmo Euclidiano

Nota Histórica 13. Euclides, conhecido como o maior mestre de geometria de todos os tempos, era um professor de

matemática em Alexandria-Egito, por volta de 300 AC. Ele coleccionou, ordenou e explicou o conhecimento matemático -aritmética, geometria - de seu tempo, em treze livros chamados Os Elementos; três desses tratavam de aritmética. O algoritmo Euclideano, para calcular o maior divisor comum, encontra-se no início do Livro VII dos Elementos.

Algoritmo 14. Sejam a, b um par de números naturais não nulos ((0,0) não tem sentido, e (a,0) = a, se $a \neq 0$). Para produzir (a,b) seguiremos o seguinte processo:

(o) sejam $a = a_1$, $b = a_2$,

(i) calcule q_i, a_{i+2} :

$$a_i = q_i a_{i+1} + a_{i+2} \quad ,$$

com

$$0 \leq a_{i+2} < a_{i+1} \quad ,$$

(ii) (a) se $a_{i+2} \neq 0$, então volte para (i) trocando i por i + 1,

(b) se $a_{i+2} = 0$, pare; o resultado é $a_{i+1} = (a,b)$.

Verificaremos a seguir que o resultado é realmente (a,b). Primeiro notamos que $a_2 > a_3 > \ldots$, e portanto o processo para depois de um certo número m + 2 de passos ($a_{m+2} = 0$). O processo nos dará o seguinte "out-put"

$$
\begin{aligned}
& a_1 = q_1 a_2 + a_3 \quad , \quad 0 < a_3 < a_2 \ , \\
& a_2 = q_2 a_3 + a_4 \quad , \quad 0 < a_4 < a_3 \ , \\
(*) \quad & \vdots \\
& a_{m-1} = q_{m-1} a_m + a_{m+1} , \quad 0 < a_{m+1} < a_m \ , \\
& a_m = q_m a_{m+1} + 0 .
\end{aligned}
$$

De

$$
a_{m-1} = q_{m-1} a_m + a_{m+1} \ , \quad a_{m+1} | a_m \ ,
$$

concluímos que $a_{m+1} | a_{m-1}$. Subindo o sistema (*), chegamos a conclusão que $a_{m+1} | a_1, a_2$. Falta-nos considerar um número natural c tal que $c | a_1, a_2$ e mostrar que $c | a_{m+1}$. Notamos que $c | a_3$ e ao descermos as equações de (*), pararemos necessariamente no fato de que $c | a_{m+1}$.

As equações (*) nos fornecem também com inteiros α, β tais que $a_{m+1} = \alpha a_1 + \beta a_2$. Subindo (novamente!) o sistema (*) obtemos as combinações lineares seguintes,

$$
\begin{aligned}
d = a_{m+1} &= a_{m-1} - q_{m-1} a_m \\
&= a_{m-1} - q_{m-1} (a_{m-2} - q_{m-2} a_{m-1}) \\
&= [(q_{m-1} q_{m-2} + 1)(-q_{m-3}) - q_{m-1}] a_{m-2} \\
&\qquad + (q_{m-1} q_{m-2} + 1) a_{m-3} \\
&= \quad \ddots \\
&= \alpha a + \beta b \ .
\end{aligned}
$$

Observação 15. Lamé deu em 1844 uma estimativa do número n das divisões necessárias para calcular (a,b). Ele mostrou que se $a \leq b$ e k é o número das cifras de a, então $n \leq 5k$. (veja [14]).

Exemplo 16. Sejam a = 255 e b = 221. Então,

$$255 = 1.221 + 34$$
$$221 = 6.34 + 17$$
$$34 = 2.17 + 0 \quad ;$$

daí, d = (a,b) = 17 e

$$\begin{aligned} d = 17 &= 221 - 6.34 \\ &= 221 - 6(255 - 1.221) \\ &= 7(221) - 6(255) \\ &= 7b - 6a. \end{aligned}$$

Teorema 17. Sejam a, b, c ∈ Z. Então,

(i) $c|ab$, $(c,b) = 1 \Longrightarrow c|a$,

(ii) $(a,c) = 1 = (b,c) \Longrightarrow (ab,c) = 1$,

(iii) $a,b|c \Longrightarrow \frac{ab}{(a,b)}\Big|c$,

(iv) $a,b|c$, $(a,b) = 1 \Longrightarrow ab|c$.

Demonstração. (i) Existem inteiros σ, β, tais que $\sigma c + \beta b = 1$. Então, $a(\sigma c + \beta b) = (a\sigma)c + (a\beta)b = a$; desta equação, tendo em vista que $c|c$, ab, obtem-se $c|a$.

(ii) Seja $(ab,c) = d$. De $(b,c) = 1$, obtem-se que $(b,d) = 1$. Como $d|ab$ e $(b,d) = 1$, pela parte (i), $d|a$. Finalmente, dos fatos $d|c$ e $d|a$, $d = 1$.

(iii) Seja $(a,b) = d$. Então existem a_1, $b_1 \in Z$, tais que $a = da_1$, $b = db_1$. Existem também c_1, $c_2 \in Z$, tais que $c = ac_1 = bc_2$. Juntando ambos sistemas obtemos,

$$c = da_1c_1 = db_1c_2 \quad ,$$

daí

$$\frac{c}{d} = a_1c_1 = b_1c_2 \quad .$$

Como $(a_1, b_1) = 1$, então por (i), $b_1|c_1$ e naturalmente $da_1b_1 (= \frac{ab}{(a,b)})$ divide c.

(iv) Esta parte é uma consequência direta de (iii).

c.q.d.

Teorema 18. Sejam $a, b \in Z$, não nulos. Então,

$$[a,b] = \frac{|ab|}{(a,b)} \, .$$

Demonstração. Evidentemente,

$$a \Big| |a| \frac{|b|}{(a,b)} \qquad \text{e} \qquad b \Big| \frac{|a|}{(a,b)} |b| \, .$$

Por outro lado, se c é um inteiro divisível por a e b, então usamos a parte (iii) do teorema anterior para concluir que

$\frac{|ab|}{(a,b)} \mid c$.

1.4. O Teorema Fundamental da Aritmética

1.4.1. Fatorização em Primos

Os números primos são os elementos mínimos da estrutura multiplicativa dos inteiros. Por exemplo,

$$1975 = 5 \times 5 \times 79$$

onde 5 e 79 são "mínimos", pois eles não podem ser fatorizados.

Definição 19. $a \in Z$ é primo se

(i) $a > 1$,

e

(ii) $b, c \in N$, $a = bc \Longrightarrow b$ ou $c = 1$.

Precisaremos do seguinte fato:

para $a, b \in N$ vale

$a \neq b \qquad a|b,\ b > 1 \Longrightarrow a < b$.

Teorema 20. Seja $a \in N$ com $a > 1$. Então existe um primo p divisor de a.

Demonstração. Por indução sobre a. Se a é primo então não temos nada a demonstrar. Podemos supor que $a = bc$,

com b, c inteiros maiores que 1. Como $b < a$, pela hipótese da indução, b possui um primo divisor p que é também um divisor de a.

c.q.d.

Teorema 21. (O Teorema Fundamental da Aritmética)

1. Todo número natural $n > 1$ tem uma fatorização canônica

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} ,$$

onde $k > 0$, os p_i's são primos tais que $p_1 < p_2 < \ldots < p_k$, e $\alpha_i > 0$ para todo i.

2. A fatorização canônica é única.

Demonstração. Por indução sobre n. Se n é primo, ou até uma potência de primo, então temos nada a demonstrar. Podemos supor que n é composto, e que o teorema é válido para todo $m < n$; isto é,

$$n = ab \quad \text{com} \quad a, b > 1$$

e ambos possuindo "boas" fatorizações. Dessas fatorizações obtemos uma fatorização de n que pode ser não canônica. Seja $\mathcal{P}$ a união do conjunto dos primos divisores de a com o conjunto correspondente de b. Seja $\mathcal{P} = \{p_1, p_2, \ldots, p_k\}$ com

$$p_1 < p_2 < \ldots < p_k \quad .$$

Para cada índice i, somamos o expoente de p_i na fatorização de a com o expoente de p_i na fatorização de b; indicamos o resultado por α_i. Então, $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ é a fatorização canônica de n.

Para demonstrar a unicidade da fatorização canônica, basta-nos observar que qualquer fatorização canônica de n produz fatorizações canônicas de a e b, e que são únicas pela hipótese de indução.

c.q.d.

Exemplo 22. Seja n = ab onde a = 175 e b = 275. Fatorizamos a e b e depois n, seguindo fielmente a demonstração do teorema.

$$a = 5 \times 35 = 5 \times 5 \times 7 = 5^2.7,$$

$$b = 5 \times 55 = 5 \times 5 \times 11 = 5^2.11;$$

então $\mathcal{P} = \{p_1, p_2, p_3\}$ onde $p_1 = 5$, $p_2 = 7$ e $p_3 = 11$. O expoente de p_1 na fatorização de a é 2 e na fatorização de b é 2, então $\alpha_1 = 2 + 2 = 4$, etc... $n = 5^4.7^1.11^1$.

Observação 23. A fatorização de um inteiro negativo -n é simplesmente (-1) x fatorização(-n).

2.4.2. O Crivo de Eratosthenes

Nota Histórica 24. Eratosthenes (276-194 AC) nasceu em Cyrene da África do Norte, estudou filosofia em Atenas ,

tornou-se o diretor da famosa biblioteca de Alexandria. Ele era eminente como matemático, geográfo, historiador, filólogo e poeta. (veja [20]).

O Teorema Fundamental da Aritmética nos garante a existência duma fatorização canônica para qualquer $n > 1$, porém o problema concreto de achá-la pode ser bastante trabalhosa. A maneira direta de proceder é de verificar, braçalmente ou pelo uso de um computador, a divisibilidade de n por inteiros m menores que n. Realmente, é suficiente verificar a divisibilidade de n pelos primos menores ou iguais a $\sqrt{n}$.

Teorema 25. Seja n um número natural composto. Então n tem um divisor primo p tal que $p \leq \sqrt{n}$.

Demonstração. Seja p o menor divisor primo de n. Então $n = pa$ para algum $a \in N$. É claro que $p \leq a$ e logo $p^2 \leq pa = n$.

c.q.d.

Exemplo 26. Seja $n = 1969$. Então $\sqrt{n} = 44,..$. Para fatorizar n é preciso experimentar com os primos ≤ 44. Verifica-se que $1969 = 11.179$. Agora para fatorizar 179, observamos que $\sqrt{179} = 13,..$, e testamos a divisibilidade de 179 pelos primos ≤ 13; a conclusão é que 179 é primo. A fatorização $1969 = 11 \times 179$ está completa.

Uma parte substancial do trabalho envolvido na fatorização de n gasta-se na determinação dos primos $\leq \sqrt{n}$. Por esta razão, será muito útil ter a nossa disposição uma lista de primos. Existem várias tabelas para os primos, naturalmente, até certo limite. A mais moderna é uma lista completa dos primeiros seis milhões de primos [2].

O cálculo dessas tabelas baseia-se num algoritmo, ou crivo, desenvolvido por Eratosthenes, e cujo princípio abordaremos a seguir.

Para determinar todos os primos menores que n, primeiro calculamos k, o maior inteiro tal que $k \leq \sqrt{n}$. Segundo, escrevemos todos os inteiros entre 2 e n. Então aplicamos o seguinte esquema:

(o) seja $p_1 = 2$,

(i) elimine da lista todos os múltiplos ℓp_i, para $\ell \geq p_i$,

(ii) (a) se $p_i \geq k$, pare,

(b) se $p_i < k$, seja p_{i+1} o primeiro número maior que p_i na lista modificada; volte para (i) trocando i por $i + 1$.

Exemplo 27. Seja $n = 30$. Então $k = 5$. Eis a lista dos números entre 2 e 30, com as modificações:

2, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, ~~9~~, ~~10~~

11, ~~12~~, 13, ~~14~~, ~~15~~, ~~16~~, 17, ~~18~~, 19, ~~20~~

~~21~~, ~~22~~, 23, ~~24~~, ~~25~~, ~~26~~, ~~27~~, ~~28~~, 29, ~~30~~.

1.5. A Função do Maior Inteiro

Definição 28. Seja a um número real. Denotamos por $[a]$ o maior inteiro que é $\leq a$. Por exemplo, $[-\frac{3}{2}] = -2$, $[1] = 1$, $[\frac{3}{2}] = 1$, $[\sqrt{5}] = 2$.

Coletamos no teorema seguinte algumas propriedades da função $[\ ]: \mathbb{R} \to \mathbb{Z}$.

Teorema 29. Sejam a, b números reais e m um inteiro. Então,

(i) $[a] \leq a < [a] + 1$,

(ii) $a < b \Longrightarrow [a] \leq [b]$ (ou seja, $[\ ]$ é uma função crescente),

(iii) $[a] + [b] \leq [a + b] \leq [a] + [b] + 1$,

e

$[a + m] = [a] + m$,

(iv) para $m > 0$, $\left[\frac{[a]}{m}\right] = \left[\frac{a}{m}\right]$.

Demonstração. As partes (i) e (ii) são óbvias.

(iii) Sejam $a = [a] + \alpha$, $b = [b] + \beta$, e $a + b = [a + b] + \delta$; então, $\alpha, \beta, \delta < 1$. Considerando os fatos,

$$a + b = ([a] + [b]) + (\alpha + \beta),$$

$$= [a + b] + \delta \ ,$$

e que

$$0 < \alpha + \beta < 2 \quad ,$$

o resultado fica provado.

(iv) Seja $a = [a] + \alpha$. Então, $\frac{a}{m} = \frac{[a]}{m} + \frac{\alpha}{m}$, com $0 \leq \frac{\alpha}{m} < \frac{1}{m}$; daí $\left[\frac{a}{m}\right] = \left[\frac{[a]}{m}\right]$.

c.q.d.

Derivamos no teorema seguinte uma fórmula que facilite a fatorização de $n!$

Teorema 30. Sejam n: inteiro positivo, p: primo, k: inteiro tal que $p^k \leq n < p^{k+1}$, e $\alpha(p)$ o expoente de p na fatorização de $n!$. Então,

(i) $\alpha(p) = \sum_{i=1}^{k} \left[\frac{n}{p^i}\right]$ (como $\left[\frac{n}{p^i}\right] = 0$ para $i > k$, $\alpha(p)$ é igual a $\sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$); e

(ii) $\frac{p^k - 1}{p - 1} \leq \alpha(p) \leq \frac{p^{k+1} - 1}{p - 1}$.

Demonstração. Tendo em vista que $n = [\frac{n}{p}]p + r$ com $0 \leq r < p$, os múltiplos de p em $n!$ são

$$1p, 2p, \ldots, ip, \ldots, [\tfrac{n}{p}]p \quad .$$

Então,

$$n! = (1p)(2p) \ldots (ip) \ldots ([\tfrac{n}{p}]p).n_1$$

$$= \left[\frac{n}{p}\right]! \; p^{\left[\frac{n}{p}\right]} \cdot n_1 \quad \text{onde}$$

$(p,n_1) = 1$. O número $\left[\frac{n}{p}\right]!$ pode conter potências não triviais de p. Pela parte (iii) do teorema anterior,

$$\left[\frac{\left[\frac{n}{p}\right]}{p}\right] = \left[\frac{n}{p^2}\right] ,$$

e assim, repetindo o mesmo argumento de antes,

$$\left[\frac{n}{p}\right]! = \left[\frac{n}{p^2}\right]! \; p^{\left[\frac{n}{p^2}\right]} \cdot n_2$$

com $(p,n_2) = 1$. Juntando as duas partes,

$$n! = \left[\frac{n}{p^2}\right]! \; p^{\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]} \; n_1 \; .$$

Então procedendo por indução sobre n, obtemos

$$n! = p^{\alpha(p)} \; n_1 \quad ,$$

onde $$\alpha(p) = \sum_{i=1}^{k} \left[\frac{n}{p^i}\right] \; .$$

(ii) Como a função $[\;]$ é monótona e $p^k \leq n < p^{k+1}$, então, $p^{k-i} = \left[\frac{p^k}{p^i}\right] \leq \left[\frac{n}{p^i}\right] \leq \left[\frac{p^{k+1}}{p^i}\right] = p^{k+1-i}$; este fato com a fórmula para a soma de uma progressão geométrica nos dará o resultado.

c.q.d.

Exemplo 31. (i) Ilustramos o processo de coleta das potências de p. Sejam n = 10, p = 2. Então,

$$\begin{aligned} 10! &= 1.2.3.4.5.6.7.8.9.10 \\ &= (2.4.6.8.10).3.5.7.9 \\ &= 2^5(1.2.3.4.5).3.5.7.9 \\ &= 2^5\ (2.4)3.5.7.9 \\ &= 2^5\ 2^2(1.2)3.5.7.9 \\ &= 2^8.3.5.3.5.7.9 \qquad ; \end{aligned}$$

da fórmula $\alpha(2) = \left[\frac{10}{2}\right] + \left[\frac{10}{4}\right] + \left[\frac{10}{8}\right] = 5 + 2 + 1 = 8.$

(ii) A fatorização de 10! é

$$10! = 2^8.3^4.5^2.7 \ .$$

(iii) Se n = 100! fosse representado na forma decimal, em quantos zeros ele terminaria?

Evidentemente, a quantidade é igual ao maior expoente β tal que $10^\beta | n!$. Seja $2^{\alpha(2)}3^{\alpha(3)}5^{\alpha(5)}\ldots$ a fatorização canônica de n! . Então, $\beta = \min(\alpha(2), \alpha(5))$. Aliás, $\beta = \alpha(5)$; pois $\left[\frac{n}{2^i}\right] \geq \left[\frac{n}{5^i}\right]$ e $\left[\frac{n}{2^i}\right] > \left[\frac{n}{5^i}\right]$ se $\left[\frac{n}{2^i}\right] \neq 0$. Portanto, $\beta = \alpha(5) = \left[\frac{100}{5}\right] + \left[\frac{100}{25}\right] = 20 + 4 = 24.$

Corolário 32. Seja $n_o = n_1 + n_2 + \ldots + n_k$, onde $n_i \in N$ para $0 \leq i \leq k$. Então,

$$(n_1!)(n_2!)\ \ldots\ (n_k!) | (n_o!) \ .$$

Demonstração. Sejam p um primo e $\alpha_i(p)$ o expoente de p na fatorização canônica de n_i para $0 \leq i \leq k$. Então $\beta(p) = \alpha_1(p) + \ldots + \alpha_k(p)$ é o expoente de p na fatorização canônica de $(n_1!)(n_2!) \ldots (n_k!)$. Para demonstrar a divisibilidade, será suficiente mostrar que qualquer que seja o primo p, $\beta(p) \leq \alpha_o(p)$.

Pela propriedade (iii) da função $[\ ]$,

$$\left[\frac{n_o}{p^i}\right] = \left[\frac{n_1 + n_2 + \ldots + n_k}{p^i}\right] \geq \left[\frac{n_1}{p^i}\right] + \left[\frac{n_2}{p^i}\right] + \ldots + \left[\frac{n_k}{p^i}\right] ;$$

da qual obtemos,

$$\sum_{i=1}^{\infty} \left[\frac{n_o}{p^i}\right] \geq \sum_{i=1}^{\infty} \left[\frac{n_1}{p^i}\right] + \ldots + \left[\frac{n_k}{p^i}\right]$$

Pelo teorema anterior,

$$\alpha_o(p) \geq \alpha_1(p) + \ldots + \alpha_k(p) \ .$$

c.q.d.

1.6. Exercícios

1. Use a boa ordenação dos números naturais para mostrar que

$$a: \text{natural},\ 0 < a \leq 1 \Longrightarrow a = 1 .$$

(Por contradição; considere d o menor elemento de $A = \{c \mid c \in N \text{ e } 0 < c < 1\}$; prove que $0 < d^2 < d$).

2. Sejam a e b inteiros com $a \neq 0$.

(i) Mostre que existe um inteiro d tal que $da-b > 0$.

(ii) Mostre que existe um inteiro d tal que $b-da > 0$.

3. Demonstre por indução as seguintes fórmulas:

(i) $1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$

(ii) $1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$

(iii) $1^3 + 2^3 + 3^3 + \ldots + n^3 = \left[\frac{n(n+1)}{2}\right]^2$

4. Sejam n, k inteiros não negativos com $k \leq n$. O símbolo $\binom{n}{k}$ define-se por $\frac{n!}{k!(n-k)!}$. Mostre que

(i) $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$ para $k \geq 1$;

(ii) $\binom{n}{k}$ é inteiro positivo.

5. Mostre a fórmula de Newton

$$(a + b)^n = a^n + \binom{n}{1}a^{n-1}b + \ldots + \binom{n}{i}a^{n-i}b^i + \ldots + b^n,$$

onde a e b são dois inteiros quaisquer.

6. Demonstrar as partes (3) e (4) do Teorema 2, I.

7. Representar, somar e multiplicar os números decimais 15, 72 nos sistemas: Romano, de base 2, de base 20 e de base 60.

8. Sejam a, b números inteiros, $b = r_k a^k + r_{k-1}a^{k-1} + \ldots + r_1 a + r_o$ o desenvolvimento de b na base a e $r_k \neq 0$. Demonstre que $a^k \leq b < a^{k+1}$.

9. Dado o número decimal $a = r_k r_{k-1} \ldots r_o$, mostre que a é divisível por 7, 11 ou 13 $\Longleftrightarrow$ $r_2 r_1 r_o - r_5 r_4 r_3 + r_8 r_7 r_6 \ldots$ é divisível respectivamente por 7, 11 ou 13 (observe que $1001 = 7.11.13$).

10. Considerando o fato que $999 = 27.37$, formule um teste para decidir quando 37 divide um número representado em forma decimal.

11. Calcular (a,b) e [a,b] para a= 7469 e b = 2464.

12. Sejam a, b inteiros não nulos e seja m um número natural. Mostrar que (ma, mb) = m(a,b).

13. O máximo divisor comum dos inteiros $a_1, a_2, \ldots, a_n$ não todos nulos, denotado por $(a_1, a_2, \ldots, a_n)$, é um número natural d tal que $d|a_1, a_2, \ldots, a_n$, e se c inteiro, e $c|a_1, a_2, \ldots, a_n$, então $c|d$. Mostre que

$(a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n)$.

14. Sejam $a_1, a_2, \ldots, a_n$ inteiros não nulos. Defina o mínimo múltiplo comum desses inteiros. Mostre que $[a_1, a_2, \ldots, a_n] = [[a_1, a_2, \ldots, a_{n-1}], a_n]$.

15. Calcular (a_1, a_2, a_3) e $[a_1, a_2, a_3]$ para $a_1 = 91$, $a_2 = 1001$, $a_3 = 1008$.

16. Demonstre que $(a,b) = (a,b,ax + by)$ ∀ inteiros x, y.

17. Demonstrar o Teorema 12, I.

18. Aplicar o algoritmo Euclideano ao par $a = 7469$, $b = 2464$, pondo em evidência todos os passos. Encontre α, β inteiros tais que

$$\alpha a + \beta b = (a,b) \quad .$$

19. Mostrar que para quaisquer inteiro k, $a = 4k + 3$ e $b = 5k + 4$ são primos entre si (isto é, $(a,b) = 1$).

20. Determine todos os primos menores que 200 (tem 46 deles).

21. Mostrar que 3856, 38567, 38569 são números primos (use o resultado do exercício anterior).

22. Mostrar que três inteiros ímpares consecutivos não podem ser todos primos, com exceção de (3,5,7).

23. Seja a um número real. Mostre que $[a + \frac{1}{2}]$ é o inteiro mais próximo ao número a.

24. Determine a maior potência de 14 que divide 100!.

25. Mostrar que

(i) α é racional $\Longleftrightarrow$ existe um número natural m tal que $[m\alpha] = m\alpha$,

(ii) a constante de Euler $e = \sum_{j=0}^{\infty} \frac{1}{j!}$ é irracional

(observe que $[(k!)e] = k! \sum_{j=0}^{k} \frac{1}{j!} < (k!)e$).

CAPÍTULO II

PROBLEMAS SOBRE PRIMOS

FATORIZAÇÃO EM DOMÍNIOS

2.1. A Sequência dos Primos - Alguns Problemas Famosos

Seja $\mathcal{P} = \{p_1, p_2, \ldots, p_n, \ldots\}$ a sequência dos primos, onde p_n é o n-ésimo primo a aparecer na sequência dos números naturais. Consideraremos nesta secção várias propriedades importantes de $\mathcal{P}$.

2.1.1. O Número dos Primos

Teorema 1. O número dos inteiros primos é infinito.

Apresentaremos duas demonstrações. A primeira que é mais simples foi dada por Euclides (Proposição 20, Livro IX dos Elementos). A segunda, de Leonard Euler (1707-1783, um dos heróis de todos os matemáticos; veja [17], p. 148), data-se dos meados do século 18 e representa o primeiro passo na Teoria Analítica dos Números.

Demonstração 1. Sejam $p_1, p_2, \ldots, p_k$ os primeiros k primos. Consideremos a fatorização de $n = (p_1 p_2 \ldots p_k) + 1$. Pelo Teorema 20, Cap. I, existe um primo q divisor de n; q não pode dividir 1 e portanto é diferente

de qualquer dos p_i's. Então qualquer que seja k, o conjunto $\{p_1, p_2, \ldots, p_k\}$ não pode conter todos os primos.

c.q.d.

Demonstração 2. Recordamos certos fatos elementares sobre séries:

(i) $r \in R$, $|r| < 1 \Longrightarrow \frac{1}{1-r} = \sum_{i=0}^{\infty} r^i$,

(ii) a série harmônica $\sum_{n=1}^{\infty} \frac{1}{n}$ é divergente,

(iii) sejam $\sum_{i=0}^{\infty} a_i$, $\sum_{i=0}^{\infty} b_i$ duas séries convergentes com valores a e b respectivamente, e $c_k = \sum_{j=0}^{k} a_{k-j}b_j$ para $k \geq 0$. Então, $\sum_{k=0}^{\infty} c_k$ (indicada também por $\sum_{i,j=0}^{\infty} a_i b_j$) converge para o valor ab.

Sejam p e q dois números primos. Então, como $\frac{1}{p}$, $\frac{1}{q} < 1$, pelos fatos (i), e (iii),

$$(1 - \tfrac{1}{p})^{-1}(1 - \tfrac{1}{q})^{-1} = \left(\sum_{i=0}^{\infty} \frac{1}{p^i}\right)\left(\sum_{i=0}^{\infty} \frac{1}{q^i}\right) = \sum_{i,j=0}^{\infty} \frac{1}{p^i q^j} .$$

Observamos que qualquer inteiro $n > 0$ cujos fatores primos são p ou q, encontra-se nesta série e uma vez só. Ou seja,

$$(1 - \tfrac{1}{p})^{-1}(1 - \tfrac{1}{q})^{-1} = \{\textstyle\sum \frac{1}{n} \big| n = p^i q^j \text{ para alguns } i,j>0\}.$$

Generalizando, temos para os primos $p_1, p_2, \ldots, p_k$,

$$\prod_{i=1}^{k} (1 - \frac{1}{p_i})^{-1} = \sum\{\frac{1}{n} | n = \prod_{i=1}^{k} p_i^{\alpha_i} \quad \text{com} \quad \alpha_i \geq 0\} .$$

Se $\mathcal{P}$ fosse finito, digamos de ordem k, então teríamos pelo Teorema Fundamental da Aritmética,

$$\prod_{i=1}^{k} (1 - \frac{1}{p_i})^{-1} = \sum_{n=1}^{\infty} \frac{1}{n} \quad ;$$

um absurdo, tendo em vista que o lado direito é a série harmônica e o lado esquerdo é um número racional.

c.q.d.

