1.25 (IMO1997)**.** *Encontrar todos os pares (x, y) de inteiros positivos tais que $x^{y^2} = y^x$.*

Dica: Sejam $x = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ e $y = p_1^{\beta_1} \dots p_n^{\beta_n}$ as fatorações canônicas de x e y. Mostre que $\alpha_j = t\beta_j$ e $x = y^t$ para algum $t \in \mathbb{Q}$ e limite os valores de t.

1.26. *Generalizar o resultado anterior para $x^{y^n} = y^x$, onde x e y são inteiros positivos.*

1.27 (IMO1984)**.** *Sejam a, b, c, d inteiros ímpares tais que $0 < a < b < c < d$ e $ad = bc$. Demonstre que se $a + d = 2^k$ e $b + c = 2^m$ para inteiros k e m, então $a = 1$.*

1.4 Congruências

Sejam $a, b, n \in \mathbb{Z}$. Dizemos que a *é congruente a b módulo n*, e escrevemos

$$a \equiv b \pmod{n}$$

se $n \mid a - b$, ou seja, se a e b deixam o mesmo resto na divisão por n. Por exemplo, temos que $17 \equiv 3 \pmod{7}$ e $10 \equiv -5 \pmod{3}$.

Proposição 1.24. *Para quaisquer $a, b, c, d, n \in \mathbb{Z}$ temos:*

1. *(Reflexividade) $a \equiv a \pmod{n}$;*
2. *(Simetria) se $a \equiv b \pmod{n}$, então $b \equiv a \pmod{n}$;*
3. *(Transitividade) se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, então $a \equiv c \pmod{n}$;*
4. *(Compatibilidade com a soma e diferença) Podemos somar e subtrair "membro a membro":*

$$\begin{cases} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{cases} \implies \begin{cases} a + c \equiv b + d \pmod{n} \\ a - c \equiv b - d \pmod{n} \end{cases}$$

Em particular, se $a \equiv b \pmod{n}$, então $ka \equiv kb \pmod{n}$ para todo $k \in \mathbb{Z}$.

Cópia Fiel

5. *(Compatibilidade com o produto) Podemos multiplicar "membro a membro":*

$$\begin{cases} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{cases} \implies ac \equiv bd \pmod{n}$$

Em particular, se $a \equiv b \pmod{n}$*, então* $a^k \equiv b^k \pmod{n}$ *para todo* $k \in \mathbb{N}$*.*

6. *(Cancelamento) Se* $\mathrm{mdc}(c, n) = 1$*, então*

$$ac \equiv bc \pmod{n} \iff a \equiv b \pmod{n}.$$

Demonstração: Para o item *(1)* basta observar que $n \mid a - a = 0$. Em *(2)*, se $n \mid a - b$, então $n \mid -(a - b) \iff n \mid b - a$. Em *(3)*, se $n \mid a - b$ e $n \mid b - c$, então $n \mid (a - b) + (b - c) \iff n \mid a - c$. Em *(4)* e *(5)*, se $n \mid a - b$ e $n \mid c - d$, então $n \mid (a - b) + (c - d) \iff n \mid (a + c) - (b + d)$, $n \mid (a - b) - (c - d) \iff n \mid (a - c) - (b - d)$ e $n \mid (a - b)c + (c - d)b \iff n \mid ac - bd$. Finalmente, como $\mathrm{mdc}(c, n) = 1$ temos que $n \mid ac - bc \iff n \mid (a - b)c \iff n \mid a - b$ pela proposição 1.9. □

As propriedades acima mostram que a relação $\equiv \pmod{n}$ ("ser congruente módulo n") tem um comportamento muito similar à relação de igualdade usual. São estas propriedades que tornam as congruências tão úteis em problemas de divisibilidade. Vejamos alguns exemplos.

Exemplo 1.25. *Demonstrar que* $31 \mid 20^{15} - 1$.

Solução: Isto é equivalente a demonstrar que $20^{15} \equiv 1 \pmod{31}$. Para isso observemos que

$$20 \equiv -11 \pmod{31} \qquad (*)$$

e assim $20^2 \equiv (-11)^2 \pmod{31} \iff 20^2 \equiv 121 \pmod{31}$. Como $121 \equiv -3 \pmod{31}$ temos

$$20^2 \equiv -3 \pmod{31}. \qquad (**)$$

Multiplicando $(*)$ e $(**)$ membro a membro, obtemos $20^3 \equiv 33 \pmod{31}$ e, como $33 \equiv 2 \pmod{31}$,

$$20^3 \equiv 2 \pmod{31}.$$

Elevando a 5, temos que $20^{15} \equiv 32 \pmod{31}$ e como $32 \equiv 1 \pmod{31}$, obtemos $20^{15} \equiv 1 \pmod{31}$, como desejado. □