As questões que se põem sobre o conjunto infinito $\mathcal{P}$ tratam-se, entre várias, de seu crescimento, densidade, distribuição dentro de N e também de suas subsequências especiais.

2.1.2. Saltos entre os Primos

Teorema 2. (i) Dado $n > 1$, existem n números compostos consecutivos,

(ii) $\overline{\lim}\{p_{k+1} - p_k | k \in N\}$ é infinito.

Demonstração. (i) A sequência

$(n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + (n+1)$

está formada de números compostos; pois $(n+1)!$ é divisível por $i + 1$ para $1 \leq i \leq n$.

(ii) Tendo em vista que $p_{k+1} - p_k$ é finito para todo k, precisamos mostrar que dado $n > 1$, existe $k \in N$ tal que $p_{k+1} - p_k > n$. Escolhemos p o maior primo tal que $p < (n+1)! + 2$. Seja k a posição de p na sequência dos primos. Então, pela parte (i),

$$p_k < (n+1)! + 2 < \ldots < (n+1)! + (n+1) < p_{k+1} \quad ;$$

a demonstração está terminada.

c.q.d.

2.1.3. A série $\sum_{i=1}^{\infty} \frac{1}{p_i}$ é divergente (veja Corolário 5, Capítulo II).

2.1.4. Primos Gêmeos

Qual é o valor de

$$\underline{\lim}\{p_{k+1} - p_k | k \in N\} \quad ?$$

O menor elemento do conjunto das diferenças $\{p_{k+1}-p_k | k \in N\}$ é 1; pois $p_2 - p_1 = 3 - 2 = 1$. Além do mais,

$$\inf\{p_{k+1} - p_k | k > 1\}, \ \ldots, \ \inf\{p_{k+1} - p_k | k > 9\}$$

são todos iguais a 2. A razão atrás deste fato é que em ca

da um dos conjuntos considerados existem primos gêmeos: p_ℓ, $p_{\ell+1}$ tais que $p_{\ell+1} - p_\ell = 2$. Exemplos de primos gêmeos são

$$(3,5),\ (5,7),\ (11,13),\ (17,19),\ (29,31).$$

Para termos uma idéia da frequência desses pares mencionamos que existem 1.224 primos gêmeos entre os 9.592 primos menores que 10^5 e existem 8.169 primos gêmeos entre os 78.498 primos menores que 10^6. Essas cogitações nos levam à conjectura seguinte,

$$\lim\{p_{k+1} - p_k \mid k \in \mathbb{N}\} = 2\ ;$$

ou numa forma mais simples,

existe um número infinito de primos gêmeos.

A sequência $\mathcal{G}$ dos primos gêmeos é menos densa que a dos primos; pois

$$\sum\{\tfrac{1}{p} \mid p \in \mathcal{G}\} \quad \text{é convergente!!}$$

(veja [7], Theorem 5.1.1., página 107), contrastando dramaticamente com o fato já mencionado de que

$$\sum\{\tfrac{1}{p} \mid p \in \mathcal{P}\} \quad \text{é divergente}\ .$$

2.1.5. A Distribuição dos Primos

Sejam $x \in \mathbb{R}$, $x > 0$ e $\pi(x)$ o número dos primos $\leq x$.

A. M. Legendre declarou em 1808 [13] que $\pi(x)$ parecia ter a forma $\frac{x}{(\log x) + A(x)}$ onde $A(x)$ é aproximadamente 1,08366.

Apesar de que Legendre foi o primeiro a publicar formas possíveis para $\pi(x)$, C. F. Gauss (1777-1855, "o príncipe dos matemáticos", veja [17, pp. 295-339]), já tinha trabalhado meticulosamente sobre o assunto em 1792-1793, mas nunca chegou a publicá-lo. Ele tabulou detalhadamente a distribuição dos primos em intervalos de 1000, de 1 até 3.000.000 ; por exemplo, existem 168 primos entre 1 e 1000, 135 entre 1000 e 2000, 127 entre 2000 e 3000, etc.; nesta tarefa e numa época "pré-computacional" ele cometeu pouquissimos erros.

Usando essa estatística Gauss chegou a conclusão de que a densidade dos primos numa vizinhança de n foi da ordem de $\frac{1}{\log n}$, e daí

$$\pi(x) \sim \int_2^x \frac{1}{\log t}\, dt \quad ;$$

($f(x) \sim g(x)$ significa que $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$); por exemplo, entre $a = 2.600.000$ e $b = 2.700.000$, ele encontrou 6.762 primos, e calculou $\int_a^b \frac{dt}{\log t} = 6.761,332$.

Depois das contribuições significativas de Legendre, Gauss, Dirichlet, Chebychev e Riemann, o Teorema do Número Primo

$$\pi(x) \sim \frac{x}{\log x} \sim \int_2^x \frac{1}{\log t}\, dt \quad ,$$

foi simultaneamente demonstrado por Ch. de la Vallée Poussin e Jaques Hadamard no ano 1896. Para uma pesquisa histórica mais detalhada recomendamos a leitura de [9].

A demonstração do teorema geral está fora das possibilidades deste livro. O leitor interessado, conhecendo as "coisas" básicas da análise, pode consultar [1] ou [8]. Porém, cabe a nós apresentar aqui um teorema de Chebychev, que é uma forma fraca, mas interessante, do Teorema do Número Primo.

A função $f(x)=\frac{x}{\log x}$ é estritamente crescente, e $f(x) < x$, quando $x > e$. Por outro lado $f(x)$ cresce mais rapidamente que x^{ε} para qualquer $0 < \varepsilon < 1$; em termos mais exatos,

$$\frac{x}{\log x} \cdot \frac{1}{x^{\varepsilon}} \to \infty$$

quando $x \to \infty$. Esta afirmação pode ser verificada usando a lei de L'Hospital .

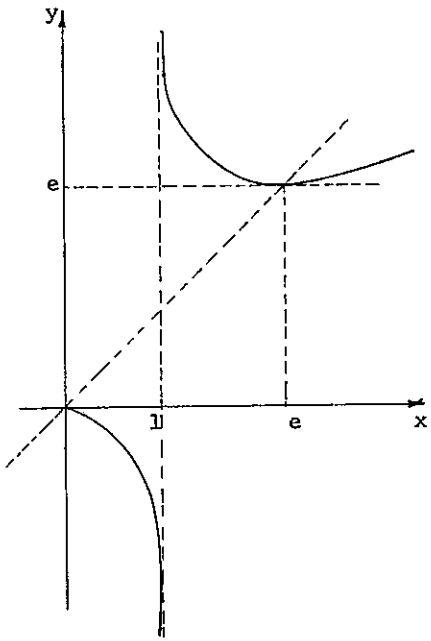


Gráfico de $f(x) = \frac{x}{\log x}$

Teorema 3 (Chebychev). Existem constantes positivas a, b tais que

$$a \frac{x}{\log x} \leq \pi(x) \leq b \frac{x}{\log x}$$

para todo $x \geq 2$.

Demonstração. Investigaremos umas propriedades de fatorização e limites de $\binom{2n}{n}$, para $n > 1$.

(i) $\binom{2n}{n}$ aparece na expansão binomial de $(1+1)^{2n}$, e portanto,

$$\binom{2n}{n} \leq 2^{2n} . \tag{1}$$

(ii) $\binom{2n}{n} = \frac{(2n)!}{n!\,n!} = \prod_{i=1}^{n} \frac{n+i}{i}$. Como $\frac{n+i}{i} \geq 2$ para $1 \leq i \leq n$, obtem-se

$$2^n \leq \binom{2n}{n} . \tag{2}$$

(iii) Seja p um primo menor que $2n$ e seja $\nu(p)$ o número natural tal que $p^{\nu(p)} \leq 2n < p^{\nu(p)+1}$. Seja também $\alpha(p)$ o expoente do primo p na fatorização de $\binom{2n}{n}$; então $\binom{2n}{n} = \prod_{p<2n} p^{\alpha(p)}$. Pelo Teorema 30, Cap. I, conclui-se que

$$\alpha(p) = \sum_{i=1}^{\nu(p)} \left[\frac{2n}{p^i}\right] - 2\left[\frac{n}{p^i}\right] .$$

Seja $n = tp^i + \varepsilon$, onde t, ε são inteiros não negativos com $0 \leq \varepsilon < p^i$. Então, $2n = (2t)p^i + 2\varepsilon$ com $0 \leq 2\varepsilon < 2p^i$. Portanto,

$$\left[\frac{2n}{p^i}\right] - 2\left[\frac{n}{p^i}\right] = 0 \quad \text{ou} \quad 1 \ .$$

Por conseguinte,

$$\alpha(p) \leq \nu(p)$$

para todo primo p com $p \leq n$, e

$$\alpha(p) = 1$$

para todo primo p com $n < p \leq 2n$. Assim obtemos,

$$\binom{2n}{n} = \prod_{p<2n} p^{\alpha(p)} \leq \prod_{p<2n} p^{\nu(p)} \ ,$$

$$\leq \prod_{p<2n} (2n) \ ,$$

$$\binom{2n}{n} \leq (2n)^{\pi(2n)} \ , \tag{3}$$

e

$$\prod_{n<p\leq 2n} p = \prod_{n<p\leq 2n} p^{\alpha(p)} \leq \binom{2n}{n}$$

$$n^{\pi(2n)-\pi(n)} < \binom{2n}{n} \ . \tag{4}$$

(iv) As desigualdades (2) e (3) produzem,

$$2^n \leq (2n)^{\pi(2n)} \ ;$$

portanto,

$$n\log 2 \leq \pi(2n)\log 2n \ ;$$

ou seja,

$$\frac{\log 2}{2} \cdot \frac{2n}{\log 2n} \leq \pi(2n) \ . \qquad (5)$$

Dado $x \geq 2$, existe n um número natural tal que

$$2n \leq x < 2(n+1).$$

Injetando x na desigualdade (5), obtemos as seguintes desigualdades

$$\frac{\log 2}{2} \frac{2n}{\log x} \leq \pi(2n) \leq \pi(x) \ ,$$

$$\frac{\log 2}{2} \frac{x/2}{\log x} \leq \pi(x) \ ,$$

$$\frac{\log 2}{4} \frac{x}{\log x} \leq \pi(x) \ , \qquad (6)$$

assim um lado da desigualdade de Chebychev foi facilmente provado.

(v) Para produzir o outro lado combinamos as desigualdades (1) e (4),

$$n^{\pi(2n)-\pi(n)} < 2^{2n} \ ;$$

daí temos,

$$(\pi(2n) - \pi(n))\log n < (2n)\log 2 \ . \qquad (7)$$

Tendo em vista que para $n \geq 2$, $n^2 \geq 2n$ vale, obtemos

$$\log n \geq \frac{\log 2n}{2} \ ;$$

portanto,

$$\pi(2n) - \pi(n) < \frac{2n}{\log n} \log 2 \leq \frac{2n}{\log 2n} 2\log 2 \qquad (8)$$

Sejam $x > 2$ e n um número natural tal que $2(n-1) \leq x < 2n$. Então,

$$\pi(x) = \pi(2n) - 1 \text{ ou } \pi(2n),$$

e

$$\pi(\tfrac{x}{2}) = \pi(n) \quad \text{ou} \quad \pi(n) - 1.$$

Portanto,

$$\pi(x) - (\pi(\tfrac{x}{2})+1) \leq \pi(2n) - \pi(n) < \frac{2n}{\log n} \log 2 \ ;$$

ou seja,

$$\pi(x) - \pi(\tfrac{x}{2}) \leq \frac{2n}{\log n}(\log 2) + 1 \ . \qquad (9)$$

Tendo em vista que $\frac{x}{\log x}$ é uma função crescente para $x>e$,

$$1 \leq \frac{1}{4} \frac{2n}{\log n} \log 2$$

e daí,

$$\pi(x) - \pi(\tfrac{x}{2}) \leq \frac{3}{2} \frac{2n}{\log n} \log 2 \ .$$

Também,

$$\pi(x) - \pi(\tfrac{x}{2}) \leq \frac{3}{2} \frac{\frac{x}{2} + 1}{\log n} \log 2 \ ,$$

$$\leq \frac{3}{2} \frac{x+2}{2\log \frac{x}{2}} \log 2 \ .$$

Tendo em vista que $2\log \frac{x}{2} > \log x$ para $x \geq 4$ e que $\frac{x+2}{2} \leq x$ obtemos,

$$\pi(x) - \pi(\tfrac{x}{2}) \leq \frac{3}{2} \frac{x+2}{\log x} \log 2 < 3 \frac{x}{\log x} \log 2 \qquad (10)$$

para $x \geq 4$.

Uma cota superior para $\pi(x)$ pode ser obtida pela soma telescópica

$$\pi(x) = (\pi(x) - \pi(\tfrac{x}{2})) + (\pi(\tfrac{x}{2}) - \pi(\tfrac{x}{4})) + \ldots$$

$$\leq 3\log 2\left(\frac{x}{\log x} + \frac{x/2}{\log x/2} + \ldots\right) ;$$

porém, a expressão do lado direito na forma desejada apresenta dificuldades. Superemos esta dificuldade mediante outra desigualdade que vamos desenvolver a seguir.

$$\pi(x)\log x - \pi(\tfrac{x}{2})\log \tfrac{x}{2}$$

$$= (\pi(x) - \pi(\tfrac{x}{2}))\log x + \pi(\tfrac{x}{2})(\log x - \log \tfrac{x}{2})$$

$$\leq 3(\log 2) \frac{x}{\log x} \log x + \pi(\tfrac{x}{2}) \log 2 ,$$

por (10). Como $\pi(\frac{x}{2}) \leq \frac{x}{2}$,

$$\pi(x)\log x - \pi(\tfrac{x}{2})\log \tfrac{x}{2} \leq \frac{7}{2} x\log 2 . \qquad (11)$$

Finalmente,

$$\pi(x)\log x = (\pi(x)\log x - \pi(\tfrac{x}{2})\log \tfrac{x}{2}) + (\pi(\tfrac{x}{2})\log\tfrac{x}{2} -$$

$$- \pi(\tfrac{x}{4})\log\tfrac{x}{4}) + \ldots \leq \frac{7}{2} \log 2(x + \frac{x}{2} + \frac{x}{4} + \ldots) \leq$$

$$\leq \frac{7}{2}(\log 2)(2x) \leq 7(\log 2)x \quad ;$$

isto é,

$$\pi(x) \leq 7(\log 2)\frac{x}{\log x}$$

que é válida para $x \geq 2$.

c.q.d.

Corolário 4. Existem constantes positivas c,d tais que

$$ck\log k < p_k < dk\log k$$

para $p_k \in \mathcal{P}$ e $k \geq 2$.

Demonstração. Pelo teorema anterior,

$$a\,\frac{p_k}{\log p_k} < \pi(p_k) < b\,\frac{p_k}{\log p_k}\,.$$

Notamos que $\pi(p_k) = k$ e $k < p_k$.

(i) $k < b\,\dfrac{p_k}{\log p_k} \Longrightarrow \dfrac{1}{b}k\,\log k < \dfrac{1}{b}k\,\log p_k < p_k$.

(ii) Para obter o outro lado da desigualdade seria o caso de tentar trocar $\log p_k$ por $\log k$ em

$$p_k < \frac{1}{a}k\,\log p_k\,.$$

Existe um número m tal que

$$\frac{p_k^{1/2}}{\log p_k} > a$$

para todo $k > m$.

Então valem as seguintes desigualdades,

$$p_k < \frac{1}{a} k \log p_k < \frac{1}{a} k . a p_k^{1/2} \quad ,$$

$$p_k^{1/2} < k \quad ,$$

e

$$\log p_k < 2 \log k \quad ,$$

para $k > m$. Utilizando a última desigualdade obtemos

$$p_k < \frac{1}{a} k \log p_k < \frac{2}{a} k \log k \quad ,$$

para $k > m$. Naturalmente, uma constante d pode ser achada tal que

$$p_k < dk \log k \quad ,$$

para $k \geqslant 2$.

c.q.d.

Corolário 5. $\sum_1^{\infty} \frac{1}{p_k}$ é divergente.

Demonstração. Tendo em vista que

$$\frac{1}{dk \log k} < \frac{1}{p_k} \quad \text{para} \quad k \geqslant 2$$

e que

$$f(x) = \frac{1}{x\log x}$$

é uma função positiva e decrescente para $x > 1$, valem as desigualdades,

$$\frac{1}{d}\int_2^{\infty} \frac{1}{x\log x}\,dx < \frac{1}{d}\sum_{k=2}^{\infty} \frac{1}{k\log k} < \sum_{k=1}^{\infty} \frac{1}{p_k} \quad .$$

É fácil achar o valor da integral, pois

$$\int_2^{\infty} \frac{1}{x\log x}\,dx = \log(\log x)\Big|_2^{\infty} = \infty \ ,$$

daí segue o resultado procurado.

c.q.d.

2.1.6. Progressões Aritméticas

Legendre publicou em 1808, no mesmo trabalho citado acima, uma outra conjectura:

se $a > 0$ e $(a,b) = 1$, então a progressão $\{an+b \mid n \in Z\}$ contém um número infinito de primos.

Dirichlet demonstrou esta conjectura em 1837 com métodos analíticos revolucionários baseados na demonstração de

Euler da infinitude dos primos (veja [1]).

Demonstraremos no Capítulo IV, e por métodos simples, a existência de uma infinitude de primos da forma an+ + 1 para qualquer a ε N. Outros casos particulares do Teorema de Dirichlet podem ser provados por pequenas variações sobre a demonstração de Euclides.

Teorema 6. Existe um número infinito de primos da forma 4n - 1.

Demonstração. Usamos a mesma técnica de Euclides . Sejam 3, 7, ..., p_k os primeiros k primos da forma 4n-1. Consideremos,

$$a = 4(3.7...p_k) - 1 ,$$

que tem a forma 4n - 1. Como todo primo ímpar é da forma 4n ± 1 e como (4n + 1)(4m + 1) = 4(4nm + m + n) + 1 = 4ℓ + + 1, um dos primos divisores q de a deve ter a forma 4n - 1. Naturalmente, q ≠ 3, 7, ..., p_k .

c.q.d.

2.1.7. A Conjectura de Goldbach

Goldbach escreveu em 1742 numa carta dirigida a Euler a seguinte conjectura que continua sem demonstração.

se n é par e n > 4, então n é a soma de dois primos ímpares.

Por exemplo, $6 = 3 + 3$, $8 = 3 + 5$, $10 = 5 + 5$, $12 = 5 + 7$.

Se a conjectura de Goldbach for verdadeira então valerá,

todo número n que é ímpar tal que $n > 9$, é a soma de três primos ímpares;

pois, $n - 3$ será par e pela conjectura de Goldbach, $n - 3 = p_1 + p_2$ para certos primos ímpares p_1, p_2.

Em 1937, Vinogradov demonstrou por métodos de aproximações bastante delicados, que existe um número natural n a partir do qual a última afirmativa é válida.

Existem outros problemas sobre os primos (veja Capítulo II de [11]). Um deles é encontrar uma fórmula geradora dos primos. Matiyasevič construiu em 1970 um polinômio de várias variáveis com coeficientes inteiros cujo conjunto imagem (quando as variáveis tomam valores inteiros) consiste de todos os primos e inteiros negativos (veja o Capítulo VI).

2.2. Fatorização em $Z[\sqrt{n}]$ e $K[x]$

Para termos uma melhor apreciação do Teorema Fundamental da Aritmética seria bom pesquisarmos a questão da fatorização em outros domínios de integridade.

Pois bem, qual é a situação no domínio dos números ra

cionais Q? Consideremos por exemplo a fatorização de 6 em Q:

$$6 = 5.\frac{6}{5} = 2.3 = \frac{2}{7} \cdot \frac{21}{11} \cdot 11 = \ldots$$

Mas qual dos 2, 3, 5, 11, $\frac{6}{5}$, $\frac{2}{7}$, $\frac{21}{11}$ é primo em Q? É evidente que dado $a \in Q$, $a \neq 0$, ele tem uma fatorização: $a=a^2.\frac{1}{a}$. Não vamos olhar para este tipo de fatorização como sendo uma "boa" fatorização.

Definição 7. Seja D um domínio de integridade. $a \in D$ chama-se primo ou irredutível se

(1) a não é inversível (isto é, não existe a' tal que $a.a' = 1$), e

(2) se $b, c \in D$ satisfazem

$$a = bc ,$$

então um deles é inversível.

Assim pela definição dada Q não possui nenhum primo; uma situação radical. Porém, Q neste sentido é igual a qualquer outro corpo.

2.2.1. O Domínio $Z[\sqrt{n}]$

Encontram-se muitos domínios não corpos dentro do conjunto dos números complexos $\mathbb{C}$. Esboçamos a seguir um de

les. Sejam n um inteiro não quadrado e

$$D = \{a + b\sqrt{n} \mid a, b \in Z\} \quad .$$

D contém todos os inteiros; basta colocar $b = 0$ e variar a. D denota-se por $Z[\sqrt{n}]$.

Antes de começar a operar com os elementos de D seria necessário saber se

$$a + b\sqrt{n} = a' + b'\sqrt{n} \Longrightarrow a = a' \ , \ b = b'.$$

A resposta é sim e fica a cargo do leitor; não é trivial! (Exercício 11).

D é um domínio.

O conjunto D é fechado pelas operações de C:

$$(a + b\sqrt{n}) + (c + d\sqrt{n}) = (a+c) + (b+d)\sqrt{n} \ ,$$

$$(a + b\sqrt{n})(c + d\sqrt{n}) = (ac+bdn) + (ad+bc)\sqrt{n}.$$

Não é nada difícil verificar que D é um anel comutativo com identidade. Para provar que D é domínio falta-nos verificar,

$$\alpha, \beta \in D \text{ com } \alpha\beta = 0 \Longrightarrow \alpha \text{ ou } \beta = 0.$$

Sejam $\alpha = a_1 + b_1\sqrt{n}$ e $\beta = a_2 + b_2\sqrt{n}$, dois elementos de D tais que $\alpha\beta = 0$. Então valem as seguintes igualdades,

$$\alpha\beta = (a_1a_2+b_1b_2n) + (a_1b_2+a_2b_1)\sqrt{n} = 0 + 0\sqrt{n} ,$$

$$a_1a_2 + b_1b_2n = 0,$$

$$a_1b_2 + a_2b_1 = 0 .$$

Suponhamos que $\alpha \neq 0$; então a_1 ou $b_1 \neq 0$. Se $b_1 = 0$ então é fácil concluir que $a_2 = b_2 = 0$ e $\beta = 0$. Ficamos com o caso $b_1 \neq 0$. Ao multiplicar a primeira equação por b_2 e a segunda por a_2 e depois de considerar a diferença entre os dois resultados, concluímos que

$$b_1b_2^2n - a_2^2b_1 = (b_2^2n - a_2^2)b_1 = 0;$$

então pelo fato de que $b_1 \neq 0$, tem-se

$$a_2^2 - b_2^2n = 0 ,$$

cuja única solução é $a_2 = b_2 = 0$.

D possui uma norma

Seja $\sigma: D \to D$ a função conjugação definida por

$$\sigma(a + b\sqrt{n}) = a - b\sqrt{n} .$$

σ é uma função bijetora e preserva as operações, isto é, para todos $\alpha, \beta \in D$, $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$, $\sigma(\alpha\beta)=\sigma(\alpha)\sigma(\beta)$ (verifique!).

Finalmente (paciência!) definimos a norma

$$\nu: D \to \mathbb{Z}_{\geq 0}$$

por

$$\nu(\alpha) = |\alpha\sigma(\alpha)| \quad .$$

Por exemplo, se $\alpha = a + b\sqrt{n}$ para $a, b \in \mathbb{Z}$,

$$\nu(\alpha) = |a^2 - b^2 n| \quad .$$

ν satisfaz as seguintes propriedades (é por isto que ν se conhece por norma),

$$\nu(\alpha) \geq 0$$

$$\nu(\alpha) = 0 \Longleftrightarrow \alpha = 0$$

$$\nu(\alpha\beta) = \nu(\alpha)\nu(\beta) \qquad \text{(verifique!)}.$$

A norma ν é útil em identificar os elementos inversíveis de D. Mais exatamente,

Teorema 8. Seja $\alpha \in D$. Então

$$\nu(\alpha) = 1 \Longleftrightarrow \alpha \text{ é inversível.}$$

Demonstração. Suponhamos que $\nu(\alpha) = 1$. Então pela definição de ν,

$$\nu(\alpha) = |\alpha\sigma(\alpha)| = 1 \ ,$$

da qual obtemos $\sigma(\alpha)$ ou $-\sigma(\alpha)$ é o inverso de α.

Reciprocamente, suponhamos que α tenha um inverso

β. Então $\alpha\beta = 1$ e

$$\nu(\alpha\beta) = \nu(\alpha).\nu(\beta) = \nu(1) = 1 .$$

Portanto, $$\nu(\alpha) = \nu(\beta) = 1.$$

Teorema de Fatorização.

Achamo-nos numa posição de demonstrar o seguinte teorema.

Teorema 9. Seja $\alpha \in D$, $\alpha \neq 0$ e α não inversível. Então existem primos $\alpha_1, \alpha_2, \ldots, \alpha_k$ em D, tais que

$$\alpha = \alpha_1\alpha_2 \cdots \alpha_k .$$

(Nada dizemos sobre a unicidade desta fatorização).

Demonstração. Procedemos por indução sobre $\nu(\alpha)$. Se $\nu(\alpha) = 1$, então α é inversível em D e não há mais nada a provar. Suponhamos que α não é primo, então $\alpha = \beta\gamma$, onde β e γ são elementos não inversíveis de D; portanto, $\nu(\beta)$, $\nu(\gamma) > 1$. Então,

$$\nu(\alpha) = \nu(\beta)\,\nu(\gamma) \quad \text{e} \quad \nu(\beta), \nu(\gamma) < \nu(\alpha) .$$

Para terminar, aplicamos a hipótese da indução a β e γ, conseguindo assim uma fatorização de α.

c.q.d.

Eis um exemplo de D onde falha a unicidade.

Exemplo 10. Seja $D = Z[\sqrt{-6}]$. Então

$$10 = 2 \times 5 = (2 + \sqrt{-6})(2 - \sqrt{-6}) .$$

Os elementos 2, 5, $2 + \sqrt{-6}$, $2 - \sqrt{-6}$ são todos primos em D. Vamos verificar este fato para $\alpha = 2 + \sqrt{-6}$ (o leitor poderá encontrar argumentos para os outros casos). $\nu(\alpha) = 10$, e se $\beta|\alpha$ então $\nu(\beta)|10$. Considerando que $\nu(\beta) = a^2 + 6b^2$ para inteiros a, b, obtemos que $a^2 + 6b^2 | 10$ e daqui, $a = \pm 2$, $b = \pm 1$.

Já que a unicidade da fatorização dos elementos de $Z[\sqrt{n}]$, dependendo de n, pode falhar, procura-se uma saída. A procura leva a Teoria Algébrica dos Números (veja [22]), onde desenvolve-se uma teoria de fatorização para os ideais de domínios. Certos tipos de domínios chamados Domínios de Dedekind admitem um teorema de fatorização única para seus ideais.

2.2.2. $K[x]$

Mostraremos sucintamente que o conjunto dos polinômios numa variável, com coeficientes vindo de um corpo K, forma um domínio de fatorização única. Outras propriedades importantes serão também demonstradas.

1. Seja D um domínio de integridade e $D[x]$ o conjunto dos polinômios

$$f(x) = a_o + a_1x + \ldots + a_tx^t = \sum_{i=0}^{t} a_ix^i$$

com coeficientes $a_i \in D$. Os polinômios

$$f(x) = a_o+a_1x+ \ldots +a_tx^t \quad \text{e} \quad \tilde{f}(x) = a_o+a_1x+\ldots+a_tx^t + 0x^{t+1},$$

são considerados iguais. Mantendo este acordo, dizemos que $f(x) = \sum_{i=0}^{t} a_ix^i$ é igual a $g(x) = \sum_{i=0}^{s} b_ix^i$ se e somente se $a_i = b_i$ para todo i.

Chamaremos os elementos de D por <u>constantes</u>.

2. Sejam $f(x) = \sum_{i=0}^{t} a_ix^i$, $g(x) = \sum_{i=0}^{s} b_ix^i \in D[x]$; se $s < t$, acrescentamos alguns zeros ao polinômio $g(x)$ fazendo com que $g(x) = \sum_{i=0}^{t} b_ix^i$. Definimos as duas operações $+$ e $.$ por

$$f(x) + g(x) = \sum_{i=0}^{t} (a_i + b_i)x^i$$

$$f(x).g(x) = a_ob_o + (a_ob_1 + a_1b_o)x + (a_ob_2 + a_1b_1 + a_2b_o)x^2 + \ldots = \sum_{k=0}^{2t} c_kx^k ,$$

onde

$$c_k = \sum_{k=i+j} a_ib_j .$$

Verifica-se que $(D[x], +, .)$ é um anel comutativo com identidade.

3. $D[x]$ é um domínio; pois se $f(x)$, $g(x)$ são dois polinômios não nulos e a_i, b_j são seus primeiros coeficientes não nulos, então o coeficiente de x^{i+j} no produto $f(x)g(x)$ é

$$c_{i+j} = a_o b_{i+j} + \ldots + a_{i-1} b_{j+1} + a_i b_j + a_{i+1} b_{j-1} + \ldots + a_{i+j} b_o$$

$$= 0 + \ldots + 0 + a_i b_j + 0 + \ldots + 0 \neq 0 \ .$$

4. Seja $f(x) = \sum_{i=0}^{t} a_i x^i$. Se $a_t \neq 0$, então t chama-se o grau do polinômio $f(x)$ e indica-se por $\partial(f(x))$. A função $\partial: D[x] - \{0\} \to Z_{\geq 0}$ satisfaz as seguintes propriedades:

(i) $\partial(f(x)) = 0 \iff f(x) = a_o \neq 0, \ a_o \in D$,

(ii) $\partial(f(x) + g(x)) \leq \max.\{\partial(f(x)), \partial(g(x))\}$,

(iii) $\partial(f(x)g(x)) = \partial(f(x)) + \partial(g(x))$.

5. Seja K um corpo. Então $K[x]$ admite um algoritmo de divisão,

dado um par $f(x)$, $g(x) \in K[x]$ com $g(x) \neq 0$, existe um outro par $q(x)$, $r(x) \in K[x]$, único tal que

$$f(x) = q(x)g(x) + r(x) \quad \text{com} \quad \partial(r(x)) < \partial(g(x)) \text{ ou } r(x)=0.$$

$a_{m+1}(x)$ é o <u>maior divisor comum</u> de $a_1(x)$ e $a_2(x)$ (denota-se por $(a_1(x), a_2(x))$, no sentido de que

$$a_{m+1}(x) | a_1(x),\ a_2(x)$$

e

$$u(x) | a_1(x),\ a_2(x) \Longrightarrow u(x) | a_{m+1}(x) \ .$$

Também, com o mesmo argumento usado para Z, existem $\alpha(x)$, $\beta(x) \in K[x]$ tais que

$$a_{m+1}(x) = \alpha(x)a_1(x) + \beta(x)a_2(x) \ .$$

9. Seja $f(x) \in K[x]$, não constante. Então, existem $p_1(x)$, $p_2(x)$, ..., $p_k(x)$ polinômios irredutíveis e α_1, α_2, ..., $\alpha_k \in N$ tais que

$$f(x) = p_1(x)^{\alpha_1}\ p_2(x)^{\alpha_2} \ \ldots\ p_k(x)^{\alpha_k}.$$

A fatorização é única a menos de uma permutação dos fatores $p_i^{\alpha_i}(x)$ e de uma multiplicação por uma constante.

<u>Demonstração</u>. A demonstração faz-se por indução sobre $\partial(f(x))$ e segue as mesmas linhas do Teorema Fundamental da Aritmética.

2.3. EXERCÍCIOS

1) Encontrar o menor n tal que $p_1 p_2 \cdots p_n + 1$ não é primo, onde $p_1, p_2, \ldots, p_n$ são os primeiros n primos.

2) Use a demonstração de Euclides para a infinitude dos primos para concluir que

$$p_n < 2^{2^n} .$$

3) Qual é o menor n para o qual

$$n,\ n+1,\ n+2,\ n+3,\ n+4,\ n+5$$

são todos compostos?

4) Demonstre que existe um número infinito de pares de primos consecutivos não gêmeos.

5) Para cada número real $x > 0$, defina $k(x)$ = número dos inteiros quadrados menores que x. Mostre que $k(x) = [\sqrt{x}]$. Mostre também que

$$\lim_{x \to \infty} \frac{k(x)}{\pi(x)} = 0 ;$$

isto é, os quadrados são mais raros que os primos.

6) Dado o Teorema do Número Primo, mostre que o número dos primos entre x e $2x$ tende para o infinito com x.

Observação: Encontra-se em [18, página 171] a demonstração de Chebychev do postulado de Bertrand:

existe um primo entre n e $2n$ para qualquer número natural $n \geq 2$.

7) Demonstre que o número dos primos tendo a forma $6n + 5$ é infinito.

8) Verifique a conjectura de Goldbach para $n \leq 50$.

9) Verifique que o polinômio

$$p(x) = x^2 - x + 41$$

é primo para todo inteiro n tal que $0 \leq n \leq 40$.

10) Demonstre que não existe um polinômio $f(x)$ com coeficientes inteiros tal que $f(1) = 2$, $f(2) = 3$, $f(3) = 5$.

11) Seja n um inteiro não quadrado. Demonstre que não existem inteiros a, b tais que $a = b\sqrt{n}$.

12) Seja $D = Z[\sqrt{n}]$ um domínio de fatorização única, e μ um primo em D. Demonstre que existe p um primo em Z, único tal que $\mu | p$.

13) Mostrar que os elementos inversíveis em $Z[\sqrt{2}]$ são ± 1, $\pm(1 + \sqrt{2})^n$.

14) Mostrar que 3 é primo em $Z[\sqrt{-1}]$ mas não é primo em $Z[\sqrt{6}]$.

15) Sejam $f(x) = 2x + 1$, $g(x) = x^2 + x + 1$. Mostre que não existem $\alpha(x)$, $\beta(x) \in Z[x]$ tais que $\alpha(x)f(x) + \beta(x)g(x) = 1$, embora $f(x)$ e $g(x)$ não possuam fatores comuns em $Z[x]$.

16) Demonstrar o Teorema da Fatorização única em $K[x]$ (página II-28).

17) Sejam K um corpo, $\alpha_1, \alpha_2, \ldots, \alpha_s$ elementos distintos de K e $\beta_1, \beta_2, \ldots, \beta_s \in K$. Sejam também

$$\varepsilon(x) = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_s)$$

$$\varepsilon_i(x) = \frac{\varepsilon(x)}{x - \alpha_i} \quad \text{para} \quad 1 \leq i \leq s \ ,$$

$$f(x) = \sum_{i=1}^{s} \frac{\varepsilon_i(x)}{\varepsilon_i(\alpha_i)} \beta_i \ .$$

Mostre que $f(\alpha_i) = \beta_i$ para todo i.

18) Sejam t, n números naturais. Demonstre,

(i) $t|n \iff x^t - 1 | x^n - 1$,

(ii) $t|n$, $\frac{n}{t}$: ímpar $\iff x^t + 1 | x^n + 1$.

(os polinômios estão considerados como elementos de $Q[x]$).

19) Sejam a, n números naturais com $n > 1$. Demonstre,

$$a^n - 1 \text{ é primo} \Longrightarrow a = 2, \quad n: \text{primo}.$$

Observação: Os números $M_p = 2^p - 1$ onde p é primo são conhecidos por números de Mersenne (Marin Mersenne 1588-1648). Na sequência dos M_p's, o primeiro número composto tem índice $p = 11$, e o maior número primo conhecido tem índice $p = 19937$.

20) Um número natural n chama-se perfeito quando $n = \sum\{d \mid d|n \text{ e } 1 \leq d < n\}$. Demonstre que se M_p é primo então $n = 2^{p-1}M_p$ é perfeito.

Observação: Não é difícil mostrar que n é perfeito $\iff n = 2^{p-1}M_p$ onde M_p é primo.

A existência de números perfeitos ímpares é um problema clássico em aberto. Sabe-se que se existir tal número, ele deve ter pelo menos 36 algarismos.

21) Sejam $a > 1$ e n números naturais. Demonstre que

$$a^n + 1 \text{ é primo} \Longrightarrow a: \text{par}, \; n = 2^m.$$

Observação: Os números $F_k = 2^{2^k} + 1$ são conhecidos por números de Fermat (Pierre Fermat 1601-1665, advogado, juiz, e grande matemático em tempo parcial) Fermat conjecturou que F_k é sempre primo. Sabe-se hoje que F_k é primo para $1 \leq k \leq 4$ e é composto para $5 \leq k \leq 16$, e para vários outros k's maiores que 16.

CAPÍTULO III

CONGRUÊNCIAS

3.1. Congruências

A divisibilidade ganhará neste capítulo uma nova fantasia: ela vai desfilar como uma congruência!

Definição 1. Seja m um inteiro não nulo. Para quaisquer inteiros a, b, dizemos que *a é congruente com b módulo m*, denotamos por

$$a \equiv b \pmod{m},$$

se e somente se $m \mid a-b$.

Por exemplo, $70 \equiv -2 \pmod{9}$, $70 \equiv 0 \pmod{10}$, $70 \equiv 4 \pmod{11}$.

Verifica-se logo que para inteiros a, b e c,

$a \equiv a \pmod{m}$

$a \equiv b \pmod{m} \Longrightarrow b \equiv a \pmod{m}$

$a \equiv b \pmod{m}$ e $b \equiv c \pmod{m} \Longrightarrow a \equiv c \pmod{m}$;

em outras palavras, a congruência é uma relação de equivalência. Esta relação satisfaz outras propriedades importantes :

$a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$

$\Longrightarrow a + c \equiv b + d \pmod{m}$, $a.c \equiv b.d \pmod{m}$,

para quaisquer inteiros a, b, c, d; isto é, a congruência preserva as operações soma e produto. Mostraremos apenas a última, e deixaremos a outra a cargo do leitor. De $a \equiv b$, $c \equiv d \pmod{m}$, concluímos que existem inteiros q, ℓ tais que $a = b + qm$ e $c = d + \ell m$; então $ac = (b + qm)(d + \ell m) = bd + b\ell m + qmd + qm\ell m = bd + (b\ell + qd + q\ell m)m$, e pela definição de congruência, $ac \equiv bd \pmod{m}$.

A teoria das congruência módulo $(-m)$ coincide com a de módulo m. Por isso, e para simplificar nossas considerações, reservaremos neste capítulo o símbolo m para indicar um inteiro positivo.

Pelo algoritmo da divisão, o resto r da divisão de um inteiro a por m satisfaz $0 \leq r < m$. Então todo inteiro a é congruente com um elemento único de

$$M_o = \{0, 1, 2, \ldots, m - 1\}.$$

Definição 2. Seja S um conjunto de inteiros. S chama-se um sistema completo de resíduos (S.C.R.) módulo m se e somente se

(i) $s, t \in S$ e $s \neq t \Longrightarrow s \not\equiv t \pmod{m}$,

(ii) $a \in Z \Longrightarrow$ existe $s \in S$ tal que $a \equiv s \pmod{m}$.

Chamamos M_o um sistema de resíduos mínimos módulo m.

Para n um inteiro fixo, o conjunto

$$M_n: n, n+1, \ldots, n + m - 1$$

é um S.C.R. módulo m.

Precisamos verificar duas condições. A primeira diz que dois elementos distintos de M_n não podem ser congruentes módulo m; isto é válido pois se

$$n + i \equiv n + j \pmod{m}$$

para i, j com $0 \leq i, j \leq m-1$, então somando a esta

$$-n \equiv -n \pmod{m}$$

obtemos

$$i \equiv j \pmod{m} \quad .$$

Para verificar a segunda condição, usamos o seguinte teorema.

Teorema 3. Seja S um conjunto de m inteiros, dois a dois não congruentes módulo m. Então S é um S.C.R. módulo m.

Demonstração. Todo elemento s de S é congruente a algum elemento i de M_o; i é único. Então definimos

$$f: S \to M_o$$

por

$$f(s) = i \iff s \equiv i \pmod{m}.$$

f é injetora, pois se para $s_1, s_2 \in S$

$$f(s_1) = i = f(s_2)$$

então

$$s_1 \equiv s_2 \pmod{m} \quad \text{e daí} \quad s_1 = s_2 .$$

Agora o fato que S e M_o possuem o mesmo número de elementos m, implica que f é sobrejetora; em outras palavras, todo elemento de M_o é congruente com algum elemento de S.

Finalmente, consideramos qualquer inteiro a. Então existem $i \in M_o$, $s \in S$ tais que

$$\begin{matrix} a \equiv i \\ \qquad\quad \pmod{m} \\ i \equiv s \end{matrix} ,$$

e assim

$$a \equiv s \pmod{m} .$$

Teorema 4. Seja $f(x) = a_o + a_1 x + \ldots + a_k x^k$ um polinômio com coeficientes a_i's inteiros. Então vale a implicação

$$a \equiv b \pmod{m} \Longrightarrow f(a) \equiv f(b) \pmod{m},$$

para quaisquer inteiros a, b.

Demonstração.

$$f(a) - f(b) = (a_o + a_1 a + \ldots + a_k a^k) - (a_o + a_1 b + \ldots + a_k b^k)$$

$$= a_1(a-b) + a_2(a^2-b^2) + \ldots + a_k(a^k-b^k).$$

Em virtude da fatorização

$$a^i - b^i = (a-b)(a^{i-1}+a^{i-2}b + \ldots + b^{i-1}),$$

que é válida para qualquer inteiro $i \geq 1$, concluímos que

$$(a-b) \mid f(a) - f(b) \quad .$$

Então se $m \mid a-b$, evidentemente

$$m \mid f(a) - f(b).$$

c.q.d.

Exemplo 5. Seja $a = (72)^6 + (72)^5 + 2$. Mostraremos que $7 \mid a$.

Seja $f(x) = x^6 + x^5 + 2$. Dado o fato que

$$72 \equiv 2 \pmod 7 ,$$

$$f(72) \equiv f(2) \pmod 7 .$$

Calculemos $f(2)$,

$$f(2) = 2^6 + 2^5 + 2 = 64+32+2 = 98 = 14.7.$$

Teorema 6. Sejam $f(x) = a_o + a_1x + \ldots + a_kx^k$ e $g(x) = b_o + b_1x + \ldots + b_\ell x^\ell$ dois polinômios com coeficientes inteiros. Dados $a, b \in Z$, vale a implicação

$$a \equiv b \pmod{m} \Longrightarrow \begin{cases} f(a)+g(a) \equiv f(b)+g(b) \\ f(a)g(a) \equiv f(b)g(b) \end{cases} \pmod{m}.$$

Demonstração. Seja $a \equiv b \pmod{m}$. Então, pelo teorema anterior,

$$f(a) \equiv f(b), \quad g(a) \equiv g(b) \pmod{m} .$$

Como a congruência preserva as operações + e ., obtemos

$$f(a)+g(a) \equiv f(b)+g(b) , \quad f(a)g(a) \equiv f(b)g(b) \pmod{m} .$$

c.q.d.

Nota Histórica 7. A teoria das congruências foi apresentada rigorosamente por C. F. Gauss, aos vinte e quatro anos, no seu livro famoso Disquisitiones Arithmeticae de 1801. Esta obra foi traduzida em 1966 para o inglês [6].

Outros matemáticos como Pierre Fermat que precederam Gauss, conheciam o cálculo de congruências e usavam-no implicitamente. Aliás, a idéia da congruência evidencia-se em certas regras práticas, tais como a "prova dos noves fora", para a verificação dos cálculos aritméticos; essas são provavelmente heranças da antiguidade.

A "prova dos noves fora" funciona do seguinte modo :

$$93 \times 74 \neq 6782 \; ; \quad \text{porque:}$$

$$9 + 3 \to 3, \quad 7 + 4 \to 2 \text{ e } 3 \times 2 = 6$$

entretanto,

$$6 + 7 + 8 + 2 \to 5 \quad \text{que é diferente de } 6.$$

A verificação coloca-se na forma 

. A transformação $a \to b$, como é evidente, é a redução de a módulo 9 para o menor número $b \geq 0$ possível.

Esta prova baseia-se na aplicação repetida do seguinte teorema.

Teorema 8. Sejam

$$\alpha = a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_o ,$$

$$\beta = b_\ell 10^\ell + b_{\ell-1} 10^{\ell-1} + \ldots + b_o ,$$

$$\alpha + \beta = c_m 10^m + c_{m-1} 10^{m-1} + \ldots + c_o ,$$

$$\alpha\beta = d_n 10^n + d_{n-1} 10^{n-1} + \ldots + d_o ,$$

as formas decimais dos inteiros α, β, $\alpha + \beta$ e $\alpha\beta$. Então,

$$(a_k + a_{k-1} + \ldots + a_o) + (b_\ell + b_{\ell-1} + \ldots + b_o) \equiv$$

$$(c_m + c_{m-1} + \ldots + c_o) \pmod 9,$$

e

$$(a_k + a_{k-1} + \ldots + a_o)(b_\ell + b_{\ell-1} + \ldots + b_o) \equiv$$

$$(d_n + d_{n-1} + \ldots + d_o) \pmod 9.$$

Demonstração. Trocando as potências 10^i por x^i nas formas decimais de α e β obtemos polinômios $f(x)$,

$g(x)$ tais que $\alpha = f(10)$, $\beta = g(10)$. Como $10 \equiv 1 \pmod 9$, obtemos que

$$f(10) \equiv f(1) \quad e \quad g(10) \equiv g(1) \pmod 9 .$$

Então, pelo teorema provado acima,

$$f(10) + g(10) \equiv f(1) + g(1)$$

e

$$f(10).g(10) \equiv f(1)g(1) \pmod 9 .$$

Finalmente notamos que $f(1)$ (respectivamente $g(1)$) é igual a soma dos algarismos de α (resp. β), o que nos leva a conclusão desejada.

c.q.d.

A lei do cancelamento nem sempre é válida no cálculo de congruências, por exemplo

$$21 \equiv 6 \pmod{15} ,$$

porém,

$$7 \not\equiv 2 \pmod{15} .$$

Teorema 9. (i) $ab \equiv ac \pmod m \iff b \equiv c \pmod{\frac{m}{(m,a)}}$

(ii) $(a,m) = 1$, $ab \equiv ac \pmod m \implies b \equiv c \pmod m$

onde a, b, c são inteiros.

Demonstração. Sejam d, m_1, a_1 inteiros tais que

$(m,a) = d$, $m = m_1 d$, $a = a_1 d$.

Então, $(a_1, \frac{m}{d}) = 1$ e verificam-se as seguintes implicações

$$m \mid ab-ac (= a_1 d(b-c)) \iff \frac{m}{d} \mid a_1(b-c) \iff \frac{m}{d} \mid b-c \quad ,$$

o que demonstra (i). A afirmação (ii) é apenas uma consequência direta de (i)

c.q.d.

Descreveremos no teorema seguinte os elementos inversíveis módulo m.

Teorema 10. Dado um inteiro a, então a congruência

$$ax \equiv 1 \pmod{m}$$

admite solução se e somente se $(a,m) = 1$.

Demonstração. Sejam a, b inteiros. Então $ab \equiv 1 \pmod{m}$ equivale a $ab - cm = 1$ para algum inteiro c, ou seja $(a,m) = 1$. Por outro lado, se $(a,m) = 1$, então a existência de b está garantida pelo algoritmo Euclideano .

Observação 11. O inverso b de a módulo m, foi determinado módulo m; os outros são todos congruentes entre si. Assim por abuso de linguagem falaremos do inverso de a mod. m, ou da solução de $ax \equiv 1 \pmod{m}$, e o indicaremos por $(\frac{1}{a})_m$.

Teorema 12. Sejam a, b inteiros primos com m. Então temos as seguintes congruências módulo m,

(i) $a(\frac{1}{a})_m \equiv 1$,

(ii) $(\frac{1}{a})_m \equiv (\frac{1}{b})_m \Longleftrightarrow a \equiv b$,

(iii) $c = (\frac{1}{a})_m \Longrightarrow (\frac{1}{c})_m \equiv a$,

(iv) $(\frac{1}{ab})_m \equiv (\frac{1}{a})_m (\frac{1}{b})_m$.

Demonstração. (Exercício 6, III).

Exemplos 13. (i) Consideremos m = 5. Então os inversos módulo 5 de

$$a = 1, 2, 3, 4$$

são respectivamente

$$b = 1, 3, 2, 4$$

(ii) Seja m = 6. Então a = 0, 2, 3, 4 não são inversíveis. Os inversos de a = 1, 5 são 1 e 5 respectivamente.

(iii) Sejam m = 51 e a = 35. Então,

$$(\frac{1}{a})_m = -16 .$$

Teorema 14 (O Teorema de Wilson). Seja p um primo. Então,

$$(p-1)! \equiv -1 \pmod{p} \quad .$$

Demonstração. Seja $M_o = \{1, 2, 3, \ldots, p-1\}$. Defina

$$\eta: M_o \to M_o \qquad \text{por}$$

$$\eta(i) \equiv \left(\frac{1}{i}\right)_p \pmod{p} \ ,$$

para cada $i \in M_o$. Pelo teorema anterior η é bijetora. Além do mais

$$\begin{aligned} \eta(i) = i &\Longleftrightarrow i^2 \equiv 1 \pmod{p} \\ &\Longleftrightarrow p \mid (i-1)(i+1) \\ &\Longleftrightarrow i \equiv \pm 1 \pmod{p} \ . \end{aligned}$$

Então,

$$\begin{aligned} (p-1)! = 1.2.3\ldots(p-1) &\equiv 1\left[2\left(\frac{1}{2}\right)_p . 3\left(\frac{1}{3}\right)_p \ldots\right](p-1) \\ &\equiv p - 1 \equiv -1 \pmod{p}. \end{aligned}$$

c.q.d.

Definição 15. Seja S um sistema completo de resíduos módulo m. O subconjunto

$$S' = \{a \mid a \in S, \ (a,m) = 1\}$$

de S chama-se um sistema reduzido de resíduos (S.R.R.) módulo m.

Exemplo 16. Seja $m = 10$ e $S = \{0, 1, 2, \ldots, 9\}$. Então, $S' = \{1, 3, 7, 9\}$.

Teorema 17. Sejam S_1, S_2 dois sistemas completos de resíduos módulo m e S_1', S_2' os S.R.R. correspondentes. Seja também

$$f: S_1 \to S_2$$

a função definida por

$$f(s_1) = s_2 \Longleftrightarrow s_1 \equiv s_2 \pmod{m}.$$

Então f restringida a S_1' estabelece uma correspondência biunívoca entre S_1' e S_2'.

Demonstração. (Exercício 9, III).

Definição 18. Seja S um S.R.R. módulo m. Definimos $\varphi(m)$ como sendo a ordem de S. φ chama-se a função de Euler.

O teorema anterior garante que $\varphi(m)$ é independente da escolha de S. Assim, por exemplo,

$\varphi(m)$ é o número dos menores inteiros positivos que são primos com m. Eis alguns dos valores de φ,

$$\varphi(1) = 1, \quad \varphi(2) = 1, \quad \varphi(3) = 2, \quad \varphi(4) = 2, \quad \varphi(5) = 4,$$

e no caso de um primo p, $\varphi(p) = p-1$.

Teorema 19 (O Teorema de Fermat). Seja p um primo e seja a um inteiro não divisível por p. Então,

$$p | a^{p-1} - 1 \ ;$$

ou seja, na linguagem das congruências,

$$a^{p-1} \equiv 1 \ (\text{mod. } p) \ .$$

Uma generalização foi publicada por Leonard Euler em 1747. Apresentaremos esta versão, da qual o Teorema de Fermat poderá ser concluído facilmente.

Teorema 20 (Euler). Seja a um inteiro que é primo com m. Então

$$a^{\varphi(m)} \equiv 1 \ (\text{mod. } m) \ .$$

Demonstração. Seja $R = \{r_1, r_2, \ldots, r_k\}$ um sistema reduzido de resíduos módulo m e $k = \varphi(m)$. Fabricamos um outro S.R.R.,

$$aR = \{ar_1, ar_2, \ldots, ar_k\} \ ;$$

isto é verdade porque $(ar_i, m) = 1$ para todo i, e os elementos de aR são não congruentes entre si. Sabemos, pelo Teorema 17, Cap. III, que todo elemento de aR é congruente com algum elemento de R, e que a correspondência resultante entre aR e R é biunívoca. Então temos,

$$(ar_1)(ar_2)\ldots(ar_k) \equiv r_1r_2\ldots r_k \pmod{m},$$

ou seja

$$a^{\varphi(m)}\left(\prod_{i=1}^{k} r_i\right) \equiv \prod_{i=1}^{k} r_i \pmod{m}.$$

Como $\prod_{i=1}^{k} r_i$ é primo com m, ele é inversível módulo m, daí $a^{\varphi(m)} \equiv 1 \pmod{m}$.

c.q.d.

Exemplos e Observações:

(i) $71 \mid 2^{70} - 1$, $2^{35} - 1$. A primeira é uma consequência do Teorema de Fermat. Como $2^{70}-1 = (2^{35}-1)(2^{35}+1)$, $71 \mid 2^{35}-1$ ou $2^{35}+1$; a primeira possibilidade é válida e pode ser verificada diretamente.

(ii) Sejam a e m dois inteiros primos entre si, e tais que

$$a^{m-1} \not\equiv 1 \pmod{m}.$$

Então, pelo Teorema de Fermat, m não é primo. Usando um computador, este critério é útil para decidir se certos números grandes não são primos. A vantagem deste método é que ele evita o uso de uma tabela extensa de números primos.

(iii) A recíproca do Teorema de Fermat não é válida; pois existem números m compostos tais que $a^{m-1} \equiv 1 \pmod{m}$ para todo inteiro a primo com m; o primeiro desses números é $m = 561$. Retornaremos a este assunto na secção 4.3.4.

3.2. Resolução de Congruências

3.2.1. Congruências Lineares . O Teorema do Resto Chines

Teorema 21. A congruência

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

é solúvel se e somente se $(a,m)|b$. Quaisquer duas soluções (se existirem) são congruentes módulo m.

Demonstração. Seja d o máximo divisor comum de a e m. Se existir uma solução c da congruência $ax \equiv b \pmod{m}$, então $m|ac - b$, e daí, necessariamente, $d|b$. Por outro lado, se $d|b$, então resolver $ax \equiv b \pmod{m}$ equivale a resolução de $a'x \equiv b' \pmod{m'}$, onde $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ e $m' = \frac{m}{d}$. Pois, se x_o fosse uma solução da primeira congruência, ele seria também uma solução da segunda e vice versa. A solução da segunda é $\alpha = (\frac{1}{a'})_{m'} b'$ e é facilmente verificável, e que $x_o = \alpha$ é uma solução de $ax \equiv b \pmod{m}$.

A última afirmação do teorema, colocamo-la como Exercício 11, III.

Teorema 22. Seja $f(x)$ um polinômio com coeficientes inteiros. Sejam $r_1, r_2, \ldots, r_k$ uma coleção de inteiros positivos primos entre si e $m = r_1 r_2 \ldots r_k$. Então, resolver

$$f(x) \equiv 0 \pmod{m}$$

equivale resolver o sistema simultâneo das congruências

$$f(x) \equiv 0 \pmod{r_i}, \quad i = 1, 2, \ldots, k.$$

Demonstração. Seja x_o uma solução de $f(x) \equiv 0 \pmod{m}$. Então, $m \mid f(x_o)$ e obviamente $r_i \mid f(x_o)$ para todo i; ou seja, $f(x_o) \equiv 0 \pmod{r_i}$ para todo i. Reciprocamente, se $f(x_o) \equiv 0 \pmod{r_i}$, ou seja $r_i \mid f(x_o)$ para todo i, então $m = m.m.c.(r_1, \ldots, r_k) \mid f(x_o)$, e assim $f(x_o) \equiv 0 \pmod{m}$.

Exemplo 23. Consideremos a congruência

$$35x \equiv 1 \pmod{51} .$$

Tendo em vista que $51 = 3.17$, então pelo teorema anterior basta-nos resolver o sistema simultâneo,

$$35x \equiv 1 \pmod{3} , \quad 35x \equiv 1 \pmod{17} .$$

Este em si reduz-se ao

$$x \equiv -1 \pmod{3} , \quad x \equiv 1 \pmod{17}.$$

As soluções da primeira congruência sao $x_o = -1 + 3k$ para qualquer inteiro k. Dessas procuramos aquelas que satisfazem a segunda congruência. Logo, k deve satisfazer

$$-1 + 3k \equiv 1 \pmod{17};$$

i.e.,

$$3k \equiv 2 \pmod{17}.$$

Dado o fato que $(\frac{1}{3})_{17} = 6$, obtemos $k_o = 2.(\frac{1}{3})_{17} = 12$ que

é uma solução da última congruência. Então, $x_o = -1 + 3k_o =$ $= 35$ é uma solução da congruência original.

Sejam $r_1, r_2, \ldots, r_k$ uma coleção de inteiros positivos primos entre si e seja $m = r_1 r_2 \ldots r_k$. Para cada i, $(\frac{m}{r_i}, r_i) = 1$ e portanto, $(\frac{1}{m/r_i})_{r_i}$ existe. Para cada i, escolhamos o menor inverso positivo e denotemos

$$\left(\frac{1}{m/r_i}\right)_{r_i} \cdot \frac{m}{r_i} \quad \text{por} \quad \varepsilon_i ;$$

evidentemente, $\varepsilon_i \equiv 1 \pmod{r_i}$ e $\varepsilon_i \equiv 0 \pmod{r_j}$ se $i \neq j$.

Os inteiros $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k$ satisfazem as seguintes propriedades de "ortogonalidade".

Teorema 24. (i) $\varepsilon_i \varepsilon_j \equiv 0 \pmod{m} \Longleftrightarrow i \neq j$.

(ii) $\sum_{i=1}^{k} a_i \varepsilon_i \equiv \sum_{i=1}^{k} b_i \varepsilon_i \pmod{m} \Longleftrightarrow a_i \equiv b_i \pmod{r_i}$ para todo i; portanto, $\{\sum_{i=1}^{k} a_i \varepsilon_i \mid 0 \leq a_i < r_i$ para $i = 1, 2, \ldots, k\}$ forma um S.C.R. módulo m.

(iii) $\sum_{i=1}^{k} \varepsilon_i \equiv 1 \pmod{m}$.

Demonstração. (Exercício 12, III).

Teorema 25. (O Teorema do Resto Chines). Sejam a_1,

$a_2, \ldots, a_k$ uma coleção de inteiros. O sistema simultâneo de equações

$$x \equiv a_i \pmod{r_i}\ ,\ i = 1,2,\ldots,k$$

tem a solução

$$x_o = \sum_{i=1}^{k} a_i \varepsilon_i \ .$$

Além do mais, todas as soluções são congruentes entre si módulo m.

Demonstração. Para cada j, tendo em vista que $\varepsilon_j \equiv 1 \pmod{r_j}$,

$$x_o \varepsilon_j \equiv x_o \pmod{r_j} \ .$$

Por outro lado,

$$x_o \varepsilon_j = \sum_{i=1}^{k} a_i \varepsilon_i \varepsilon_j \equiv a_j \varepsilon_j^2 \pmod{m} \ .$$

Então, para cada j,

$$x_o \equiv x_o \varepsilon_j \equiv a_j \pmod{r_j} \ .$$

A última afirmação é uma simples aplicação da parte (ii) do teorema anterior.

c.q.d.

Exemplo 26. Consideremos novamente a congruência $35x \equiv 1 \pmod{51}$, cuja resolução foi mostrada equivalente à do sistema $x \equiv -1 \pmod{3}$, $x \equiv 1 \pmod{17}$. Pelo Teorema

do Resto Chines as soluções não congruentes da congruência original é

$$x_o = (\tfrac{1}{17})_3 . 17 . (-1) + (\tfrac{1}{3})_{17} . 3 . 1 \quad ,$$

$$x_o = 35 \ .$$

Manteremos no seguinte teorema a notação do Teorema do Resto Chines.

Teorema 27. Seja $f(x)$ um polinômio com coeficientes inteiros. Para cada i, $1 \leq i \leq k$, seja a_i uma solução de $f(x) \equiv 0 \pmod{r_i}$. Então,

$$x_o = \sum_{i=1}^{k} a_i \epsilon_i$$

é uma solução de $f(x) \equiv 0 \pmod{m}$.

Demonstração. O Teorema do Resto Chines afirma que $x_o \equiv a_i \pmod{r_i}$ para todo i. Daí,

$$f(x_o) \equiv f(a_i) \equiv 0 \pmod{r_i}$$

para todo i. Como $r_i | f(x_o)$ para $i = 1, 2, \ldots, k$,

$$m = m.m.c.(r_1, r_2, \ldots, r_k) | f(x_o) \ ;$$

ou seja, $f(x_o) \equiv 0 \pmod{m}$.

c.q.d.

Corolário 28. Sejam $f(x)$ um polinômio com coefici

entes inteiros, e m um inteiro positivo tendo a fatorização canônica $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Então,

$$f(x) \equiv 0 \pmod{m} \text{ tem solução}$$

$$\Longleftrightarrow$$

$$f(x) \equiv 0 \pmod{p_i^{\alpha_i}} \text{ tem solução para cada } i.$$

Exemplo 29. Encontrar todas as soluções de

$$f(x) = x^2 + 5x + 9 \equiv 0 \pmod{15}.$$

Consideremos o sistema

$$f(x) \equiv x^2 - x \equiv 0 \pmod{3}$$

$$f(x) \equiv x^2 - 1 \equiv 0 \pmod{5}.$$

As soluções não congruentes módulo 3 da primeira são $a_1 = 0$, $a_2 = 1$ e da segunda que são não congruentes módulo 5, $b_1 = -1$, $b_2 = 1$.

Então pelo Teorema do Resto Chines,

$$f(x) \equiv 0 \pmod{15}$$

admite quatro soluções não congruentes módulo 15, elas são

$$a_{ij} = (\tfrac{1}{5})_3 . 5 . a_i + (\tfrac{1}{3})_5 . 3 . b_j$$

$i, j = 1, 2$. Logo, $c_{11} = -6$, $c_{12} = 6$, $c_{21} = 4$, $c_{22} = 16$.

4.2.2. Congruências de Graus Gerais (Métodos de redução).

A resolução de $f(x) \equiv 0 \pmod{p^{\alpha}}$ onde $\alpha \geq 2$, pode ser reduzida à de $f(x) \equiv 0 \pmod{p}$. Aliás, tendo em vista que $f(x) \equiv 0 \pmod{p^{\alpha}}$ implica em $f(x) \equiv 0 \pmod{p^{\alpha-1}}$, o método para achar as soluções da primeira seria encontrar inicialmente as soluções $a_1, a_2, \ldots, a_s$, não congruentes módulo $p^{\alpha-1}$, da segunda e depois voltar para a primeira e testar $x = a_i + tp^{\alpha-1}$ onde $0 \leq t < p$.

Então o método geral consiste na construção a partir das soluções de $f(x) \equiv 0 \pmod{p}$ as de $f(x) \equiv 0 \pmod{p^2}$, e com essas subir gradativamente até chegar as de $f(x) \equiv 0 \pmod{p^{\alpha}}$. Esta subida será facilitada pelos resultados seguintes.

Seja $f(x) = a_o + a_1x + a_2x^2 + \ldots + a_kx^k$ um polinômio com coeficientes inteiros. Consideremos $f(x + y)$.

$$f(x+y) = a_o + a_1(x+y) + a_2(x+y)^2 + a_3(x+y)^3 + \ldots + a_k(x+y)^k$$

$$= a_o + a_1(x+y) + a_2(x^2+2xy+y^2) + a_3(x^3+3x^2y+3xy^2+y^3) + \ldots$$

$$= a_o + a_1x + a_2x^2 + a_3x^3 + \ldots$$
$$+ y(a_1 + 2a_2x + 3a_3x^2 + \ldots)$$
$$+ y^2(a_2 + 3a_3x + \ldots) + y^3(a_3 + \ldots)$$
$$+ \ldots$$

Esta expansão inicial sugere que

$$f(x+y) = f(x) + yf'(x) + y^2 \frac{f''(x)}{2!} + y^3 \frac{f^{(3)}(x)}{3!} + \ldots$$

que nada mais é que a expansão de Taylor!

Teorema 30. $f(x+y) = f(x) + yf'(x) + \ldots + y^i \frac{f^{(i)}(x)}{i!}$

$$+ \ldots + y^k \frac{f^{(k)}(x)}{k!} \quad ;$$

para cada i, $\frac{f^{(i)}(x)}{i!}$ é um polinômio com coeficientes inteiros.

Demonstração. (Exercício 16, III ; proceda por indução sobre k, escreva $f(x) = f_1(x) + a_k x^k$, use a hipótese da indução para desenvolver $f_1(x+y)$ e a expansão binomial para desenvolver $(x + y)^k$).

Teorema 31. Seja $f(a) \equiv 0 \pmod{p^\beta}$. Então para

$$a' = a + tp^\beta \quad ,$$

$$f(a') \equiv 0 \pmod{p^{\beta+1}} \iff tf'(a) \equiv -\frac{f(a)}{p^\beta} \pmod{p}$$

$$\iff \begin{cases} f'(a) \equiv \frac{f(a)}{p^\beta} \equiv 0 \pmod{p} \\ \text{ou} \\ (f'(a), p) = 1. \end{cases}$$

Demonstração. Seja $a' = a + tp^\beta$, onde t será determinado para que $f(a') \equiv 0 \pmod{p^{\beta+1}}$. Pela expansão de Taylor,

$$f(a') = f(a+tp^{\beta}) = f(a) + (tp^{\beta})f'(a) + (t\,p^{\beta})^2\,\frac{f''(a)}{2!} + \ldots$$

Então, de $f(a') \equiv 0 \pmod{p^{\beta+1}}$, obtem-se

$$0 \equiv f(a)+(tp\ )f'(a) \pmod{p^{\beta+1}}.$$

Tendo em vista que $p^{\beta} \mid f(a)$, esta congruência pode ser posta na forma

$$tf'(a) \equiv -\frac{f(a)}{p^{\beta}} \pmod{p},$$

e ela possui soluções se e somente se $(f'(a),p) = 1$ ou $p \mid f'(a)$, $\frac{f(a)}{p^{\beta}}$.

c.q.d.

Exemplo 32. Seja $f(x) = x^2 + 5x - 9$; então,

$$f'(x) = 2x + 5 .$$

Desejamos encontrar todas as soluções de

$$f(x) \equiv 0 \pmod{25}.$$

As soluções de

$$f(x) \equiv x^2+1 \equiv 0 \pmod{5}$$

são $x \equiv \pm 2 \pmod{5}$.

Sejam $a_1 = -2$, $a_2 = 2$. Então,

$$f(a_1) = -15,\ f(a_2) = 5,\ f'(a_1) = 1,\ f'(a_2) = 9.$$

Resolvamos

$$t_1 f'(a_1) \equiv -\frac{f(a_1)}{5}$$

e

$$t_2 f'(a_2) \equiv -\frac{f(a_2)}{5} \pmod 5 .$$

Então, $t_1 \equiv 3$ e $t_2 \equiv 1 \pmod 5$; daí as soluções de $f(x) \equiv 0 \pmod{5^2}$ são congruentes com $a_1' = -2 + 3.5 = 13$, $a_2' = 2 + 5 = 7$, módulo 25.

Embora não tenhamos meios de resolver $f(x) \equiv 0 \pmod p$ para um polinômio f de grau geral, é ainda possível reduzir f para um outro de grau menor que p.

Teorema 33. Seja p um primo. Então todo inteiro satisfaz a congruência

$$x^p \equiv x \pmod p .$$

Demonstração. O que temos aqui nada mais é que uma variação do Teorema de Fermat.

Corolário 34. Seja p um primo. Dado um polinômio $f(x)$ com coeficientes inteiros, existe $g(x)$ um polinômio com coeficientes inteiros e de grau menor que p tal que

$$f(a) \equiv g(a) \pmod p$$

para qualquer inteiro a.

Demonstração. Pelo teorema anterior,

$$x^p.x^i = x^{p+i}$$

$$\equiv x.x^i = x^{i+1} \pmod{p}$$

está satisfeita para todos os inteiros. Então $g(x)$ obtem-se trocando x^{p+i} por x^{1+i} no polinômio $f(x)$.

c.q.d.

Exemplo 35. Seja $p = 5$ e $f(x) = 2x^7+x^6+3x^3+1$. Então a congruência

$$f(x) \equiv 2x^3 + x^2 + 3x^3 + 1$$

$$\equiv 5x^3 + x^2 + 1 \equiv x^2 + 1 \pmod{5}$$

está satisfeita por todos os inteiros.

3.2.3. Congruências Quadráticas

Sejam p um primo e $f(x) = ax^2 + bx + c$ um polinômio com coeficientes inteiros tal que $(a,p) = 1$.

A nossa primeira observação, que é uma consequência direta do Teorema 33, Cap. III, é que para $p = 2$, $f(x)$ é equivalente a um polinômio linear. Daqui por diante p será um primo ímpar.

As seguintes congruências são equivalentes módulo p,

$$f(x) = ax^2 + bx + c \equiv 0 \ ,$$

$$x^2 + (\tfrac{1}{a})_p.bx + (\tfrac{1}{a})_p.c \equiv 0 \quad ,$$

$$x^2 + (\tfrac{1}{a})_p.bx + \left[(\tfrac{1}{2})_p(\tfrac{1}{a})_p b\right]^2 \equiv \left[(\tfrac{1}{2})_p(\tfrac{1}{a})_p.b\right]^2 - (\tfrac{1}{a})_p.c \ ,$$

$$4a^2\left[x + (\tfrac{1}{2a})_p.b\right]^2 \equiv b^2 - 4ac \quad .$$

Portanto, $f(x) \equiv 0 \pmod{p}$ tem soluções se e somente se $\Delta(= b^2 - 4ac)$ tem raiz quadrática módulo p (isto é, existe um inteiro n tal que $n^2 \equiv \Delta \pmod{p}$).

Quando existirem as raízes quadráticas módulo p de um inteiro d, as denotaremos por $\pm(d)_p^{1/2}$.

Assim, as soluções de $f(x) \equiv 0 \pmod{p}$ são:

$$x = (\tfrac{1}{2a})_p\left[-b \pm (\Delta)_p^{1/2}\right] \quad .$$

Exemplo 36. Seja $f(x) = 3x^2 + 7x + 1$ e seja $p=13$. Então, $\Delta = b^2 - 4ac = 49 - 12 = 37 \equiv -2 \pmod{13}$. Para decidir a questão da existência de $(-2)^{1/2}$, consideremos o S.C.R.

$$S = \{0, \pm1, \pm2, \ldots, \pm6\}$$

e

$$S^2 = \{0, 1, 4, \overset{-4}{9}, \overset{3}{16}, \overset{-1}{25}, \overset{-3}{36}\} \ .$$

Então, como -2 é não congruente a nenhum elemento de S^2 módulo 13, $(-2)^{1/2}$ não existe e $f(x) \equiv 0 \pmod{13}$ não tem solução.

Apresentaremos a seguir um critério para decidir se -1 tem raízes quadráticas módulo p.

Decidir se um inteiro tem ou não raízes quadráticas módulo p será assunto exclusivo do Capítulo VI.

Teorema 37. $x^2 \equiv -1 \pmod{p}$ tem solução se e somente se $p = 4k + 1$ para algum inteiro k.

Demonstração. ($\Longrightarrow$) Seja a um inteiro tal que

$$a^2 \equiv -1 \pmod{p}.$$

Então, pelo Teorema de Fermat,

$$a^{p-1} \equiv 1 \equiv (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p} ;$$

daí, $\frac{p-1}{2}$ é par.

($\Longleftarrow$) Esta parte é uma aplicação do Teorema de Wilson: $(p-1)! \equiv -1 \pmod{p}$.

$$\begin{aligned} 1.2.3\ldots(p-3)(p-2)(p-1) &= 1.(p-1).2.(p-2)\ldots(\tfrac{p-1}{2})(\tfrac{p+1}{2}) \\ &\equiv (-1^2)(-2^2)\ \ldots\ (-(\tfrac{p-1}{2})^2) \\ &\equiv (-1)^{\frac{p-1}{2}}\ (1.2\ldots\tfrac{p-1}{2})^2 \pmod{p}. \end{aligned}$$

Como $\frac{p-1}{2}$ é par e $(p-1)! \equiv -1 \pmod{p}$, obtemos

$$(\tfrac{p-1}{2}!)^2 \equiv -1 \pmod{p}.$$

c.q.d.

3.3. A Função de Euler (Fórmula)

Teorema 38. Seja $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ a fatorização canônica de m como produto de potências de primos. Então,

$$\varphi(m) = \prod_{i=1}^{k} p_i^{\alpha_i - 1} (p_i - 1).$$

Apresentaremos a seguir duas demonstrações; a primeira é direta e depende de considerações sobre a ordem da união de vários conjuntos; a segunda é uma aplicação do Teorema do Resto Chines.

Demonstração 1. Consideremos os conjuntos $T = \{i \mid 0 \leq i < n\}$ e $T' = \{i \mid 0 < i < n \text{ e } (i,n) = 1\}$. Em vez de calcular $|T'|$, calculamos a ordem de seu complemento U em T (Claro que $|T'| = |T| - |U|$). U consiste dos números a tais que $1 \leq a \leq m$, e $(a,m) \neq 1$. Então, $a \in U \Longrightarrow a$ é divisível por algum p_j, $1 \leq j \leq k$. Expressamos este fato como

$$U = U_{p_1} \cup U_{p_2} \cup \ldots \cup U_{p_k}$$

onde, para $r|m$ e $r > 1$, definimos

$$U_r = \{a \mid a \in U \text{ e } r|a\} .$$

Observamos que

$$U_r = \{1.r,\ 2.r,\ \ldots,\ \tfrac{n}{r}.r\}$$

e portanto

$$|U_r| = \frac{n}{r} \quad .$$

Observamos também que

$$U_r \cap U_s = U_{rs} \ ,$$

quando $(r,s) = 1$.

Interrompemos a demonstração para fazermos umas considerações sobre a ordem da união de vários conjuntos finitos.

Nota-se a seguinte fórmula para calcular a ordem da união dos conjuntos finitos A e B:

$$|A \cup B| = |A| + |B| - |A \cap B| \ ;$$

a qual pode ser generalizada, com a ajuda da lei distributiva

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C),$$

onde C é um terceiro conjunto:

$$|A \cup B \cup C| = (|A|+|B|+|C|)-(|A \cap B|+|A \cap C|+|B \cap C|) + \\ + |A \cap B \cap C|$$

De modo geral, considerando $A_1, A_2, \ldots, A_k$ conjuntos finitos, e

$$A_{i_1 i_2, \ldots i_t} = A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_t}$$

para $1 \leq i_1 < i_2 < \ldots < i_t \leq k$, obtem-se a fórmula

$$(*) \quad \left|\bigcup_{i=1}^{k} A_i\right| = \sum_{i=1}^{k} |A_i| - \sum_{i_2=2}^{k} |A_{i_1 i_2}| + \ldots$$

$$+ (-1)^{t+1} \sum_{i_t=t}^{k} |A_{i_1 i_2 \ldots i_t}| + \ldots + (-1)^{\varepsilon} |A_{12\ldots k}|$$

onde $\varepsilon = 1$ se k é par e -1 se k é ímpar.

Voltemos para a demonstração. Ao aplicar a fórmula (*) a U e depois de incorporar o resultado em $|T'| = |T| - |U|$, obtemos

$$|T'| = m(1 - \sum_{i=1}^{k} \frac{1}{p_i} + \sum_{i_2=1}^{k} \frac{1}{p_{i_1} p_{i_2}} + \ldots$$

$$+ \ldots + (-1)^{\varepsilon} \frac{1}{p_1 p_2 \cdots p_k}) \quad .$$

Surpresa!! A expressão entre os parêntesis nada mais é que o desenvolvimento de

$$\prod_{i=1}^{k} (1 - \frac{1}{p_i}) \quad ;$$

daí

$$|T'| = \varphi(m) = \prod_{i=1}^{k} p_i^{\alpha_i} (1 - \frac{1}{p_i}) = \prod_{i=1}^{k} p_i^{\alpha_i - 1} (p_i - 1).$$

c.q.d.

Demonstração 2. Dividamos a demonstração em dois lemas.

Lema 1. φ é multiplicativa no sentido seguinte:

$$m = rs,\ (r,s) = 1 \Longrightarrow \varphi(m) = \varphi(r)\varphi(s).$$

Consideramos um exemplo. Seja $m = 15 = 3.5$, e seja $M'_o = \{1, 2, 4, 7, 8, 11, 13, 14\}$, que é um S.R.R. módulo 15. Construamos o seguinte quadro, onde $i \in M'_o$:

i	1	2	4	7	8	11	13	14
i mod. 3	1	2	1	1	2	2	1	2
i mod. 5	1	2	4	2	3	1	3	4

Notamos que as colunas formadas por i (mod. 3), i(mod. 5) são todas distintas.

Demonstração do Lema 1. Sejam M'_o , R'_o , S'_o os S.R.R. mínimos módulo m, r e s respectivamente, Definimos,

$$\rho: M'_o \to R'_o \times S'_o$$

por $$\rho(i) = (j_1, j_2) \ ,$$

onde $i \equiv j_1 \pmod{r}$, $i \equiv j_2 \pmod{s}$. Mostraremos que é bijetora e de tal fato concluíremos que

$$\varphi(m) = |M'_o| = |R'_o \times S'_o| = |R'_o\ S'_o| = \varphi(r)\varphi(s).$$

Sejam $i_1 \in R'_o$ e $i_2 \in S'_o$; então pelo Teorema do

Resto Chines existe x_o tal que

$$x_o \equiv i_1 \pmod{r},\ x_o \equiv i_2 \pmod{s}.$$

É claro que $(x_o, m) = 1$. Agora seja i o mínimo resíduo de x_o (mod. m). Então temos

$$\rho(i) = (i_1, i_2) \quad ; \quad \text{ou seja,}$$

ρ é sobrejetora. O que falta agora é mostrar que ρ é injetora. Mas isto é fácil: se $\rho(i) = \rho(i') = (j_1, j_2)$, então ,

$$i \equiv i' \equiv j_1 \pmod{r}\ ,\ i \equiv i' \equiv j_2 \pmod{s}\ ,$$

e daí,

$$r, s \mid i - i' \quad , \quad m \mid i - i' \ .$$

c.q.d

Lema 2. Seja p um primo e $\alpha > 0$. Então

$$(p^{\alpha}) = p^{\alpha-1}(p - 1).$$

(A demonstração faz-se por contagem. Neste particular, as duas demonstrações do teorema coincidem).

Terminando, consideremos a fatorização canônica de m, $m = \prod_{i=1}^{k} p_i^{\alpha_i}$. Então por aplicações repetidas dos Lemas 1 e 2, obtemos,

$$\varphi(m) = \prod_{i=1}^{k} (p_i^{\alpha_i}) = \prod_{i=1}^{k} p_i^{\alpha_i - 1} (p_i - 1).$$

c.q.d.

3.4. Exercícios

1) Encontrar todo n tal que $n \equiv 5 \pmod{19}$, com $0 < n < 100$.

2) Dê um sistema completo de resíduos módulo19 cujos elementos são todos múltiplos de 5.

3) Dê um exemplo que mostre a falibilidade da "prova dos nove fora".

4) Mostrar que

$$sa \equiv sb \pmod{sr} \Longrightarrow a \equiv b \pmod{r}.$$

5) Encontre as soluções das congruências

$$5x \equiv 1 \pmod{19}, \quad 5x \equiv 16 \pmod{19}.$$

6) Demonstrar o Teorema 12, III.

7) Dê um exemplo de um sistema reduzido de resíduos módulo 50.

8) Mostre que $m > 1$ é primo se e somente se $m \mid (m-1)!+1$.

9) Demonstrar o Teorema 17, III.

10) Demonstrar que $42 \mid n^7 - n$ para todo inteiro n.

11) Demonstrar a última afirmação do Teorema 21, III.

12) Demonstrar o Teorema 24, III.

13) Encontre todas as soluções não congruentes de cada uma das seguintes congruências

$$3x \equiv 14 \pmod{35}, \quad 47x \equiv 85 \pmod{100}.$$

14) Resolver as congruências

$$x^2 + 5x + 6 \equiv 0 \pmod{5}$$
$$x^2 + 5x + 6 \equiv 0 \pmod{7}$$
$$x^2 + 5x + 6 \equiv 0 \pmod{35}.$$

15) Seja $f(x) \in Z[x]$, $m = r_1 r_2 \ldots r_s$ onde $r_1, r_2, \ldots, r_s$ são números naturais primos entre si. Sejam também N_i o número das soluções não congruentes módulo r_i de $f(x) \equiv 0 \pmod{r_i}$ para todo i. Encontre uma fórmula para o número N das soluções não congruentes módulo m de $f(x) \equiv 0 \pmod{m}$ em termos dos N_i's.

16) Demonstre o Teorema 30, III.

17) Encontre todas as soluções não congruentes da congruência $x^2 + 5x + 6 \equiv 0 \pmod{75}$.

18) Sejam r, s números naturais e $t = (r,s)$. Mostre que

$$a^r \equiv 1 \equiv a^s \pmod{m} \Longrightarrow a^t \equiv 1 \pmod{m}.$$

19) Sejam $q_1, q_2, \ldots, q_k$ os primeiros k primos da forma $4n + 1$. Use o Teorema 37, IV para mostrar

$$p \text{ primo}, \; p \mid \left(\prod_{i=1}^{k} q_i^2\right) + 1 \Longrightarrow p = 4\ell + 1 \text{ para algum inteiro } \ell.$$

Assim, pode concluir que existe uma infinitude de primos da forma $4n + 1$.

20) Calcule $\varphi(n)$ para $n = 5, 10, 100, 3.600$.

21) Encontre todo n tal que $\varphi(n)$ é ímpar.

22) Dado n um número natural, mostre que $\varphi(x) = n$ tem um número finito de soluções.

23) Pesquisar as propriedades do número n para o qual

$$\varphi(x) = n$$

tem somente uma solução.

A coleção das classes distintas indica-se por $R/_I = \{I + a | a \in S$, onde S é o conjunto dos representantes das classes distintas. $R/_I$ faz-se num anel simplesmente por

$$(I + a) + (I + b) = I + (a + b)$$

$$(I + a).(I + b) = I + a.b \ .$$

$R/_I$ chama-se um <u>anel quociente</u> de R. (verifique que $(R/_I, +, .)$ é um anel!).

Congruência módulo m define uma relação de equivalência sobre Z, o que nos fornece uma partição dos inteiros

$$Z = \bigcup \{S(a) | a \in Z\}$$

onde

$$S(a) = \{b | b \equiv a \ (\text{mod. } m)\} \ ;$$

costuma-se indicar $S(a)$ por $\overline{a}$. Ao escolhermos um sistema completo de resíduos, digamos R_o: 0, 1, ..., m - 1, obtemos

$$Z = \overline{0} \cup \overline{1} \cup \ \ldots \cup \overline{m - 1} \ .$$

Assim por exemplo, quando $m = 2$,

$$Z = \overline{0} \cup \overline{1} \ ,$$

onde

$$\overline{0} = \{\ldots, -4, -2, 0, 2, 4, \ldots\} \ ,$$

$$\overline{1} = \{\ldots, -3, -1, 1, 3, 5, \ldots\} \ .$$

Notamos que $\overline{0}$ é um ideal de Z gerado por m, e que

$$\overline{i} = \overline{0} + i \quad , \quad \text{para} \quad 0 \leq i < m - 1 \ .$$

Então

$$\frac{Z}{\overline{I}} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\} \ ,$$

denotado por Z_m , faz-se um anel mediante o processo definido acima. Z_m é um anel comutativo possuindo m elementos, onde a identidade da soma é $\overline{0}$, e a identidade do produto é $\overline{1}$.

Apesar de que Z seja um domínio, Z_m pode deixar de sê-lo, isto é, dependendo de m, pode existir divisores de zero em Z_m .

Por exemplo, se $m = 6$, então $\overline{3}$ e $\overline{4}$ são diferentes de $\overline{0}$, mas

$$\overline{3}.\overline{4} = \overline{12}$$

e como $12 \equiv 0 \pmod{6}$,

$$\overline{12} = \overline{0} \ .$$

Teorema 1. Seja $\overline{a} \neq \overline{0}$. Então,

(i) $\overline{a}$ é um divisor de zero $\Longleftrightarrow$ $(a,m) \neq 1$,

(ii) $\overline{a}$ é inversível $\Longleftrightarrow$ $(a,m) = 1$.

Demonstração. Seja $(a,m) = d$. Então,

$$\overline{\left(\frac{m}{d}\right)} \neq \overline{0} \Longleftrightarrow d \neq 1 \ .$$

Quando $d \neq 1$, podemos verificar que $\bar{a}.\overline{(\frac{m}{d})} = \bar{0}$; ou igualmente, que $\bar{a}$ é um divisor de zero.

Quando $d = 1$, existem inteiros α, β tais que $1 = \alpha a + \beta m$; ou na linguagem de congruência,

$$\alpha a \equiv 1 \pmod{m} ,$$

o que se traduz em

$$\bar{\alpha}\,\bar{a} = \bar{1} .$$

Então $\bar{\alpha}$ é o inverso multiplicativo de $\bar{a}$; em particular fica mostrado que $\bar{a}$ não pode ser um divisor de zero: se $\bar{0} = \bar{a}.\bar{b}$, então

$$\bar{0} = \bar{\alpha}.\bar{0} = \bar{\alpha}.\bar{a}.\bar{b} = (\bar{\alpha}.\bar{a})\bar{b} = \bar{b} .$$

c.q.d.

Sejam

$D(m) = \{\bar{a} \mid \bar{a} \in Z_m ,\ \bar{a}$ divisor de zero$\}$,

$U(m) = \{\bar{a} \mid \bar{a} \in Z_m ,\ \bar{a}$ inversível$\}$.

Corolário 2. (i) $Z_m = D(m) \cup U(m)$,

(ii) $D(m) \cap U(m) = \phi$,

(iii) $D(m)$ é fechado para o produto,

(iv) $U(m)$ é um grupo de ordem $\varphi(m)$.

Corolário 3. Se Z_m é um domínio, então m é primo e Z_m é um corpo.

As demonstrações desses corolários serão relegados aos Exercícios 2 e 3, IV.

5.2. Estrutura do Anel Z_m.

Sejam A e B dois aneis com identidades. O conjunto

$$C = A \times B = \{(a,b) | a \in A , \quad b \in B\}$$

pode ser transformado num anel com identidade, definindo as operações na seguinte forma,

$$(a,b) + (a',b') = (a + a', b + b')$$

$$(a,b).(a',b') = (aa', bb') \quad ;$$

a identidade de $A \times B$ é $(1,1)$.

O novo anel contém "cópias" de A e B. Pois valem as afirmativas

$A' = \{(a,0) | a \in A\}$ é isomorfo com A,

$B' = \{(0,b) | b \in B\}$ é isomorfo com B,

$$A', B' \subseteq C \quad .$$

Além do mais, todo elemento de C é a soma de um elemento

de A' com um elemento de B',

$$(a,b) = (a,0) + (b,0);$$

um fato que exprime-se por

$$C = A' + B' \ ;$$

aliás esta expressão de (a,b) é única para todo $a \in A$, $b \in B$, o que se exprime por

$$C = A' \oplus B' \ .$$

Teorema 4. Seja $m = rs$, onde r e s são inteiros primos entre si. Então,

(i) $Z_m = Z_m\,\overline{r} \oplus Z_m\,\overline{s}$,

(ii) $Z_m\,\overline{r} \cong Z_s$ e

$Z_m\,\overline{s} \cong Z_r$,

(iii) $Z_m \cong Z_s \times Z_r$.

Antes de dar a demonstração vamos experimentar com um exemplo.

Exemplo 5. Sejam $m = 6$, $r = 2$, $s = 3$. Então,

$Z_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$,

$Z_6\,\overline{2} = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\} = \{\overline{0}, \overline{2}, \overline{4}\}$,

e $Z_6\,\overline{3} = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}\} = \{\overline{0}, \overline{3}\}$.

Um fato que é braçalmente verificável é que todo elemento de Z_6 é a soma de elementos únicos de $Z_6\ \overline{2}$ e $Z_6\ \overline{3}$; dito diferentemente, $Z_6 = Z_6\ \overline{2} \oplus Z_6\ \overline{3}$.

Seja $A = Z_6\ \overline{2}$; A é um anel. A igualdade

$$\overline{4}.\overline{4} = \overline{16} = \overline{4} \quad ,$$

sugere que $\overline{4}$ é a identidade multiplicativa de A. Aliás, temos

$$\overline{0} = \overline{0}.\overline{4} \ , \quad \overline{2} = \overline{2}.\overline{4} \quad , \quad \overline{4} = \overline{1}.\overline{4} \quad .$$

Notamos que

$$\overline{i}.\overline{4} + \overline{j}.\overline{4} = \overline{(i+j)}.\overline{4} = \overline{k}.\overline{4} \quad ,$$

onde k satisfaz

$$i+j \equiv k \pmod 3$$

$$0 \leq k < 3 \quad ,$$

e no caso do produto que

$$\overline{i}.\overline{4}.\overline{j}.\overline{4} = \overline{i.j}.\overline{4} = \overline{k}.\overline{4} \ ,$$

onde k satisfaz

$$ij \equiv k \pmod 3$$

$$0 \leq k < 3$$

Ora, a conclusão é evidente:

$$Z_6\ \overline{2} = \{\overline{0.4},\ \overline{1.4},\ \overline{2.4}\}$$

é um Z_3 disfarçado! Isto é,

$$Z_6\ \overline{2} \cong Z_3 \ .$$

Numa maneira semelhante concluímos que

$$Z_6\ \overline{3} \cong Z_2 \ .$$

Demonstração do Teorema 4. Sejam

$$\varepsilon_1 = (\frac{1}{m/r})_r \frac{m}{r} = (\frac{1}{s})_r\ s \ ,$$

$$\varepsilon_2 = (\frac{1}{m/s})_s \frac{m}{s} = (\frac{1}{r})_s\ r \ .$$

Então, pelo Teorema do Resto Chines, o conjunto

$$S = \{a_1\varepsilon_1 + a_2\varepsilon_2 \mid 0 \le a_1 < r\ ,\ \ 0 \le a_2 < s\}$$

contém rs (= m) elementos não congruentes módulo m; ou seja , S é um SCR módulo m.

Recordamos que em Z_m valem

$$\overline{\varepsilon}_1\overline{\varepsilon}_2 = \overline{0}\ ,\ \ \overline{\varepsilon}_1^{\,2} = \overline{\varepsilon}_1\ ,\ \ \overline{\varepsilon}_2^{\,2} = \overline{\varepsilon}_2\ ,$$

e que $$|Z_m\ \overline{\varepsilon}_1| = r,\ \ |Z_m\ \overline{\varepsilon}_2| = s.$$

Definamos as funções

$$\epsilon_1 : Z_r \to Z_m\,\bar{\epsilon}_1 \qquad , \qquad \epsilon_2 : Z_s \to Z_m\,\bar{\epsilon}_2$$

por

$$\epsilon_1(\bar{a}) = \bar{a}.\bar{\epsilon}_1 \qquad , \qquad \epsilon_2(\bar{a}) = \bar{a}.\bar{\epsilon}_2 \quad ,$$

respectivamente. ϵ_1 , ϵ_2 estabelecem os isomorfismos

$$Z_r \cong Z_m\,\bar{\epsilon}_1 \ , \quad Z_s \cong Z_m\,\bar{\epsilon}_2 \ ,$$

respectivamente. Finalmente, a função

$$\epsilon_1 \times \epsilon_2 : Z_r \times Z_s \to Z_m$$

definida por $\epsilon_1 \times \epsilon_2(a,b) = \bar{a}.\bar{\epsilon}_1 + \bar{b}.\bar{\epsilon}_2$, é um isomorfismo de $Z_r \times Z_s$ sobre Z_m .

c.q.d.

<u>Corolário 5</u>. Seja $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Então,

$$Z_m \cong Z_{p_1^{\alpha_1}} \times Z_{p_2^{\alpha_2}} \times \ldots \times Z_{p_k^{\alpha_k}} \ .$$

4.3. <u>U(m)</u>

Daremos nesta secção uma descrição bem detalhada da estrutura algébrica do grupo U(m) das unidades (elementos

inversíveis) do anel Z_m .

Sabemos que $U(m)$ é um grupo comutativo de ordem $\varphi(m)$. Apresentaremos a seguir o primeiro resultado sobre a decomposição de $U(m)$.

Teorema 6. Seja $m = rs$, com $(r,s) = 1$. Então,

$$U(m) \cong U(r) \times U(s) \ ,$$

donde,

$$\varphi(m) = \varphi(r)\varphi(s) \ .$$

Demonstração. Sejam $u = (u_1,u_2)$, $u' = (u_1',u_2')$, dois elementos de $Z_r \times Z_s$. Então,

$uu' = (1,1)$ (a identidade multiplicativa de $Z_r \times Z_s$)

$\Longleftrightarrow u_1u_1' = 1$ e $u_2u_2' = 1$;

em outras palavras, o grupo das unidades do anel $Z_r \times Z_s$ é $U(r) \times U(s)$.

Ao restringir

$$e_1 \times e_2 : Z_r \times Z_s \to Z_m$$

o isomorfismo definido na Secção 5.2, pág. 9, a $U(r) \times U(s)$, obtemos um isomorfismo entre $U(r) \times U(s)$ e $U(m)$.

c.q.d.

Corolário 7. Sejam $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ a fatorização canônica de m. Então,

$$U(m) \cong U(p_1^{\alpha_1}) \times U(p_2^{\alpha_2}) \times \ldots \times U(p_k^{\alpha_k}) \quad .$$

Demonstração. (Óbvia).

Tendo em vista a decomposição de U(m), a nossa tarefa de descrever U(m) limita-se a investigar a estrutura de $U(p^{\alpha})$, onde p é primo. Para este fim injetaremos em nosso discurso uma dose (esperamos que não esteja forte demais) de Teoria dos Grupos.

4.3.1. Variantes da Notação (G, *).

Sabemos que um grupo é um par (G, *) formado por um conjunto não vazio G, e uma operação *. Costuma-se trocar o símbolo "*" por "." e passar logo a fazer as seguintes permutações

a*b	por a.b ou ab
a identidade e	1
a*a*a*...*a (k vezes)	a^k
o inverso de a	a^{-1}

É um hábito comum, suprimir o símbolo da operação "." da notação (G,.); assim fala-se simplemente do grupo G .

Quando o grupo $(G,*)$ é comutativo ($a*b = b*a$ para todos $a, b \in G$), convem muitas vezes fazer as seguintes trocas

$a * b$	por	$a + b$
a identidade e	"	0
$a*a*\ldots*a$ (k vezes)	"	ka
o inverso de a	"	$-a$;

a notação aditiva é preferível quando é preciso considerar $a.a\ldots a(= a^k)$; pois a forma aditiva é $k^t a$.

4.3.2. Grupos Cíclios - O Teorema de Lagrange

Definição 8. Sejam $(G, .)$ um grupo e $a \in G$.

(i) $\langle a \rangle$ indica o conjunto $\{a^k | k \in Z\}$, que é um subgrupo de G.

(ii) A ordem de a, denotada por $o(a)$, define-se como sendo a ordem do grupo $\langle a \rangle$.

(iii) Se $G = \langle a \rangle$ então diz-se que G é um grupo cíclico.

Os dois exemplos canônicos de grupos cíclicos são $(Z, +)$, de ordem infinita, e $(Z_n, +)$, de ordem n.

Denotamos o grupo $(Z_n, +)$ por $C(n)$.

Teorema 9. Seja G um grupo cíclico de ordem n. Então, $G \cong C(n)$.

Demonstração. Seja $a \in G$ tal que $G = \langle a \rangle$. Defina

$$\sigma: G \to C(n)$$

por $\sigma(a^k) = \overline{k}$ para qualquer inteiro k. σ é um isomorfismo de G sobre $C(n)$. c.q.d.

Teorema 10. Sejam r e s dois inteiros naturais primos entre si. Então

$$C(r) \times C(s) \cong C(rs) \quad .$$

Demonstração. Definamos $\sigma: C(r) \times C(s) \to C(rs)$ por

$$\sigma(\overline{\ell}, \overline{m}) = \overline{x_o} \quad ,$$

onde

$$x_o = (\tfrac{1}{s})_r \, s\ell + (\tfrac{1}{r})_s \, rm \quad ;$$

recordemos que x_o é a solução do sistema

$$x \equiv \ell \pmod{r}$$

$$x \equiv m \pmod{s} \quad ,$$

como temos visto no Teorema do Resto Chines. É fácil verificar que σ estabelece o isomorfismo desejado.

c.q.d.

Teorema 11. Sejam G um grupo, $a \in G$ de ordem finita e m, r inteiros não negativos. Então,

(i) $a^m = 1 \Longleftrightarrow o(a) \mid m$,

(ii) $o(a) = n \Longrightarrow o(a^r) = \frac{n}{(n,r)}$.

Demonstração. (i) Lembremos que $o(a)$ denota a ordem do conjunto $\{a^i \mid i \in Z\}$. Por consequência da finitude de $o(a)$, existem k, ℓ inteiros distintos tais que $a^k = a^\ell$. Então,

$$a^k.a^{-\ell} = a^{k-\ell} = a^\ell.a^{-\ell} = 1$$

e

$$1 = (a^{k-\ell})^{-1} = a^{\ell-k} \quad ;$$

daí segue-se que

$$\mathcal{O} = \{t \mid t > 0 \text{ e } a^t = 1\}$$

não é vazio. Estudemos o menor elemento n de $\mathcal{O}$. Em primeiro lugar,

$$\langle a \rangle = \{a^i \mid 0 \leq i < n\} \quad ;$$

pois, qualquer que seja $j \in Z$,

$$a^{n+j} = a^n.a^j = 1.a^j \ .$$

Dado a minimilidade de n, não pode haver coincidências no conjunto $\langle a \rangle$ descrito acima; i.e., $o(a) = n$. Em segundo lugar,

$$t \in \mathcal{O} \Longrightarrow n \mid t \quad :$$

pelo algoritmo da divisão, existem q, s inteiros tais que $t = nq + s$ com $0 \leq s < n$; portanto,

$$1 = a^t = a^{nq+s} = (a^n)^q . a^s = 1 . a^s \quad ,$$

e da minimalidade de n, $s = 0$.

(ii) Seja $u \in Z$. Pela parte (i) tem-se

$$(a^r)^u = 1 \Longleftrightarrow n \mid ru$$

e claro,

$$n \mid ru \Longleftrightarrow \frac{n}{(n,r)} \mid u \quad .$$

c.q.d.

Teorema 12. (O Teorema de Lagrange) Seja G um grupo finito e seja H um subgrupo de G. Então

$$|H| \;\Big|\; |G| \quad .$$

Demonstração. Definamos uma relação $\sim$ sobre G: dados $a, b \in G$,

$$a \sim b \Longleftrightarrow ab^{-1} \in H \quad ;$$

verifica-se diretamente que $\sim$ é uma relação de equivalência.

Seja $a \in G$. Então,

$$\bar{a} = \{b \mid b \in G, \quad b \sim a\}$$

é uma classe de equivalência representada por a. Dado $b \in \bar{a}$ tem-se que $ba^{-1} = h$ e que $b = ha$ para algum $h \in H$. Por conseguinte vale

$$\bar{a} = \{ha \mid h \in H\} .$$

O conjunto $\bar{a}$ é denotado por Ha e é chamado uma classe lateral a direita de H em G.

Nota-se que, para $h, h' \in H$,

$$ha = h'a \Longrightarrow ha.a^{-1} = h'a.a^{-1} \Longrightarrow h = h' \quad ,$$

e portanto,

$$|Ha| = |H| \quad .$$

Naturalmente, $\sim$ sendo uma relação de equivalência sobre G, as classes de equivalência (de número necessariamente finito, pois G é finito) formam uma partição de G. Sejam $a_1, a_2, \ldots, a_k \in G$, representantes das diferentes classes (k chama-se índice de H em G e denota-se por $[G:H]$). Então,

$$G = Ha_1 \cup Ha_2 \cup \ldots \cup Ha_k$$

com

$$Ha_i \cap Ha_j = \phi \quad \text{se} \quad i \neq j .$$

Finalmente, contamos a ordem de G,

$$|G| = |Ha_1| + |Ha_2| + \ldots + |Ha_k|$$

$$= k|H| .$$

c.q.d.

Corolário 13. Seja G um grupo finito de ordem n. Então vale

$$a^n = 1$$

para qualquer $a \in G$.

(Na linguagem de equações: todo elemento de G é uma solução da equação $x^n = 1$).

Demonstração. Pelo Teorema de Lagrange, $o(a)|n$ e assim, $a^n = 1$.

c.q.d.

Corolário 14. (Teorema de Euler) Seja $\bar{a} \in U(m)$. Então,

$$\bar{a}^{\varphi(m)} = \bar{1} \ ;$$

isto é,

$$(a,m) = 1 \Longrightarrow a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Demonstração. É suficiente mencionar que $|U(m)| = \varphi(m)$.

4.3.3. Teoremas de Decomposição para Grupos Comutativos Finitos.

Sejam $(A,+)$, $(B,+)$ dois grupos comutativos. O grupo $(A \times B, +)$ definido por

$$(a,b) + (a',b') = (a + a', b + b')$$

para quaisquer $a, a' \in A$, $b, b' \in B$, é um grupo comutativo.

Mostraremos nos dois teoremas seguintes que o grupo

$$C(2) \times C(2^2) \times C(5) \times C(7) \times C(7^3)$$

é um exemplo típico de um grupo comutativo finito.

Teorema 15. Sejam G um grupo comutativo finito não trivial ($|G| > 1$) e p um primo. Suponhamos que todo elemento de G é de ordem potência de p. Então existem inteiros positivos $\beta_1, \beta_2, \ldots, \beta_t$ tais que

$$G \cong C(p^{\beta_1}) \times C(p^{\beta_2}) \times \ldots \times C(p^{\beta_t}) .$$

$|G| = p^{\alpha}$ onde $\alpha = \beta_1 + \beta_2 + \ldots + \beta_t$.

Demonstração. A operação de G será "+". Descreveremos em seguida um processo iterativo para conseguir a decomposição desejada.

Escolha $a_1 \in G$ com a maior ordem possível. Seja $A_1 = \langle a_1 \rangle$. Se $B_1 = \{b | b \in G, \langle b \rangle \cap A_1 = \{0\}\}$ for vazio pa

ramos a construção; no caso contrário, escolhemos $a_2 \in B_1$, com a maior ordem possível. Seja $A_2 = \langle a_1 \rangle \oplus \langle a_2 \rangle$. Se $B_2 = \{b \mid b \in G, \langle b \rangle \cap A_2 = \{0\}\}$ for vazio, paramos a construção; no caso contrário, escolhemos $a_3 \in B_2$ com a maior ordem possível. Seja $A_3 = \langle a_1 \rangle \oplus \langle a_2 \rangle \oplus \langle a_3 \rangle$. Etc... O fato que G é finito implica na existência de k tal que B_k é vazio; pois $|A_{i+1}| = |A_i| . o(a_{i+1})$.

Mostraremos que $A_k = G$. Será suficiente provar uma proposição que nos dê $b \in G$ com $\langle b \rangle \cap A_i = \{0\}$ toda vez que $G - A_i \neq \phi$. Em termos exatos: se $b \in G - A_i$ onde $1 \leq i \leq k$, então existe $a \in A_i$ tal que $\langle b-a \rangle \cap A_i = \{0\}$.

Procedemos por indução sobre i. Seja $i = 1$. Seja também ℓ o menor inteiro tal que $p^\ell b \in A_1$. Então, $p^\ell b = up^m a_1$ para $u, m \in Z$, $(u,p) = 1$ e $m \geq 0$. De $o(a_1) \geq o(b)$ obtemos $m \geq \ell$; porque,

$$o(p^\ell b) = \frac{o(b)}{p^\ell} = o(up^m a_1) = o(p^m a_1) = \frac{o(a_1)}{p^m} ,$$

donde, $p^m \geq p^\ell$ e $m \geq \ell$. Assim,

$$p^\ell(up^{m-\ell} a_1 - b) = 0 .$$

Sejam $a = up^{m-\ell} a_1$ e $b' = a - b$; então, $\langle b' \rangle \cap A = \{0\}$ (verifique!).

Agora suponhamos que a proposição esteja válida para $i > 1$. Vamos mostrá-la para $i + 1$. Pois bem, seja $b \in G - A_{i+1}$;

: $\langle b \rangle \cap A_{i+1} = \{0\}$, escolhemos simplesmente $a = 0$. Por outro lado, se $\langle b \rangle \cap A_i \neq \{0\}$, então pela hipótese da indução existe $a \in A_i$ tal que, para $b' = a - b$; $\langle b' \rangle \cap A_i = \{0\}$; claro que $b' \in G - A_{i+1}$. Pela escolha de a_{i+1}, $o(b') \leq o(a_{i+1})$. Se $\langle b' \rangle \cap A_{i+1} = \{0\}$, então "missão cumprida". Caso contrário, escolhemos ℓ mínimo tal que $p^{\ell} b' \in A_{i+1}$. Então,

$$p^{\ell} b' = p^{r} a' + up^{s} a_{i+1}$$

onde $a' \in A_i$, $\ell \leq s \leq r$ e $(u,p) = 1$. Assim,

$$p^{\ell}\left\{(p^{r-\ell} a' + up^{s-\ell} a_{i+1}) - b'\right\} = 0.$$

Sejam $a'' = p^{r-\ell} a' + up^{s-\ell} a_{i+1}$, e

$$b'' = a'' - b' ;$$

então,

$$\langle b'' \rangle \cap A_{i+1} = \{0\} ;$$

com que terminamos a demonstração da proposição e do teorema.

c.q.d.

Teorema 16. Seja G um grupo comutativo finito de ordem m. Seja $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ a fatorização canônica de m em potências de primos $p_1, p_2, \ldots, p_k$. Então existem grupos comutativos G_i $(i = 1, 2, \ldots, k)$ tais que $|G_i| = p_i^{\alpha_i}$ e $G \cong G_1 \times G_2 \times \ldots \times G_k$.

Demonstração. A operação de G será "+". Sejam $a \in G$ e $n = o(a)$. Pelo Teorema de Lagrange, $n = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$ com $0 \leq \gamma_i \leq \alpha_i$ para $i = 1, 2, \ldots, k$. Para cada i, definimos $a_i = \frac{n}{p_i^{\gamma_i}} a$. Então, sem maiores dificuldades, temos

$$o(a_i) = p_i^{\gamma_i}, \quad \langle a_i \rangle \cap \langle a_j \rangle = \{0\} \quad \text{quando} \quad i \neq j,$$

e

$$\langle a \rangle = \langle a_1 \rangle \oplus \langle a_2 \rangle \oplus \ldots \oplus \langle a_k \rangle.$$

Agora definimos para cada i,

$$G_i = \{b \mid b \in G \text{ e } p_i^{\alpha_i} b = 0\}.$$

G_i é um subgrupo de G constituído por elementos de ordem alguma potência de p_i. Por conseguinte, pelo teorema anterior, $|G_i| = p_i^{\delta_i}$ para algum $\delta_i \geq 0$. Também, como $p_i^{\alpha_i} a_i = p_i^{\alpha_i - \gamma_i} na = 0$, $a_i \in G_i$. Assim, em vista do primeiro parágrafo, valem

$$G = G_1 \oplus G_2 \oplus \ldots \oplus G_k$$

e

$$|G| = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}.$$

Finalmente, pela unicidade da fatorização de m, deduzimos que $\delta_i = \alpha_i$ para todo i.

c.q.d.

Corolário 17. Seja $(G,+)$ um grupo comutativo de ordem $m > 1$.

(i) se $m = p$, p primo, então $px = 1$ tem exatamente p soluções em $G \Longleftrightarrow G$ é cíclico.

(ii) G é cíclico $\Longleftrightarrow$ para cada $s|n$, $s > 0$, $sx = 1$ tem exatamente s soluções.

Demonstração. (i) Pelo Teorema 15, deste capítulo,

$$G = \langle a_1 \rangle \oplus \langle a_2 \rangle \oplus \ldots \oplus \langle a_t \rangle ,$$

onde para cada i, $\langle a_i \rangle$ é de ordem p^{β_i}, $\beta_i \neq 0$. As soluções de $px = 1$ em G formam o subgrupo

$$G_o = \langle b_1 \rangle \oplus \langle b_2 \rangle \oplus \ldots \oplus \langle b_t \rangle$$

onde

$$b_i = p^{\beta_i - 1} a_i .$$

Evidentemente G_o é de ordem p^t; daí $|G_o| = p \Longleftrightarrow t = 1$ (isto é, G é cíclico).

(ii) ($\Longleftarrow$) Pelos Teoremas 15 e 16, é suficiente mostrar que cada G_i é cíclio, o que pode ser feito facilmente pondo $s = p_i$ na parte (i).

($\Longrightarrow$) Seja $G = \langle a \rangle$. Então as soluções da equação formam o subgrupo de G

$$\langle \tfrac{n}{s} a \rangle$$

que tem ordem s.

Observação 18. A palavra "exatamente" no corolário pode ser trocada por "no máximo" (verifique!).

Trocando a operação aditiva pela operação multiplicativa o corolário que acabamos de mostrar lê-se assim.

Corolário 19. Seja (G,.) um grupo comutativo de ordem $m > 1$.

(i) Seja $m = p^{\alpha}$, p primo. Então $x^p = 1$ tem exatamente p soluções $\Longleftrightarrow$ G é cíclico.

(ii) G é cíclico $\Longleftrightarrow$ para cada $s|n$, $s > 0$, $x^s = 1$, tem exatamente s soluções.

Definição 20. Seja (G,.) um grupo de ordem $m > 1$, e seja t o menor inteiro positivo tal que

$$x^t = 1$$

está satisfeita para todos os elementos de G. Então t, denotado por e(G), chama-se o expoente de G.

Observação 21. Sabemos que a equação

$$x^{|G|} = 1$$

está satisfeita para todos os elementos do grupo (G,.). Então, pelo algoritmo da divisão,

$$e(G) \Big| |G| \ .$$

Teorema 22. (i) Sejam A e B grupos finitos de ordens relativamente primas, e G o grupo produto cartesiano A × B. Então,

$$e(G) = e(A) \times e(B).$$

(ii) Seja A um grupo de ordem potência de primo. Então, e(A) = a maior ordem de todos os elementos de G.

Demonstração. Exercício 9, IV.

Juntando as duas partes do teorema enunciado acima torna-se possível calcular e(G) para qualquer grupo comutativo finito; por exemplo, para $G = C(2) \times C(2^2) \times C(5) \times C(7) \times C(7^3)$, $e(G) = 2^2.5.7^3$.

4.3.4. $U(p^\alpha)$

Sejam p um primo e α um inteiro ≥ 1.

Teorema 23. (i) p ímpar $\Longrightarrow U(p^\alpha) \cong C(p-1) \times C(p^{\alpha-1})$

(ii) $$U(2^\alpha) \cong \begin{cases} C(1) & \text{se } \alpha = 1 \\ C(2) & \text{se } \alpha = 2 \\ C(2) \times C(2^{\alpha-2}) & \text{se } \alpha > 2 \end{cases}$$

Aplicação 24. Esclarecemos aqui o mistério do Exemplo (iii), III-14, onde m = 561 (composto) e $a^{m-1} \equiv 1 \pmod m$ para todo a que é primo com m.

Como $m = 561 = 3.11.17$,

$$U(m) \cong U(3) \times U(11) \times U(17)$$

$$\cong C(2) \times C(10) \times C(16)$$

$$\cong C(2) \times C(2) \times C(5) \times C(16) ;$$

portanto, o expoente de $U(m)$ é $5.16 = 80$. Logo,

$$a^{80} \equiv 1 \pmod{561} .$$

para qualquer inteiro a que é primo com 561. Dado o fato que 560 é um múltiplo de 80, naturalmente obtem-se

$$a^{560} \equiv 1 \pmod{561}$$

para todo a tal que $(a,561) = 1$.

A demonstração do teorema será parcelada em vários lemas.

Lema 25. $U(p) \cong C(p - 1)$.

Demonstração. Z_p é um corpo; pois $Z_p = U(p) \cup \{0\}$. Seja $p(x) = x^{p-1} - 1$. $p(x) = 0$ possui no máximo $p-1$ soluções em Z_p. Todas elas existem em Z_p, formam o grupo $U(p)$, e são distintas.

Seja t um inteiro positivo divisor de $p - 1$; então $x^t - 1 | x^{p-1} - 1$. Por conseguinte, $x^t = 1$ tem exatamente t soluções em $U(p)$. Ora, essa é a condição estipulada no Co

rolário 17 para que $U(p)$ seja um grupo cíclico.

c.q.d.

Lema 26. As soluções de $x^{p-1} = 1$ em $U(p^\alpha)$ formam um grupo cíclico de ordem $p - 1$.

Demonstração. $U(p^\alpha)$ tem ordem $(p-1)p^{\alpha-1}$; portanto, $U(p^\alpha) \cong U_1 \times U_2$, onde $|U_1| = p - 1$ e $|U_2| = p^\alpha$.

$x^{p-1} = 1$ tem $p - 1$ soluções em $U(p^\alpha)$. Precisamos mostrar que para cada $s > 0$ com $s|p-1$,

$$x^s = 1$$

tem no máximo s soluções em $U(p^\alpha)$.

Seja a um inteiro tal que $a^s \equiv 1 \pmod{p^\alpha}$; então, $a^s \equiv 1 \pmod{p}$. Usando o lema anterior, é suficiente mostrar que duas soluções a, b não congruentes de $x^s \equiv 1 \pmod{p}$, são não congruentes módulo p. Mostraremos o contra-positivo. Sejam a, b inteiros tais que

$$a = b + \ell p^\beta$$

com $(\ell,p) = 1$ e $1 \leq \beta \leq \alpha$, e tais que

$$a^s \equiv b^s \equiv 1 \pmod{p^\alpha},$$

Usando a expansão binomial,

$$a^s = (b + \ell p^\beta)^s = b^s + t.b^{s-1}(\ell p^\beta) + \ldots + t.b(\ell p^\beta)^{s-1} + (\ell p^\beta)^s.$$

Consideremos esta igualdade módulo p^{α}; visto que $a^s \equiv b^s$ (mod. p^{α}), temos,

$$0 \equiv s.b^{s-1}(\ell p^{\beta}) + \ldots + (\ell p^{\beta})^s \pmod{p^{\alpha}} .$$

Ao "dividir" esta congruência por p^{β}, obtemos

$$s.b^{s-1} + \binom{s}{2} b^{s-2}\ell^2 p^{\beta} + \ldots + \ell^s p^{\beta(s-1)} \equiv 0 \pmod{p^{\alpha-\beta}} .$$

A hipótese $\alpha \neq \beta$ nos levará ao absurdo $p \mid s\, b^{s-1}$. Portanto, $\alpha = \beta$.

c.q.d.

Lema 27. (i) Sejam p ímpar, e $a = 1 + p$. Então, para todo $\beta \geq 1$,

$$a^{p^{\beta-1}} = 1 + tp^{\beta}$$

com $(t,p) = 1$.

(ii) Sejam $p = 2$ e $a = 5$ $(= 1 + p^2)$. Então, para todo $\beta \geq 2$,

$$a^{2^{\beta-2}} = 1 + t2^{\beta}$$

com $(t,2) = 1$.

Demonstração. (i) Procederemos por indução sobre β.

O caso $\beta = 1$ é evidentemente válido. Suponhamos

que $\beta > 1$ e

$$a^{p^{\beta-1}} = 1 + tp^{\beta}$$

com $(t,p) = 1$. Então,

$$a^{p^{\beta}} = (1 + tp^{\beta})^{p}$$

$$= 1 + \binom{p}{1}tp^{\beta} + \binom{p}{2}(tp^{\beta})^{2} + \ldots + (tp^{\beta})^{p}$$

$$= 1 + \left(t + \binom{p}{2}t^{2}p^{2\beta-\beta-1} + \binom{p}{3}t^{3}p^{3\beta-\beta-1} + \ldots\right)p^{\beta+1}$$

Os termos, dentro do parenteses, do terceiro em diante são todos múltiplos de p. O segundo termo $\binom{p}{2}t^{2}p^{\beta-1}$ pode deixar de sê-lo somente para $\beta = 1$ e $p = 2$. Portanto, a expressão dentro do parenteses é primo com p.

(ii) Exercício 11, IV.

Corolário 28. Mantendo a notação do lema anterior em cada uma das suas partes, temos,

(i) $o(\bar{a})$ em $U(p^{\beta})$ é $p^{\beta-1}$,

(ii) $o(\bar{a})$ em $U(2^{\beta})$ é $2^{\beta-2}$.

Demonstração. Exercício 12, IV.

Chamamos a atenção do leitor para o fato de que a parte "p ímpar" do teorema está feita. Falta-nos considerar o caso $p = 2$.

Para $p = 2$ e $\alpha \leq 2$ as afirmações do teorema podem ser verificadas diretamente. Quando $\alpha > 2$, $\overline{s}$ tem ordem $2^{\alpha-2}$ em $U(2^{\alpha})$, logo precisamos apenas de encontrar um elemento de ordem dois fora de $\langle\overline{s}\rangle$, e daí o isomorfismo $U(2^{\alpha}) \cong C(2) \times C(2^{\alpha-2})$ será estabelecido.

Lema 29. Seja $\beta > 2$. Então

(i) $\overline{-1}$ é de ordem dois em $U(2^{\beta})$,

(ii) $5^{i} \not\equiv -1 \pmod{2^{\beta}}$, para nenhum inteiro $i \geq 0$.

Demonstração. (i) (esta parte é evidente).

(ii) Suponhamos que

$$5^{i} \equiv -1 \pmod{2^{\beta}},$$

para algum inteiro $i \geq 0$. Então

$$5^{i} \equiv -1 \pmod{4} ;$$

porque $4 \mid 2^{\beta}$. Mas,

$$5 \equiv 1 \pmod{4}$$

e

$$5^{i} \equiv 1 \pmod{4} ;$$

como $1 \not\equiv -1 \pmod{4}$, chegamos a uma contradição.

c.q.d.

Em síntese, o teorema está demonstrado.

4.4. A expansão decimal de $\frac{m}{n}$

Sejam m, n inteiros positivos com $m < n$ e $(m,n) = 1$.

Aplicaremos nesta secção resultados sobre congruências para analisar as regularidades que aparecem na expansão decimal de $\frac{m}{n}$. Diz-se que parte das investigações aritméticas de Gauss baseou-se neste problema.

Daremos primeiro alguns exemplos.

$$\frac{1}{2} = 0,5\overline{0}\ , \quad \frac{1}{3} = 0,\overline{3}\ , \quad \frac{2}{3} = 0,\overline{6}, \quad \frac{1}{4} = 0,25\overline{0},$$

$$\frac{1}{5} = 0,2\overline{0}\ , \quad \frac{2}{5} = 0,4\overline{0}, \quad \frac{3}{5} = 0,6\overline{0}, \quad \frac{4}{5} = 0,8\overline{0}\ ,$$

$$\frac{1}{6} = 0,1\overline{6}\ , \quad \frac{5}{6} = 0,8\overline{3}, \quad \frac{1}{7} = 0,\overline{142857}\ ,$$

$$\frac{2}{7} = 0,\overline{285714}, \quad \frac{3}{7} = 0,\overline{428571}, \quad \frac{4}{7} = 0,\overline{571428}$$

$$\frac{5}{7} = 0,\overline{714285}\ , \qquad \frac{6}{7} = 0,\overline{857142}\ .$$

Neste cálculo, o símbolo $\overline{i}$ indica uma repetição sucessiva do ciclo i.

A nossa primeira observação, que é bem conhecida, é que todas as representações terminam com $\overline{i}$ (quer dizer , tornam-se periódicas); reciprocamente, um número cuja representação decimal é eventualmente periódica é racional (Exercício 17, IV.

A periodicidade explica-se pelo fato que no processo de expansão, a divisão aplica-se um número ilimitado de vezes, produzindo sempre restos pertencentes ao conjunto finito 0, 1, 2, ..., n, e portanto necessariamente um deles reaparece; consequentemente, o processo da divisão reproduz os quocientes conseguidos inicialmente e com a mesma ordem .

Os restos encontrados no processo da expansão de $\frac{m}{n}$ são simplesmente os valores não negativos mínimos de

$$m,\ 10m,\ 10^2.m,\ \ldots,\ 10^k.m \pmod{n} \ .$$

Algumas expansões, como no caso de $n = 3, 7$ são puramente periódicas. Outras como nos casos $n = 2, 4, 5, 6$ são eventualmente periódicas.

Se $n = 2^a5^b$ e $c = \max\{a,b\}$, então $10^c \equiv 0 \pmod{n}$, e a representação dará zeros a partir da c-ésima posição ; isto ocorre nos casos $n = 2, 4, 5$.

Se $(n,10) = 1$, então 10 é inversível módulo n. Seja k a ordem de $\overline{10}$ em U(n); então $10^k \equiv 1 \pmod{n}$ e donde concluímos que a expansão de $\frac{m}{n}$ é puramente periódica de período k; nota-se que o período k é independente de m.

Para a situação mista $n = 2^a5^bq$ com $(q,10) = 1$, colocamos $c = \max\{a,b\}$ e concluímos

$$10^c = 2\ 5\ d\ , \quad \frac{10^c}{n} = \frac{d}{q} \quad \text{com} \quad (d,q) = 1 \ ;$$

então a partir do c-ésimo lugar, começam os algarismos da expansão de $\frac{d}{q}$.

Acabamos de demonstrar o

Teorema 30. Seja $\frac{m}{n}$ um número racional tal que $m < n$, $(m,n) = 1$ e seja $n = 2^a 5^b q$ com $(q,10) = 1$. Então a expansão decimal de $\frac{m}{n}$ é da forma

$$0.,\ a_1 a_2 \ldots a_c \overline{b_1 b_2 \ \ldots \ b_k}$$

onde $c = \max\{a,b\}$ e k = ordem de 10 módulo q.

O caso $n = 7$, chama a nossa atenção: o ciclo de $\frac{m}{7}$ é uma permutação cíclica do ciclo de $\frac{1}{7}$.

Acontece que $\overline{10}$ é um gerador do grupo $U(7)$: $10^0 \equiv 1$, $10^1 \equiv 3$, $10^2 \equiv 30 \equiv 2$, $10^3 \equiv 20 \equiv 6$, $10^4 \equiv 60 \equiv 4$, $10^5 \equiv 40 \equiv 5$, $10^6 \equiv 50 \equiv 1 \pmod 7$; assim,

$$m \equiv 10^j \pmod 7 \quad \text{para algum } j$$

e

$$10^i m \equiv 10^{i+j} \pmod 7 ,$$

e portanto, o ciclo de $\frac{m}{7}$ consegue-se dando um salto sobre os j primeiros lugares no ciclo de $\frac{1}{7}$. Por exemplo, para $m = 2$, $2 \equiv 10^2 \pmod 7$,

o ciclo de $\frac{1}{7}$ é 142857 e

o ciclo de $\frac{2}{7}$ é 285714

Empregamos os mesmos argumentos para demonstrar um resultado geral.

Teorema 31. Sejam $(n,10) = 1$, $\frac{1}{n} = 0,\overline{a_1 a_2 \cdots a_k}$, e $r_1, \ldots, r_k$ os restos ordenados na mesma ordem como eles aparecem no processo da expansão de $\frac{1}{n}$. Então

$$\frac{r_i}{n} = 0,a_{i+1}a_{i+2}\cdots a_k a_1 a_2 \cdots a_i \; .$$

4.5. O Problema dos Elementos Primitivos

Gauss se interessou no problema dos primos p para os quais 10 é uma raiz primitiva da unidade módulo p; quer dizer, $\overline{10}$ é um gerador de $U(p)$. Ele chegou a convicção de que o número destes primos é infinito.

Eis os primeiros dez destes primos,

7, 17, 19, 23, 29, 47, 59, 61, 97, 109 .

Emil Artin (1898-1962) deu em 1927, argumentos probabilísticos para justificar a

Conjectura 32. Seja a um inteiro diferente de -1 e não quadrado. Então o número dos primos para os quais a é uma raiz primitiva da unidade módulo p é infinito.

Foi demonstrado por C. Hooley em 1967 que a conjectura de Artin é verdadeira dada a veracidade de uma outra chamada pela Hipótese de Riemann (data-se desde 1860 e originou com uma tentativa de Riemann para demonstrar o Teorema do Número Primo; considerada um dos problemas mais importantes da matemática contemporânea).

4.6. Infinitude dos primos da forma an + 1

Mostraremos nesta secção, com métodos algébricos a nosso dispor, um caso particular do Teorema de Dirichlet.

Teorema 33. Seja a um inteiro positivo. Então a progressão $\{an + 1 | n \in Z\}$ contém um número infinito de primos.

Dividiremos a demonstração em vários passos.

1. Dado $f(x) \in Z[x]$ não constante, existem infinitos primos p para os quais $f(x) \equiv 0 \pmod{p}$ tem uma solução.

Demonstração. Seja $f(x) = a_o + a_1x + \ldots + a_tx^t$. Se $a_o = 0$, então $f(0) = 0 \equiv 0 \pmod{p}$, para qualquer primo p. Suponhamos que $a_o \neq 0$ e que $f(x) \equiv 0 \pmod{p}$ tenha soluções para os primos $p_1, p_2, \ldots, p_k$ (entre esses encontram-se certamente os primos fatores de a_o). Daremos a

seguir um método para aumentar o conjunto destes primos.

Seja $x' = a_o p_1 p_2 \cdots p_k x$; então,

$$f(x') = a_o + a_1 a_o p_1 p_2 \cdots p_k x + \cdots + a_k (a_o p_1 p_2 \cdots p_k x)^t$$

$$= a_o (1 + b_1 x + \cdots + b_t x^t) = a_o g(x) \quad .$$

Tendo em vista que $g(x)$ não é constante, existe um inteiro x_o tal que $y_o = g(x_o) \neq \pm 1$. Como $g(0) = 1$ e $p_1 p_2 \cdots p_k \mid b_i$ para $1 \leq i \leq t$, resulta que $(p_1 p_2 \cdots p_k, y_o) = 1$; assim, para qualquer primo q divisor de y_o ,

$$f(y_o) \equiv 0 \pmod{q} \quad \text{e claro,} \quad q \neq p_i \qquad 1 \leq i \leq k.$$

2. Seja a como no teorema e seja $A(x) = x^a - 1$. Então por 1., existem infinitos primos p para os quais $A(x) \equiv 0$, ou seja $x^a \equiv 1 \pmod{p}$ tem solução. Seja $x_o^a \equiv 1 \pmod{p}$ para um inteiro x_o e um primo p e seja também $b = o(\overline{x_o})$ em $U(p)$. Então, pelos Teoremas de Fermat e de Lagrange, $b \mid p-1$ e $p = bn + 1$ para algum inteiro n . Tendo em vista que $b \mid a$, seria interessante reduzir o polinômio $A(x)$ para um outro que não admita soluções com ordens $< a$, módulo p.

3. $A(x) = 0$ tem soluções distintas em $\mathbb{C}$. Elas são

$$1, \; e^{\frac{2\pi i}{a}}, \; \ldots, \; e^{j\frac{2\pi i}{a}}, \; \ldots, \; e^{(a-1)\frac{2\pi i}{a}},$$

que formam um grupo cíclico multiplicativo de ordem a (lembramos que $i = \sqrt{-1}$ e $e^{i\theta} = \cos\theta + i\,\mathrm{sen}\theta$ para qualquer θ número real).

Um elemento $e^{j\frac{2\pi i}{a}}$ que tem ordem a (isto acontece quando $(j,a) = 1$) será chamado uma raiz a-ésima primitiva da unidade.

4. Seja $\psi(x) = \text{m.m.c.}\{x^b - 1 \mid 0 < b < a \text{ e } b|a\}$ em $Q[x]$. Dados os fatos,

$$x^b - 1 | A(x)$$

e

$$e^{b\frac{2\pi i}{a}} \neq 1 \ ,$$

quando $b|a$ e $b > 0$, obtem-se evidentemente que

$$\psi(x)|A(x) \quad \text{e} \quad \psi(x) \neq A(x).$$

Seja $\xi(x) \in Q[x]$ tal que $A(x) = \psi(x)\xi(x)$. As raízes de $\xi(x)$ em $\mathbb{C}$ são justamente as raízes a-ésimas primitivas da unidade. Este é um fato em $\mathbb{C}$ e, para certos primos p, pode deixar de sê-lo em U(p).

5. $\psi(x)$ e $\xi(x)$ são primos entre si em $\mathbb{C}[x]$ e logo também em $Q[x]$. Por , existem $\alpha(x)$, $\beta(x) \in Q[x]$ tais que

$$\alpha(x)\psi(x) + \beta(x)\xi(x) = 1 \ .$$

Precisamos transformar $\alpha(x)$, $\beta(x)$, $\xi(x)$ em polinômios com coeficientes inteiros ($\xi(x)$, realmente, é um elemento de $Z[x]$, mas para efeito deste argumento podemos viver com menos). Existem a, b, c inteiros positivos tais que $a\alpha(x)$, $b\beta(x)$, $c\xi(x) \in Z[x]$. Sejam $d = abc$, $\alpha_1(x) = d\alpha(x)$, $\beta_1(x) = ab\beta(x)$, $\xi_1(x) = c\xi(x)$. Então,

$$\alpha_1(x)\psi(x) + \beta_1(x)\xi_1(x) = d .$$

6. Sejam $\pi(a)$: o conjunto dos primos para os quais $\xi_1(x) \equiv 0 \pmod{p}$ tem soluções, δ: os primos divisores de d. Então obviamente, $\pi(a) - \delta$ é infinito.

Seja $p \in \pi(a) - \delta$, e seja x_o um inteiro tal que $\xi_1(x_o) \equiv 0 \pmod{p}$. Verificaremos que $o(\overline{x_o}) = a$ em $U(p)$. Tendo em vista que $\xi_1(x) | dA(x)$,

$$dA(x_o) \equiv 0 , \quad A(x_o) \equiv 0 \quad e \quad x_o^a \equiv 1$$

são válidas módulo p. Suponhamos por absurdo que $o(\overline{x_o}) = b$ com $b < a$. Então,

$$x_o^b \equiv 1 , \quad x_o^b - 1 \equiv 0 \quad e \quad \psi(x_o) \equiv 0$$

módulo p. Daí, obtemos que

$$d = \alpha_1(x_o)\psi(x_o) + \beta_1(x_o)\xi_1(x_o) \equiv 0 \pmod{p};$$

um absurdo, pois $p \nmid d$.

c.q.d.

4.7. EXERCÍCIOS

1. Sejam $D = Z[\sqrt{2}]$ e $I = \{2a + b\sqrt{2} \mid a, b \in Z\}$. Mostre que $\frac{D}{I} \cong Z_2$.

2. Demonstrar o Corolário 2, IV.

3. Demonstrar o Corolário 3, IV.

4. Sejam A e B aneis. Seja $C = A \times B$ o anel com as operações definidas por

$$(a,b) + (a',b') = (a+a', b+b')$$

$$(a,b).(a',b') = (aa', bb').$$

Mostre que $A' = \{(a,0) \mid a \in A\}$ é um ideal em C.

5. Sejam A e B ideais $\neq \{0\}$ de Z_{15} tais que

$$Z_{15} = A \oplus B .$$

Mostre que $A \cong Z_3$ e $B \cong Z_5$ ou vice versa.

6. Demonstre que a função σ definida no Teorema 10, IV, é um isomorfismo.

7. Seja (G, +) um grupo comutativo. Sejam A, B subgrupos cíclicos de G tais que

$$G = A \oplus B \quad \text{com} \quad o(A) = n, \quad o(B) = m .$$

Mostre que G é cíclico se e somente se $(n,m) = 1$.

8. Verifique a afirmação da Observação 21, IV.

9. Demonstre o Teorema 22, IV.

10. Seja m um número natural composto tal que

$$a^{m-1} \equiv 1 \pmod{m}$$

para todo inteiro a que é primo com m. Mostre que

(i) m é ímpar, sem fatores quadrados $\neq 1$.

(ii) m é divisível por pelo menos três primos distintos.

11. Demonstre (ii) do Lema 27 , IV.

12. Demonstrar Corolário 28, IV.

13. Demonstre: $U(m)$ é cíclico se e somente se $m = 2$, 4, p^{α} ou $2p^{\alpha}$, onde p é um primo ímpar.

14. Mostrar que $a^{84} \equiv 1 \pmod{735}$ para todo inteiro a que é primo com 735.

15. Quantas soluções não congruentes tem a congruência

$$x^6 \equiv 1 \pmod{735}?$$

16. Pesquisar a questão: "Quantas soluções não congruentes tem

$$x^n \equiv 1 \pmod{m}?"$$

17. Demonstre que um número cuja representação decimal é eventualmente periódica é racional.

18. Mostrar que

(i) 10 é uma raiz primitiva módulo 17,

(ii) o ciclo de $\frac{1}{17}$ é 0588235294117647,

(iii) o ciclo de $\frac{4}{17}$ é 2352941176470588.

19. Sejam a, b números naturais primos entre si. Mostre que $\{an + b | n = 0, 1, 2, \ldots\}$ contem um número infinito de elementos que são mutuamente primos entre si.

20. Demonstrar que $\{an + 1 | n = 0, 1, 2, \ldots\}$ contem um número infinito de elementos fatoráveis em exatamente s primos distintos, qualquer que seja o número natural s.

CAPÍTULO V

RECIPROCIDADE QUADRÁTICA

5.1. Resíduos Quadráticos

Sejam $f(x) = ax^2 + bx + c$ um polinômio com coeficientes inteiros de grau dois e p um primo que não divide a. Foi demonstrado em 4.2.3 a redução de $f(x) \equiv 0 \pmod{p}$ para $y^2 \equiv \Delta \pmod{p}$, onde $\Delta = b^2 - 4ac$.

O propósito deste capítulo é de derivar a lei de reciprocidade quadrática com que poderemos decidir rapidamente quando $x^2 \equiv a \pmod{p}$ (dito de uma outra forma, quando $x^2 - a$ se fatoriza em fatores de grau um módulo p) é solúvel, para qualquer inteiro a e qualquer primo p. Se a congruência tem solução então dizemos que a é um *resíduo quadrático* módulo p; caso contrário, dizemos que a é um *resíduo não quadrático* módulo p. As mesmas definições fazem-se ao trocar p por um inteiro $m > 0$.

Exemplo 1. Sejam $p = 7$ e $S = \{0, \pm 1, \pm 2, \pm 3\}$. Os resíduos quadráticos módulo 7 são

$$0,\ 1,\ 4\ (\equiv -3),\ 9\ (\equiv 2)\ ,$$

e os resíduos não quadráticos são

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

A reciprocidade quadrática enquadra-se dentro do se

guinte problema geral: dado $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_o \in Z[x]$ irredutível, descrever os primos p para os quais $f(x)$ decompõe-se em fatores de grau um módulo p. Este problema foi resolvido para uma classe de polinômios chamados abelianos, onde a lei conhece-se por a Lei de Reciprocidade de Artin.

Como $x^2 \equiv x \pmod 2$ nossas considerações têm substância não trivial somente para p, primo ímpar. Para o resto do capítulo p significará um primo ímpar.

Seja $U = U(p)$. Lembramos que U é um grupo cíclico de ordem $p - 1$. Seja g um gerador de U. Então,

$$U^2 = \{\bar{a}^2 | \bar{a} \in U\} = \langle g^2 \rangle$$

é um subgrupo de U de ordem $\frac{p-1}{2}$. U^2 consiste de todas as classes representadas por resíduos quadráticos módulo p; em outras palavras, para $(b,p) = 1$,

$$b \text{ é quadrático módulo } p \iff b^2 \in U^2 .$$

Pelo Teorema de Lagrange, $[U:U^2] = 2$ e daí U é a união de duas classes laterais. Seja $\bar{h} \in U - U^2$; então

$$U = U^2 \cup U^2 \bar{h} .$$

$U^2\bar{h}$ consiste de todas as classes representadas por resíduos não quadráticos módulo p.

Observamos que o produto de um elemento de U^2 com um elemento de $U^2\bar{h}$ é um elemento de $U^2\bar{h}$, e que o produto

de dois elementos quaisquer de $U^2\bar{h}$ pertence a U^2.

Teorema 2. Seja a um inteiro não divisível por p. Então,

(i) $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$

(ii) a é resíduo quadrático módulo $p \iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$,

(iii) a é resíduo não quadrático módulo $p \iff a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Demonstração. (i) As soluções de $x^2 \equiv 1 \pmod{p}$ são $x \equiv \pm 1 \pmod{p}$. Tendo em vista que

$$(a^{\frac{p-1}{2}})^2 = a^{p-1} \equiv 1 \pmod{p},$$

segue que

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}.$$

(ii) Se a é resíduo quadrático, então $\bar{a} \in U^2$ e assim $\bar{a}^{(p-1)/2} = \bar{1}$. Por outro lado, se $a^{(p-1)/2} \equiv 1 \pmod{p}$, então $o(\bar{a}) \mid \frac{p-1}{2}$; o fato de que U é cíclico implica que $\bar{a} \in \langle g^2 \rangle = U^2$.

(iii) A demonstração desta parte faz-se juntando as partes (i) e (ii).

c.q.d.

Exemplo 3. Verificaremos que a = 3 é um resíduo não quadrático módulo 7, mas é resíduo quadrático módulo 11.

$$3^{\frac{7-1}{2}} = 27 \equiv -1 \pmod{7}$$

$$3^{\frac{11-1}{2}} = 3^5 = 3^3.3^2 \equiv 5(-2) \equiv 1 \pmod{11}\ .$$

Seja $T = U^{\frac{p-1}{2}} = \{\overline{-1}, \overline{1}\}$. T é um subgrupo de U de ordem dois. O teorema anterior mostra que a função $\lambda: U \to T$ definida por $\lambda(\overline{a}) = \overline{a}^{(p-1)/2}$ leva U^2 sobre $\overline{1}$ e $U^2\overline{h}$ sobre $\overline{-1}$. Como $(\overline{ab})^{(p-1)/2} = \overline{a}^{(p-1)/2}\,\overline{b}^{(p-1)/2}$, λ é um homomorfismo de U sobre T.

Definição 4. Seja (a,p) = 1. Definimos o símbolo de Legendre por

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{se a é um resíduo quadrático módulo p} \\ -1 & \text{se a é um resíduo não quadrático módulo p.} \end{cases}$$

Notamos que um inteiro a é resíduo quadrático módulo p, se p|a ou $\left(\frac{a}{p}\right) = 1$.

No teorema seguinte colocamos as várias propriedades de resíduos quadrático em termo do símbolo de Legendre.

Teorema 5. Sejam a, b inteiros primos com p. Então,

(i) $a \equiv b \pmod{p} \Longrightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,

(ii) $\left(\frac{a^2}{p}\right) = 1$,

(iii) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$,

(iv) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Demonstração. Exercício 4, V.

5.2. O Lema de Gauss

Seja $(a,p) = 1$. Definimos os seguintes conjuntos:

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

$S = Ba = \{a, 2a, \ldots, \frac{p-1}{2}a\}$;

S_o: os elementos do S.C.R. mínimo M_o que são congruentes com algum ia S,

$S_o = \{s_1, s_2, \ldots, s_k; r_1, r_2, \ldots, r_n\}$

onde

$0 < s_i < \frac{p}{2}$ para $1 \leq i \leq k$,

$\frac{p}{2} < r_i < p$ para $1 \leq i \leq n$,

(observamos que $n = \frac{p-1}{2} - k$),

$S_1 = \{s_1, s_2, \ldots, s_k; p - r_1, p - r_2, \ldots, p - r_n\}$.

Se $A = \{a_1, a_2, \ldots, a_k\}$ é um subconjunto de k inteiros, então ΠA indica $a_1 a_2 \ldots a_k$ e $\sum A$ indica $a_1 + a_2 + \ldots + a_k$.

Teorema 6. (O lema de Gauss)

$$\left(\frac{a}{p}\right) = (-1)^n \quad .$$

Demonstração. $B = S_1$, porque S_1 consiste de $\frac{p-1}{2}$ inteiros positivos distintos todos $\leq \frac{p-1}{2}$.

As seguintes afirmativas são fáceis de provar,

$$\Pi S = a^{\frac{p-1}{2}} \Pi B \quad ,$$

e módulo p,

$$\Pi S_o \equiv \Pi S \quad ,$$

$$\Pi B = \Pi S_1 \equiv (-1)^n \Pi S_o \quad ,$$

$$\Pi S_o \equiv (-1)^n \Pi B \quad ,$$

$$(-1)^n \Pi B \equiv \Pi S_o \equiv \Pi S \equiv a^{\frac{p-1}{2}} \Pi B \quad .$$

Tendo em vista os dois extremos da última congruência e como $(\Pi B, p) = 1$, obtemos que

$$a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p} \; ;$$

logo,

$$\left(\frac{a}{p}\right) = (-1)^n$$

c.q.d.

Exemplo 7. Sejam $p = 17$, $a = 5$. Então,

$$B = \{1, 2, 3, 4, 5, 6, 7, 8\} ,$$

$$S = Ba = \{5, 10, 15, 20, 25, 30, 35, 40\} ,$$

$$S_o = \{5, 10, 15, 3, 8, 13, 1, 6\}$$

$$= \{1, 3, 5, 6, 8; 10, 13, 15\} .$$

Assim obtemos $n = 3$ e daí $(\frac{5}{17}) = (-1)^3 = -1$; ou seja, 5 é uma raiz não quadrática módulo 17.

O teorema anterior foi conseguido através de aplicar Π ao conjunto Ba. Desta vez consideraremos a aplicação de $\sum$ ao mesmo conjunto.

Teorema 8. (i) Seja $(a,2p) = 1$ e $t = \sum_{1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right]$. (encontra-se uma interpretação geométrica de t na secção seguinte). Então,

$$\left[\frac{a}{p}\right] = (-1)^t .$$

(ii) $$(\frac{2}{p}) = (-1)^{(p^2-1)/8} .$$

Demonstração. $\sum B$ é uma progressão aritmética e portanto,

$$\sum B = \frac{1}{2} \frac{p-1}{2}(\frac{p-1}{2} + 1) = \frac{p^2-1}{8} . \qquad (1)$$

$$\sum S = \sum_{j=1}^{\frac{p-1}{2}} ja = a\sum B . \qquad (2)$$

De outro modo, como $ja = \left[\frac{ja}{p}\right]p + \rho_a(j)$ com $0 \leq \rho_a(j) < p$,

$$\sum S = \sum_{j=1}^{\frac{p-1}{2}} \left(\left[\frac{ja}{p}\right]p + \rho_a(j) \right)$$

$$= \left(\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] \right) p + \sum_{j=1}^{\frac{p-1}{2}} \rho_a(j) \quad . \tag{3}$$

Tendo em vista que $\rho_a(j) \equiv ja \pmod{p}$, obtemos,

$$\sum_{j=1}^{\frac{p-1}{2}} \rho_a(j) = \sum S_o = \sum_{i=1}^{k} s_i + \sum_{i=1}^{n} r_i \quad , \tag{4}$$

Encorporamos (4) em (3),

$$\sum S = tp + \sum_{i=1}^{k} s_i + \sum_{i=1}^{n} r_i \tag{5}$$

$$\begin{aligned} \sum S_1 &= \sum_{i=1}^{k} s_i + \sum_{i=1}^{n} p - r_i \\ &= \sum_{i=1}^{k} s_i + np - \sum_{i=1}^{n} r_i \quad . \end{aligned} \tag{6}$$

Lembramos que $B = S_1$; assim por (6),

$$\sum B = \sum_{i=1}^{k} s_i + np - \sum_{i=1}^{n} r_i \quad . \tag{7}$$

De (2) e (5) resulta,

$$a\sum B = tp + \sum_{i=1}^{k} s_i + \sum_{i=1}^{n} r_i \quad . \tag{8}$$

Subtraindo (7) de (8), obtemos que

$$(a - 1)\sum B = (t - n)p + 2\sum_{i=1}^{n} r_i \cdot \qquad (9)$$

A equação (9) módulo 2, lê-se ,

$$0 \equiv (t - n)+0 \pmod 2$$

se a é ímpar; ou seja

$$a \text{ ímpar} \Longrightarrow t \equiv n \pmod 2$$

e

$$\left(\frac{a}{p}\right) = (-1)^n = (-1)^t.$$

Quando a = 2, a equação (9) lê-se como

$$\sum B = (t - n)p + 2\sum_{i=1}^{n} r_i \ ;$$

como $\left[\frac{ja}{p}\right] = \left[\frac{2j}{p}\right] < p$ para $1 \leq j \leq \frac{p - 1}{2}$, tem-se t = 0 e portanto,

$$\sum B = -np + 2\sum_{i=1}^{n} r_i$$

e

$$\sum B \equiv n \pmod 2 \qquad (10).$$

Assim por (1),

$$n \equiv \frac{p^2 - 1}{8}$$

ou seja,

$$(\frac{2}{p}) = (-1)^{\frac{p^2 - 1}{8}} .$$

c.q.d.

Exemplo 9. Sejam $p = 17$, $a = 3$, $b = 6$. Então,

$$\frac{p - 1}{2} = 8, \quad \frac{p^2 - 1}{8} = 18, \quad \left[\frac{ja}{p}\right] = 0 \quad \text{se} \quad 0 \leq j \leq 5 ,$$

e

$$t = \left[\frac{18}{17}\right] + \left[\frac{20}{17}\right] + \left[\frac{24}{17}\right] = 3 .$$

Assim temos,

$$(\frac{3}{17}) = (-1)^t = 1$$

$$(\frac{6}{17}) = (\frac{2}{17})(\frac{3}{17}) = (-1)^{18}(-1)^3 = -1 .$$

Corolário 10. (i) $(\frac{2}{p}) = 1 \Longleftrightarrow$ p é da forma 8k+1 ou 8k - 1.

(ii) $x^2 \equiv 2 \pmod{m}$ tem soluções $\Longleftrightarrow$ $4 \nmid m$ e se $p|m$, p: ímpar, então $p = 8k + 1$ ou $8k - 1$.

Demonstração. (i) Pelo teorema anterior,

$$(\frac{2}{p}) = 1 \Longleftrightarrow \frac{p^2 - 1}{8} \text{ é par}$$

$$\Longleftrightarrow p^2 \equiv 1 \pmod{16} .$$

De antemão, p tem uma das formas $4h + 1$, $4h - 1$. Se

$p = 4h + 1$, então $p^2 = 16h^2 + 8h + 1 \equiv 8h + 1 \pmod{16}$; daí para $p = 4h + 1$,

$$p^2 \equiv 1 \pmod{16} \iff 2 \mid h$$

$$\iff p \text{ é da forma } 8k+1.$$

O argumento para o caso $p = 4h - 1$ é inteiramente semelhante ao caso anterior.

(ii) (Exercício 8, V).

c.q.d.

Corolário 11. (i) $(\frac{-2}{p}) = 1 \iff p$ é da forma $8k+1$ ou $8k + 3$.

(ii) $x^2 \equiv -2 \pmod{m}$ tem solução $\iff$

$4 \nmid m$ e se $p \mid m$, p: ímpar, então $p = 8k+1$ ou $8k + 3$.

Demonstração. $(\frac{-2}{p}) = (\frac{-1}{p})(\frac{2}{p}) = (-1)^{\frac{p-1}{2}} (-1)^{\frac{p^2-1}{8}}$. Logo,

$$(\frac{-2}{p}) = 1 \iff \frac{p-1}{2} + \frac{p^2-1}{8} \text{ é par}$$

$$\iff p^2 + 4p - 5 \equiv 0 \pmod{16} .$$

Para completar, repetimos o método do corolário anterior.

c.q.d.

Os corolários acima enunciados foram conhecidos por Fermat. Ele não deu as demonstrações, embora tenha afirmado que as obteve. Depois, Euler procurou-as sem êxito, e foi Lagrange quem publicou as primeiras demonstrações rigorosas.

5.3. O Teorema da Reciprocidade Quadrática

Teorema 12. Sejam p e q primos distintos. Então,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} ;$$

uma outra forma é

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

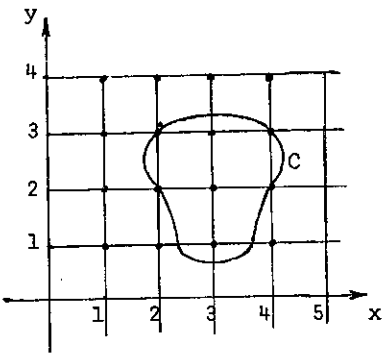
Nota Histórica 13. A primeira demonstração deste teorema foi dada por Gauss e encontra-se no seu livro Disquisitiones Arithmeticae onde menciona-se que Euler conhecia o resultado em 1775 e que Legendre publicou uma demonstração deficiente (minuciosamente analisada com certo humor nas seções 151, 296, 297 de Disq. Arith.) em 1785.

Contam que Gauss encontrou 8 demonstrações diferentes e que existem atualmente não menos que 152 delas!

Apresentaremos uma demonstração que é essencialmente de Eisenstein (aluno brilhante de Gauss, morreu aos 29 anos de idade). Primeiro vamos introduzir umas noções geométricas.

Seja $\mathcal{L} = \{(a,b) \mid a,b \in N\}$.

será considerado como um subconjunto do plano $\mathbb{R}^2$. Para efeito desta secção, nos convém adotar a seguinte notação:



seja C uma curva fechada (triângulo, retângulo, etc.) no plano, então

$\nu(C)$ = o número dos pontos de $\mathcal{L}$ dentro e sobre a borda de C.

Lema 14. Seja T o triângulo definido (ou ladeado) por $y = 0$, $y = bx$, $x = c$, onde b e c são reais positivos. Então

$$\nu(T) = \sum_{j=1}^{[c]} [bj] \quad ,$$

j sendo uma variável com valores inteiros.

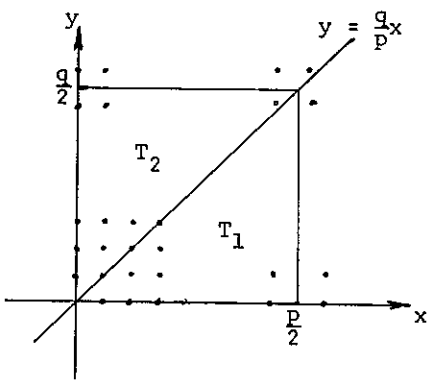
Demonstração. Os pontos de $\mathcal{L}$ que estão no triângulo T se encontram sobre as retas $x = 1, 2, \ldots, [c]$. Cada segmento de $x = j$ no triângulo T contém $[bj]$ pontos de $\mathcal{L}$. Então

$$\nu(T) = \sum_{j=1}^{[c]} [bj] \ .$$

c.q.d.

Pelo que acabamos de mostrar, podemos interpretar $t = \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right]$ do Teorema 8, como sendo $\nu(T)$, onde T é o triângulo definido por $y = 0$, $y = \frac{a}{p}x$, $x = \frac{p}{2}$.

Demonstração do Teorema 12. Seja Q o retângulo ladeado por $x = 0$, $x = \frac{p}{2}$, $y = 0$, $y = \frac{q}{2}$. Então existem $\frac{p-1}{2}$ e $\frac{q-1}{2}$ inteiros positivos sobre os lados $x = 0$, $y = 0$ respectivamente; assim



$$\nu(Q) = \frac{p-1}{2}.\frac{q-1}{2} \ .$$

A reta $y = \frac{q}{p}x$ é uma diagonal de Q. Sejam T_1 e T_2 os triângulos debaixo e em cima o diagonal. Observamos que $y = \frac{q}{p}x$ é inteiro somente quando x é um múltiplo de p. Assim esta diagonal de Q não contem pontos de $\mathcal{L}$. Portanto,

$$\nu(Q) = \nu(T_1) + \nu(T_2).$$

Pelo lema anterior

$$\nu(T_1) = \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{jq}{p}\right]$$

e

$$\nu(T_2) = \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{jp}{q}\right] \quad .$$

Então,

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\nu(T_1)}(-1)^{\nu(T_2)} = (-1)^{\nu(T_1)+\nu(T_2)}$$

$$= (-1)^{\nu(Q)} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

c.q.d.

Exemplo 15. Mostraremos que 30 é um resíduo não quadrático módulo 53.

$$\left(\frac{30}{53}\right) = \left(\frac{2}{53}\right)\left(\frac{3}{53}\right)\left(\frac{5}{53}\right) ;$$

$\left(\frac{2}{53}\right) = -1$, pelo Corolário , e o fato que $53 \equiv 5 \pmod 8$;

$$\left(\frac{3}{53}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{53-1}{2}}\left(\frac{53}{3}\right) = \left(\frac{53}{3}\right) = \left(\frac{2}{3}\right) = -1 ;$$

$$\left(\frac{5}{53}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{53-1}{2}}\left(\frac{53}{5}\right) = \left(\frac{3}{5}\right) = -1 ;$$

então $\left(\frac{30}{53}\right) = -1$.

Juntamos no seguinte teorema as caracterizações dos primos p tais que $\left(\frac{a}{p}\right) = 1$ para $a = -1, 2, 3, 5, 7$.

Teorema 16. Seja p um primo.

$$(\frac{-1}{p}) = 1 \iff p \equiv +1 \pmod 4$$

$$(\frac{2}{p}) = 1 \iff p \equiv \pm 1 \pmod 8$$

$$(\frac{3}{p}) = 1 \iff p \equiv \pm 1 \pmod{12}$$

$$(\frac{5}{p}) = 1 \iff p \equiv \pm 1 \pmod{10}$$

$$(\frac{7}{p}) = 1 \iff p \equiv \pm 1, \pm 3, 9, -11 \pmod{28}.$$

Demonstração. (Exercício 11, V).

6.4. Testar se n é primo

Para saber se um certo inteiro n é primo, é suficiente testar a divisibilidade de n pelos primos $p \leq \sqrt{n}$, que chamamos por primos testes. A quantidade dos primos testes cresce com n. Portanto quando n é "grande" torna-se importante encontrar meios, diferentes e mais eficientes que o da divisão longa, para reduzir o conjunto dos primos testes.

A lei de Reciprocidade Quadrática nos fornece um desses meios.

Teorema 17. Seja p um primo ímpar menor que n. Então, $p|n \iff$ para qualquer inteiro a, vale que

a é um resíduo quadrático (mod. n) $\Longrightarrow$ a é um resíduo quadrático (mod. p).

Demonstração. ($\Longrightarrow$) Como $p|n$, $b^2 \equiv a \pmod{n}$ $\Longrightarrow$ $b^2 \equiv a \pmod{p}$.

($\Longleftarrow$) $kn \equiv 0 \pmod{n}$ para qualquer inteiro k, e assim pela hipótese do teorema, $p|kn$ ou $(\frac{kn}{p}) = 1$. Como p é ímpar, $(\frac{s}{p}) = -1$ para algum inteiro s. Então sn é quadrático módulo n e não será quadrático módulo p, a menos que $p|n$.

c.q.d.

Assim por exemplo, seja 2 um resíduo quadrático módulo n; então dos primos testes ímpares, precisamos considerar somente aqueles que satisfazem $p \equiv \pm 1 \pmod{8}$. Se 3 é um outro resíduo quadrático módulo n, reduzimos o conjunto desses primos ainda mais pela condição

$$p = 3 \quad \text{ou} \quad p \equiv \pm 1 \pmod{12} \ ;$$

as duas condições simultâneas são equivalente a

$$p \equiv \pm 1 \pmod{24}.$$

Os primos menores que 200 satisfazendo esta congruência são

$$23, \ 47, \ 71, \ 73, \ 97 \ .$$

Daí, se n é ímpar ≤ 40.000 e se 2 e 3 são resíduos quadráticos módulo n, então é preciso testar no máximo 5 primos em vez de 46 !

Um método para gerar resíduos quadráticos "pequenos" baseia-se nas seguintes observações:

(i) $kn = b^2 - a \Longrightarrow a$ é resíduo quadrático módulo n,

(ii) a, b resíduos quadráticos módulo n (b pode ser simplesmente um quadrado) e $a = bc \Longrightarrow c$ é resíduo quadrático módulo n.

Por exemplo, seja $n = 39569$. Então,

$$n = (199)^2 - 32$$
$$= (201)^2 - 832 \ ;$$

dessas equações obtemos os resíduos quadráticos

$$32 \ (= 4^2.2) \ , \quad 832 \ (= 4^3.13) \ ,$$

e deles os resíduos quadráticos

$$2, \ 13 \ .$$

5.5. Exercícios

1. Seja p um primo. Mostre que

$$x^2 + x + 1 \equiv 0 \pmod{p}$$

é solúvel se e somente se $p = 3$ ou p tem a forma $6k + 1$.

2. Generalizar o problema anterior.

3. Encontre todos os resíduos quadráticos módulo 29.

4. Demonstrar o Teorema 5, V.

5. Calcule os valores de $(\frac{a}{b})$, quando $a = 2, 3, 5$ e $b=7, 11, 13$.

6. Seja p um primo. Demonstre que todo resíduo quadrático módulo p é congruente com i^2 para algum i onde $0 \leq i \leq \frac{p-1}{2}$.

7. Sejam p um primo e $\{a_o, a_1, \ldots, a_{\frac{p-1}{2}}\}$ um conjunto de resíduos quadráticos módulo p que são mutuamente não congruentes. Demonstre que

$$p > 3 \Longrightarrow a_o + a_1 + \ldots + a_{\frac{p-1}{2}} \equiv 0 \pmod{p}.$$

8. Demonstrar a parte (ii) do Corolário 10, V.

9. Seja C um círculo centrado na origem com raio um inteiro $n > 0$. Mostre que

$$\nu(C) = (2n - 1)^2 + 4.$$

10. Calcule $(-\frac{10}{33})$.

11. Demonstrar as partes do Teorema 16, V, correspondentes a $(\frac{3}{p})$, $(\frac{5}{p})$, $(\frac{7}{p})$.

12. Fatorizar os números 9997, 10003 usando o teste exposto na secção 5.4.

CAPÍTULO VI

EQUAÇÕES DIOFANTINAS

6.1. Diofantus-Hilbert

Diofantus de Alexandria (?250 DC) escreveu uma obra importante entitulada Arithmetica na qual ele tratou certas equações algébricas tais como $ax + by = c$, $x^2 + y^2 = z^2$, $x^4 + y^4 + z^4 = u^2$ e suas soluções inteiras, ou racionais, positivas. (veja [12])

A equação

$$f(x_1, x_2, \ldots, x_k) = 0$$

chama-se uma equação Diofantina, quando f é um polinômio de coeficientes inteiros e quando se exige que as soluções sejam inteiras.

Não pretendemos discutir a solução da equação Diofantina geral. Aliás, não existem meios para fazê-lo. Por exemplo, relativamente pouco é conhecido sobre as soluções da equação Diofantina

$$f(x_1, x_2, x_3) = 0$$

onde f é o polinômio cúbico geral. Em particular, não se sabe se

$$x_1^3 + x_2^3 + x_3^3 = 30$$

admite soluções inteiras.

Trataremos neste capítulo das equações $a_1x_1 + a_2x_2 + \ldots + a_kx_k = c$, $x^n + y^n = z^n$ para $n = 2, 4$, $x^2 - y^2 = n$, $x^2 + y^2 = n$, $x_1^2+x_2^2+x_3^2+ x_4^2 = n$. O livro referência sobre equações Diofantinas é de Mordell [16].

O grande matemático alemão David Hilbert (1862-1943) enunciou, no Congresso Internacional dos Matemáticos de 1900 em Paris, vários problemas que influenciaram e continuam a influenciar o rumo da matemática moderna. O décimo problema de Hilbert foi encontrar um algoritmo que pode decidir se uma equação Diofantina geral possui ou não soluções inteiras.

Uma teoria de Conjuntos Diofantinos foi desenvolvida por Julia Robinson, Martin Davis e outros para lidar com o décimo problema de Hilbert. Um conjunto S de inteiros positivos chama-se um conjunto Diofantino se e somente se existe um polinômio f de várias variáveis com coeficientes inteiros tal que S = os valores positivos de f quando as variáveis de f tomam valores inteiros.

O toque final que acabou com o problema foi dado pelo matemático russo Yuri Matiyasevič em 1970. O resultado final:

não existe um tal algoritmo!

Um co-produto do trabalho de Matiyasevie foi a construção de um polinômio $P(x_1, \ldots, x_n)$ de coeficientes inteiros com $n = 21$, de grau 21 tal que

$$x_1, \ldots, x_n \text{ naturais }, \quad P(x_1, \ldots, x_n) > 0$$

$$\Longrightarrow \quad P(x_1, \ldots, x_n) \text{ primo},$$

e todos os primos podem ser assim gerados. Salientamos que $P(x_1, \ldots, x_n)$ assume valores negativos para um conjunto infinito de inteiros $x_1, \ldots, x_n > 0$.

Depois de ter estudado este capítulo o leitor poderá apreciar o artigo de Martin Davis "Hilbert's tenth problem is unsolvable" (veja [3]).

6.2. $\sum_{i=1}^{k} a_i x_i = c$

Consideremos primeiro o caso

$$ax + by = c \tag{1}$$

onde a, b são inteiros não nulos. Seja $d = (a,b)$. Evidentemente, (1) não tem solução se $d \nmid (a,b)$.

Suponhamos que $d \mid (a,b)$; vamos mostrar que (1) tem soluções e vamos determiná-las. Podemos supor que $d = 1$; pois, (x_o, y_o) é uma solução de (1) $\Longleftrightarrow$ (x_o, y_o) é uma solução de $\frac{a}{d} x + \frac{b}{d} y = \frac{c}{d}$. Da equação (1) obtemos a congruência $ax \equiv c \pmod{b}$, cujas soluções são

$$x = x_o + bt$$

onde $x_o = c(\frac{1}{a})_b$ e t é qualquer inteiro. Tendo em vista que $b|c - ax_o$, obtemos de (1),

$$y = \frac{c - ax_o}{b} - at .$$

Por exemplo, as soluções de $10x + 6y = 8$ são as mesmas de $5x + 3y = 4$; pondo $a = 5$, $b = 3$, $c = 4$, obtemos que

$$(\frac{1}{5})_3 = 2 \quad , \quad x_o = 8$$

e as soluções são

$$x = 8 + 3t \ , \quad y = -12 - 5t$$

para qualquer inteiro t.

Agora consideremos a equação geral

$$a_1x_1 + a_2x_2 + \ldots + a_kx_k = c \qquad (2)$$

onde os a_i's são inteiros não nulos. Seja $d = (a_1, a_2, \ldots, a_k)$. Evidentemente, se $d\nmid c$, (2) não admite soluções inteiras. Por outro lado, se $d|c$, podemos supor $d = 1$. Daremos a seguir um método para diminuir o número das variáveis da equação (2). Aproveitando este método podemos usar indução sobre o número das variáveis de (2) para demonstrar a existência de suas soluções.

Lema 1. Sejam α, β, γ, δ inteiros tais que $\alpha\delta - \beta\gamma = 1$.

Sejam também $x_1 = \alpha u_1 + \beta u_2$, $x_2 = \gamma u_1 + \delta u_2$. Então, x_1, x_2 são inteiros $\Longleftrightarrow$ u_1, u_2 são inteiros.

Demonstração. Basta resolver essas equações para u_1 e u_2, $u_1 = \delta x_1 - \beta x_2$, $u_2 = -\gamma x_1 + \alpha x_2$.

c.q.d.

Substituímos as expressões de x_1, x_2 do lema anterior na equação (2), obtendo

$$(a_1\alpha+a_2\gamma)u_1 + (a_1\beta+a_2\delta)u_2 + a_3x_3 + \ldots + a_kx_k = c \qquad (3)$$

O mesmo lema nos garante que

$(u_1, u_2, x_3, \ldots, x_k)$ é uma solução de (3)

$\Longleftrightarrow$

$(x_1, x_2, x_3, \ldots, x_k)$ é uma solução de (2).

Temos a liberdade de escolher α, β, γ, δ, porém mantendo a condição $\alpha\delta - \beta\gamma = 1$. Sejam

$$\alpha = \frac{a_2}{(a_1,a_2)} \quad , \quad \gamma = -\frac{a_1}{(a_1,a_2)} \ .$$

Então, $(\alpha,\gamma) = 1$ e pelo uso do algoritmo Euclideano obtemos os valores de δ e β. Essas escolhas transformam a equação (2) no seguinte sistema equivalente,

$$x_1 = \alpha u_1 + \beta u_2 \quad ,$$

$$x_2 = \gamma u_1 + \delta u_2 \quad ,$$

$$\alpha = \frac{a_2}{(a_1,a_2)} , \quad \gamma = - \frac{a_1}{(a_1,a_2)} ,$$

$$\alpha\delta - \beta\gamma = 1 ,$$

$$(a_1,a_2)u_2 + a_3x_3 + \ldots + a_kx_k = c ;$$

na última vale $((a_1,a_2), a_3, \ldots, a_k, c) = 1$. Repetindo este processo conseguiremos as soluções na forma paramétrica,

$$x_1 = \alpha_{11}u_1 + \alpha_{12}u_2 + \ldots + \alpha_{1\ k-1}u_{k-1} + \beta_1$$

$$x_2 = \alpha_{21}u_1 + \alpha_{22}u_2 + \ldots + \alpha_{2\ k-1}u_{k-1} + \beta_2$$

$$\vdots$$

$$x_k = \alpha_{k1}u_1 + \alpha_{k2}u_2 + \ldots + \alpha_{k\ k-1}u_{k-1} + \beta_k$$

onde os α_{ij} e os β_i's são inteiros e os u_i's são variáveis tomando valores inteiros.

Exemplo 2. Encontrar todas as soluções inteiras de

$$10x_1 + 6x_2 + 5x_3 = 8 .$$

Sejam $a_1 = 10$, $a_2 = 6$, $a_3 = 5$, $c = 8$. Então,

$$\alpha = 3, \quad \gamma = -5 \quad \text{e} \quad \alpha\delta - \beta\gamma = 3\delta + 5\beta = 1;$$

daí

$$\beta = -1 , \quad \delta = 2 .$$

Também,

$$x_1 = 3u_1 - u_2 \ , \quad x_2 = -5u_1 + 2u_2$$

e

$$2u_2 + 5x_3 = 8.$$

A solução da última equação é

$$u_2 = 5v + 24 \ , \quad x_3 = -2v - 8 \ .$$

Assim as soluções da equação original são

$$x_1 = 3u - 5v - 24$$

$$x_2 = -5u + 10v + 48$$

$$x_3 = 0u - 2v - 8$$

para quaisquer inteiros u e v.

6.3. A Equação de Fermat $x^n + y^n = z^n$

6.3.1. $x^2 + y^2 = z^2$

O teorema de Pitágoras afirma que, dado um triângulo reto com as medidas, z para a hipotenusa, x, y para os outros lados, então $x^2 + y^2 = z^2$. Esta equação admite soluções inteiras, tais como $x = 0$, $y = \pm z$ e $x = \pm z$, $y = 0$ que vamos chamar soluções triviais, e outras não triviais como, $x = 3$, $y = 4$, $z = 5$. A fórmula para gerar todas as soluções inteiras foi conhecida desde a antiguidade e acha-se

provada na Arithmética de Diofantus.

Seja (x,y,z) uma tripla de inteiros tais que $xy \neq 0$ e

$$x^2 + y^2 = z^2 \qquad (1),$$

e seja $d = (x,y)$. Então,

$$(x^2,y^2) = d^2 \ , \quad d^2 | z^2 \quad \text{e} \quad d|z \ .$$

Os inteiros $x' = \frac{x}{d}$, $y' = \frac{y}{d}$, $z' = \frac{z}{d}$ são primos entre si e formam uma solução de (1); chamamos (x',y',z') uma solução reduzida. Determinaremos a seguir as soluções reduzidas (x,y,z) de (1).

Reescrevendo (1) como

$$x^2 = z^2 - y^2 = (z-y)(z+y) \qquad (2)$$

nos permita estudar a fatorização de x. Seja p um primo divisor de x; então, $p^2|x^2$ e daí tem-se as três possibilidades seguintes,

$$p^2|z-y \quad \text{ou} \quad p^2|z+y \quad \text{ou} \quad p|z+y \ , \ z-y \ .$$

Da última possibilidade tiramos a conclusão que $p = 2$; pois, $p|(z+y)+(z-y)$, $(z+y)-(z-y)$ e assim $p|2(z,y)$. Por conseguinte, se p é ímpar então

$$p^2|z+y \quad \text{ou} \quad p^2|z-y \ .$$

Em outras palavras, $(u,v) = 1$ e existe um inteiro $\alpha \geq 0$

tal que

$$z - y = 2^{\alpha}u^2 \ , \quad z + y = 2^{\alpha}v^2 \ ;$$

portanto temos,

$$\begin{aligned} 2z &= 2^{\alpha}(u^2 + v^2) \\ 2y &= 2^{\alpha}(-u^2 + v^2) \end{aligned} \qquad (3).$$

Lembramos que $(z,y) = 1$ e assim de (3),

$$0 \leq \alpha \leq 1 \ .$$

Do caso $\alpha = 1$, surge o primeiro tipo de solução,

$$z = u^2 + v^2, \quad y = -u^2 + v^2, \quad x = 2uv \qquad (4)$$

onde,

u, v são de paridades distintas e $(u,v) = 1$.

Do caso $\alpha = 0$, surge o segundo tipo de solução,

$$z = \frac{u^2 + v^2}{2}, \quad y = \frac{-u^2 + v^2}{2} \ , \quad x = uv \qquad (5)$$

onde,

u, v são ambos ímpares e $(u,v) = 1$.

Notamos que em (4), x: par, y: ímpar e que em (5), x: ímpar, y: par. Notamos também que x e y são simétricos na equação (1). Consequentemente, as soluções reduzidas podem ser reexpressas nas seguintes formas

(i) $x = 2uv$, $y = -u^2 + v^2$, $z = u^2 + v^2$ com u e v inteiros quaisquer de paridades distintas com $(u,v) = 1$,

ou

(ii) (a forma (i) com x e y trocados).

6.3.2. O Último Teorema de Fermat

Foi em 1637 quando Pierre Fermat anotou na margem de uma das páginas de Arithmetica por Diofantus que a equação

$$x^n + y^n = z^n \qquad (1)$$

tem soluções triviais para $n > 2$ e se desculpou de escrever a demonstração por falta de espaço suficiente. Apesar dos esforços de gerações sucessivas de matemáticos o "último teorema de Fermat" continua em aberto. Nem tudo foi em vão; por exemplo, as tentativas de Ernst Eduard Kummer (1810 - 1893) resultaram no desenvolvimento da Teoria Algébrica dos Números.

Seja m um inteiro positivo divisor de n e seja $n' = \frac{n}{m}$. De uma solução (x,y,z) não trivial de (1) obtem-se $(x^{n'},y^{n'},z^{n'})$ uma solução não trivial de $x^m + y^m = z^m$. Logo, para mostrar o "último teorema de Fermat" seria suficiente considerar $n = 4$ ou um primo ímpar. No que se segue vamos resolver o primeiro caso.

Para uma exposição mais detalhada do problema de Fermat recomendamos a leitura de [21].

6.3.3. No seguinte demonstraremos que as soluções de

$$x^4 + y^4 = z^2 \tag{2}$$

são triviais. Este resultado implica evidentemente o caso $n = 4$ da conjectura de Fermat.

Suponhamos por absurdo que (2) tenha soluções não triviais. Então se encontram entre elas soluções (x,y,z) que são reduzidas com x, y, z não nulas. Dessas escolhemos (x,y,z) com o menor z possível.

Notamos que (x^2,y^2,z) é uma solução da equação

$$X^2 + Y^2 = Z^2. \tag{3}$$

Então, pela secção anterior, podemos supor que x: par, y: ímpar e que existem u, v inteiros primos entre si e de paridades distintas tais que

$$x^2 = 2uv \tag{4}$$

$$y^2 = u^2 - v^2 \tag{5}$$

$$z = u^2 + v^2 . \tag{6}$$

Da equação (5), observa-se que (v,y,u) é uma solução reduzida de (3); assim, obtemos v: par do fato y: ímpar. Da equação (4), existem inteiros positivos x_1, x_2 tais que

$$u = x_1^2, \quad v = 2x_2^2 . \tag{7}$$

Substituindo as expressões de u e v de (7) em (5) obtem-se

$$(2x_2^2)^2 + y^2 = (x_1^2)^2 \quad . \tag{8}$$

Tendo em vista que $(2x_2^2, y, x_1^2)$ é uma solução reduzida de (3), existem x_3, x_4 inteiros primos entre si e de paridades distintas tais que

$$v = 2x_2^2 = 2\, x_3 x_4 \tag{9}$$

$$y = x_3^2 - x_4^2 \tag{10}$$

$$x_1^2 = x_3^2 + x_4^2 \quad . \tag{11}$$

De (9), tiramos a conclusão crucial de que

$$x_3 = x_3'^2 \ , \quad x_4 = x_4'^2 \quad . \tag{12}$$

Voltamos para (11) onde substituímos as expressões de x_3 e x_4, obtendo

$$(x_3')^4 + (x_4')^4 = x_1^2 \quad . \tag{13}$$

Assim surgiu (x_3', x_4', x_1') uma nova solução reduzida da equação original (2). Observamos finalmente que $0 < x_1 < z$, em choque com a escolha inicial de z.

6.4. Os Inteiros n de Forma $f(\vec{x})$

Seja $f(x_1, \ldots, x_n)$ $(= f(\vec{x}))$ um polinômio em k variáveis com coeficientes inteiros. Quando os x_i's são inteiros, $f(\vec{x})$ toma valores inteiros; procura-se uma descrição desses valores.

Os polinômios $f(\vec{x})$ que vamos considerar são

$$x_1^2 - x_2^2 \ , \quad x_1^2 + x_2^2 \ , \quad x_1^2 + x_2^2 + x_3^2 + x_4^2 \ .$$

6.4.1. $x_1^2 - x_2^2 = n$.

Teorema 3. Existem inteiros x_1, x_2 tais que

$$x_1^2 - x_2^2 = n$$

se e somente se $n = ab$ para inteiros a, b de mesma paridade. Em particular, todo inteiro ímpar tem esta representação.

Demonstração. Sejam $x_1^2 - x_2^2 = n$, $x_1 - x_2 = a$ e $x_1 + x_2 = b$. Então,

$$x_1 = \frac{a + b}{2} \ , \qquad x_2 = \frac{b - a}{2} \ .$$

Para que x_1 e x_2 sejam inteiros, evidentemente a e b devem ser da mesma paridade; esta condição é também suficiente.

Quando n é ímpar, pode existir várias escolhas para a e b; porém, a mais simples é $a = 1$, $b = n$.

c.q.d.

6.4.2. $x_1^2 + x_2^2 = n$.

Teorema 4. Seja n um inteiro positivo

$n = x_1^2 + x_2^2 \iff$ n quadrado

ou

existem inteiros g, n_o, s tais que $n = g^2 n_o$ e $s^2 \equiv -1 \pmod{n_o}$.

Demonstração. ($\Longrightarrow$) Suponhamos que n é não quadrado; então $x_1 \neq 0 \neq x_2$. Seja $g = (n, x_1)$; então, $g | x_2$, $g^2 | n$ e $n = g^2 n_o$ para um inteiro n_o. Pondo $x_1' = \frac{x_1}{g}$, $x_2' = \frac{x_2}{g}$ e $n_o = \frac{n}{g^2}$, obtemos

$$x_1'^2 + x_2'^2 = n_o .$$

Portanto,

$$x_1'^2 \equiv -x_2'^2 \pmod{n_o},$$

e

$$(x_1' \cdot (\tfrac{1}{x_2'})_{n_o})^2 \equiv -1 \pmod{n_o} .$$

($\Longleftarrow$) Podemos supor que n é não quadrado. Além do mais, para efeito da demonstração, n é redutível a n_o. Pois se x_1, x_2 são inteiros tais que

$$x_1^2 + x_2^2 = n_o ,$$

então,

$$(x_1 g)^2 + (x_2 g)^2 = n_o g^2 = n \ .$$

Sejam

$$s^2 \equiv -1 \pmod{n},$$

e

$$T = \{a + sb \mid a, b \text{ inteiros com } 0 \leq a, b < \sqrt{n}\}.$$

n sendo não quadrado,

$$[\sqrt{n}] < \sqrt{n} < 1 + [\sqrt{n}] \ ,$$

e daí,

$$|T| = (1 + [\sqrt{n}])^2 > n \ .$$

Existem dois elementos $a + sb$, $a' + sb'$ de T tais que

$$a + sb \equiv a' + sb' \pmod{n}.$$

Sejam $a_o = a - a'$, $b_o = b' - b$. Os inteiros s, a_o, b_o satisfazem as seguintes condições

$$s^2 \equiv -1 \pmod{n} \qquad (1)$$

$$a_o \equiv sb_o \pmod{n} \qquad (2)$$

$$0 \leq |a_o|, |b_o| < \sqrt{n} \ . \qquad (3)$$

Pelas condições (1), (2),

$$a_o \neq 0 \neq b_o,$$

e

$$0 < |a_o|, |b_o| < \sqrt{n} . \qquad (4)$$

A última desigualdade dá

$$0 < a_o^2 + b_o^2 < 2n . \qquad (5)$$

Por (2),

$$a_o^2 \equiv s^2 b_o^2 \pmod{n} ,$$

e por (1),

$$a_o^2 - s^2 b_o^2 \equiv a_o^2 + b_o^2 \equiv 0 \pmod{n} . \qquad (6)$$

Finalmente, obtemos de (5) e (6),

$$a_o^2 + b_o^2 = n .$$

c.q.d.

6.4.3. O Problema de Waring

Waring afirmou em 1792 que todo inteiro positivo é a soma de 4 quadrados, 9 cubos, 17 potências quartas, assim sugerindo que para cada k existe um inteiro s dependendo somente de k para os quais a equação diofantina

$$n = x_1^k + x_2^k + \ldots + x_s^k$$

tem pelo menos uma solução de inteiros $x_1, x_2, \ldots, x_s \geq 0$.

A maneira de resolver este problema não foi nada ób

vio. O caso $k = 2$ que vamos expor apresentou dificuldades inesperadas a ambos Euler e Lagrange. Outros casos específicos foram resolvidos até que em 1909 Hilbert deu a primeira solução completa para cada k. Para este fim Hilbert mostrou que dado k, existem inteiros m, $n > 0$ e $a_{ij} \geq 0$ tais que

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)^k n = \sum_{i=1}^{m} (a_{i1}x_1 + a_{i2}x_2 + a_{i3}x_3 + a_{i4}x_4)^{2k}.$$

Apresentaremos a seguir a demonstração do caso k=2 .

Teorema 5 (Euler-Lagrange). Todo inteiro positivo pode ser realizado como a soma dos quadrados de no máximo quatro inteiros.

Seja $\nu(\vec{x}) = \nu(x_1,x_2,x_3,x_4) = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Antes de dar a demonstração do teorema vamos notar algumas das propriedades de $\nu(\vec{x})$.

Lema 6.- $\nu(\vec{x})\nu(\vec{y}) = \nu(\vec{z})$, onde as coordenadas de $\vec{z}$ são

$$z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \quad ,$$

$$z_2 = x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 \quad ,$$

$$z_3 = x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4 \quad ,$$

$$z_4 = x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2 .$$

Lema 7. Seja α um número real. Então,

$$\nu(\alpha\vec{x}) = \alpha^2\nu(\vec{x}) .$$

Lema 8. $\nu(x_1+x_2,\ x_2-x_1,\ x_3+x_4,\ x_4-x_3) = 2\nu(\vec{x})$.

Lema 9. Seja m um inteiro > 1. Sejam x_i, y_i inteiros tais que $x_i \equiv y_i \pmod{m}$, para $i = 1, 2, 3, 4$. Então,

$$\nu(\vec{x})\nu(\vec{y}) = \nu(\vec{z}) ,$$

e $\vec{z}$ satisfaz,

$$z_1 \equiv \nu(\vec{x}) \pmod{m}$$

$$z_2 \equiv z_3 \equiv z_4 \equiv 0 \pmod{m}.$$

Os lemas enunciados acima podem ser verificados diretamente (Exercício 9, VI).

Demonstração do Teorema 5. Dado o primeiro lema, é suficiente demonstrar o teorema para n um primo, e até um primo ímpar. Seja p um primo ímpar.

Primeiramente mostraremos que existem inteiros m, x_1, x_2, x_3, x_4 tais que $\nu(\vec{x}) = mp$, com $0 < m < p$. Com este fim, sejam

$$A = \{a^2 \mid 0 \leq a \leq \frac{p-1}{2}\},$$

e

$$B = \{-b^2-1 \mid 0 \leq b \leq \frac{p-1}{2}\}.$$

Os elementos de A são não congruentes módulo p; igualmente dito para os elementos de B. O conjunto $A \cup B$ contém $p+1$ elementos distintos. Portanto, $a^2 \equiv -b^2 - 1 \pmod{p}$ para certos inteiros a, b satisfazendo, $0 \leq a,b \leq \frac{p-1}{2}$. Expressamos a congruência anterior na forma

$$a^2 + b^2 + 1 = mp$$

para algum inteiro m. Eis uma estimativa de m,

$$mp = a^2 + b^2 + 1 \leq (\frac{p-1}{2})^2 + (\frac{p-1}{2})^2 + 1 = \frac{(p-1)^2}{2} +$$

$$+ 1 < p^2$$

e assim, $m < p$.

Em segundo lugar, escolhemos de todos os múltiplos de p produzidos por ν o mínimo $m' > 0$. Desejamos mostrar que $m' = 1$. Seja $\vec{x}$ tal que $\nu(\vec{x}) = m'p$.

Suponhamos que $2 \mid m'$. O número dos inteiros pares entre x_1, x_2, x_3, x_4 é 0, 2 ou 4. Quando exatamente dois dos x_i's são pares, reenumeramo-os fazendo com que x_1 e x_2 sejam pares. Mantendo este acordo podemos afirmar que em todos os casos,

$$x_1 + x_2, \quad x_1 - x_2, \quad x_3 + x_4, \quad x_4 - x_3$$

são números pares. Usando os lemas 7 e 8, obtemos

$$\nu\left(\frac{x_1 + x_2}{2}, \frac{x_2 - x_1}{2}, \frac{x_3 + x_4}{2}, \frac{x_4 - x_3}{2}\right) =$$

$$= \frac{1}{2}\nu(\vec{x}) = \frac{m'}{2}\, p \quad ;$$

contradizendo a minimalidade de m'.

Suponhamos que $3 \leq m' < p$. Para $1 \leq i \leq 4$, consideremos y_i inteiro tal que

$$y_i \equiv x_i \pmod{m'} \quad \text{e} \quad 0 \leq |y_i| \leq \frac{m' - 1}{2} .$$

Tendo em vista que $\nu(\vec{y}) \equiv \nu(\vec{x}) \pmod{m'}$, $\nu(\vec{y}) = \ell m'$ para algum inteiro ℓ. Naturalmente, $m' \leq 4(\frac{m' - 1}{2})^2 = (m'-1)^2$, e portanto, $0 \leq \ell \leq \frac{(m' - 1)^2}{m'} < m'$. Se $\ell = 0$, $y_1^2 + y_2^2 + y_3^2 + y_4^2 = 0$ e desta igualdade se desencadeiam as seguintes conclusões,

$$y_1 = y_2 = y_3 = y_4 = 0 \ ,$$

$$x_1 \equiv x_2 \equiv x_3 \equiv x_4 \equiv 0 \pmod{m'},$$

$$(m')^2 | \nu(\vec{x}) \ ,$$

e $$(m')^2 = mp \ , \quad m' = p \ ;$$

a última está em contradição com $m' < p$.

Chegamos a última etapa da demonstração. Considera

mos o produto $\nu(\vec{x})\nu(\vec{y})$. Pelo lema 6, $\nu(\vec{x})\nu(\vec{y}) = \nu(\vec{z})$, e portanto,

$$m'p.\ m'\ell = \nu(\vec{z}) .$$

Usando o lema 9, obtemos que

$$z_1 \equiv \nu(\vec{x}) \equiv 0 , \quad z_2 \equiv z_3 \equiv z_4 \equiv 0 \ (\text{mod. } m') ;$$

daí,

$$p\ell = \nu(\tfrac{1}{m'}\vec{z}) \qquad \text{com} \qquad \ell < m' ;$$

contradizendo a minimalidade de m'.

c.q.d.

6.5. Exercícios

1. Seja c um inteiro positivo ímpar. Demonstre que

$$x^2 + 1 = y^3 + (2c)^3$$

não tem soluções inteiras. (Fatorize o lado direito e observe que os primos divisores do lado esquerdo são da forma $4k + 1$).

2. Seja $f(x) \in Z[x]$. Mostre que se $f(n)$ é primo para $n > N$, onde N é algum número natural, então $f(x)$ é um primo. (Suponha $f(x)$ não constante; seja $f(x_o) = y_o$ e observe que $f(x_o + ty_o) = f(x_o) + f'(x_o)(ty_o) + \ldots + \frac{f^{(k)}(x_o)}{k!}(ty_o)^k = y_o(1 + f'(x_o) + \ldots))$.

3. Encontre todas as soluções inteiras de cada uma das seguintes equações

$$2x + 3y = 5, \quad 2x + 3y + 4z = 7,$$

$$2x + 3y + 4z + 5w = 11.$$

4. Demonstre que se n é um inteiro ≥ 3, então n é um elemento de alguma tripla de inteiros (x,y,z) que satisfazem $x^2 + y^2 = z^2$.

5. Mostre que a equivalência entre "o último teorema de Fermat" e "$x^n + y^n = 1$ não admite soluções racionais não triviais para $n > 2$". Traçar os gráficos de $x^3 + y^3 = 1$,

$x^4 + y^4 = 1$, no plano.

6. Demonstre que $x^4 + 4y^4 = z^2$ não tem soluções inteiras não triviais.

7. Demonstre que todo inteiro n pode ser colocado na forma $x^2 + y^2 - z^2$.

8. Verifique a identidade

$$\sum_{i=1}^{4} (z^3 + x_i)^3 + (z^3 - x_i)^3 = 8z^9 + 6z^3\left(\sum_{i=1}^{4} x_i^2\right) .$$

9. Demonstre os Lemas 6, 7, 8, 9, VI.

10. Mostrar que nenhum inteiro da forma $4^m(8k + 7)$ é a soma de três quadrados.

REFERÊNCIAS*

1. Ayoub, Raymond - An Introduction to the Analytic Theory of numbers, American Mathematical Society, Rhode Island , (1963).

2. Baker, C. L., Gruenberger, F. J. - The First Six Million Prime Numbers, The Rand Corporation, Santa Monica , (1957).

3. Davis, Martin - "Hilbert's Tenth Problem is Unsolvable" , Amer. Math. Monthly, 80 (1973), pp. 233-269.

4. Dickson, L. E. - History of the Theory of Numbers, (3 volumens) Carnegia Institution (1923).

5. Figueiredo, D. G. de - Números Irracionais e Transcendentes, Monografias de Matemática (19), IMPA, Rio de Janeiro (1974).

6. Gauss, C. F. - Disquisitiones Arithmeticae, transl. A. A. Clarke, Yale, New Haven (1966).

7. Gelfond, Linnik - Elementary Methods in Analytic Number Theory, George Allen and Unwin Ltd., London (1965).

8. Gioia, A. A. - The Theory of Numbers - An Introduction , Markham Publishing Company - Chicago (1970).

9. Goldstein, L. J. - "A History of the Prime Number Theorem" Amer. Math. Monthly, 80 (1973), pp. 599-615.

---

* Esse material bibliográfico encontra-se, na sua maioria , na excelente biblioteca do IMPA.

10. Groza, V. S. - A Survey of Mathematics - Elementary Concepts and Their Historical Developement, Holt, Rinehart and Winston, New York (1968).

11. Hardy, Wright - The Theory of Numbers, 3rd ed., Oxford University Press (1954).

12. Heath - Diophantus of Alexandria, Cambridge (1910).

13. Legendre - Essai sur la Theorie de Nombres, 2nd ed., Paris (1808).

14. Lamé - Comptes Rendus, 19, página 867.

15. Monteiro, L. H. J., Elementos de Álgebra, Col. Elementos de Matemática, Ao Livro Técnico, Rio de Janeiro (1969).

16. Mordell, L. J. - Diofantine Equations, Academic Press , London (1969).

17. Newman, J. R. - The World of Mathematics, George Allen and Unwin Ltd, London (1961).

18. Niven, Zuckerman - An Introduction to the Theory of Numbers, 2nd ed., Wiley, New York (1962).

19. Sierpiński, W. - 250 Problems in Elementary Number Theory, American Elsevier Publishing Company, New York (1970).

20. Waerden, B. L. van der - Science Awakening, P. Noordhoff Ltd, Holland (1954).

21. Vandiver, H. S. - "Fermat's Last Theorem", Amer. Math . Monthly, 53 (1946), pp. 555-578.

22. Weil, A. - Number Theory, Springer Verlag, New York(1968).