Exemplo 1.26. *Encontre os restos das divisões de*

1. 3^{1000} *por* 101
2. $5^{3^{20}}$ *por* 13

Solução: Como $3^4 \equiv -20 \pmod{101}$, elevando ao quadrado obtemos $3^8 \equiv 400 \pmod{101} \iff 3^8 \equiv -4 \pmod{101}$. Multiplicando por 3^2, obtemos $3^{10} \equiv -36 \pmod{101}$. Portanto

$$\begin{aligned} 3^{20} &\equiv 1296 \pmod{101} &&\iff 3^{20} \equiv -17 \pmod{101} \\ 3^{40} &\equiv 289 \pmod{101} &&\iff 3^{40} \equiv -14 \pmod{101} \\ 3^{80} &\equiv 196 \pmod{101} &&\iff 3^{80} \equiv -6 \pmod{101} \\ 3^{80} \cdot 3^{20} &\equiv (-6)\cdot(-17) \pmod{101} &&\iff 3^{100} \equiv 1 \pmod{101}. \end{aligned}$$

Assim, elevando a última congruência a 10, obtemos $3^{1000} \equiv 1 \pmod{101}$, ou seja, 3^{1000} deixa resto 1 na divisão por 101.

Para encontrar o resto da divisão de $5^{3^{20}}$ por 13, note que como $5^4 \equiv 1 \pmod{13}$, os restos de 5^n por 13 se repetem com período 4:

$$\begin{array}{llll} 5^0 \equiv 1 \pmod{13} & 5^4 \equiv 1 \pmod{13} & & \\ 5^1 \equiv 5 \pmod{13} & 5^5 \equiv 5 \pmod{13} & & \\ 5^2 \equiv -1 \pmod{13} & 5^6 \equiv -1 \pmod{13} & & \\ 5^3 \equiv -5 \pmod{13} & 5^7 \equiv -5 \pmod{13} & & \cdots \end{array}$$

Por outro lado, temos $3 \equiv -1 \pmod 4 \implies 3^{20} \equiv 1 \pmod 4$, isto é, 3^{20} deixa resto 1 na divisão por 4. Assim, $5^{3^{20}} \equiv 5^1 \pmod{13}$, ou seja, $5^{3^{20}}$ deixa resto 5 na divisão por 13. □

O problema a seguir tem uma história interessante. Em um artigo publicado em 1969, D. J. Lewis afirmava que a equação $x^3 - 117y^3 = 5$ tem no máximo 18 soluções inteiras. Na verdade, ela não possui nenhuma, como foi provado dois anos mais tarde por R. Finkelstein e H. London, utilizando métodos de Teoria Algébrica dos Números. Em 1973, F. Halter-Koch e V. Şt. Udresco observaram independentemente que existe uma prova muito mais simples deste fato, como mostra o exemplo a seguir.

Exemplo 1.27. *Mostre que a equação $x^3 - 117y^3 = 5$ não possui soluções inteiras.*

Solução: Observe que como 117 é múltiplo de 9, qualquer solução inteira deve satisfazer

$$x^3 - 117y^3 \equiv 5 \pmod 9 \iff x^3 \equiv 5 \pmod 9.$$

Porém, x só pode deixar resto $0, 1, \ldots, 8$ na divisão por 9. Analisando estes 9 casos, temos

x mod 9	0	1	2	3	4	5	6	7	8
x^3 mod 9	0	1	8	0	1	8	0	1	8

Ou seja, x^3 só pode deixar resto 0, 1 ou 8 na divisão por 9. Logo $x^3 \equiv 5 \pmod 9$ é impossível e a equação não possui soluções inteiras. □

Exemplo 1.28 (AusPol2002)**.** *Encontrar todas as ternas (a, b, c) de inteiros não negativos tais que $2^a + 2^b + 1$ é múltiplo de $2^c - 1$.*

Solução: O problema pede para determinar quando $2^a + 2^b + 1 \equiv 0 \pmod{2^c - 1}$. Note que como $2^c \equiv 1 \pmod{2^c - 1}$, escrevendo $a = cq_1 + a'$ e $b = cq_2 + b'$ com $0 \leq a', b' < c$ temos que

$$\begin{aligned} & 2^a + 2^b + 1 \equiv 0 \pmod{2^c - 1} \\ \iff & (2^c)^{q_1} \cdot 2^{a'} + (2^c)^{q_2} \cdot 2^{b'} + 1 \equiv 0 \pmod{2^c - 1} \\ \iff & 2^{a'} + 2^{b'} + 1 \equiv 0 \pmod{2^c - 1} \end{aligned}$$

que é o mesmo problema com a' e b' no lugar de a e b. Assim, basta resolver o problema supondo $0 \leq a, b < c$. Temos alguns casos a analisar.

Não há soluções com $c = 0$ e para $c = 1$ temos que $(a, b, 1)$ é solução para todos os $a, b \geq 0$. Se $c = 2$, temos que apenas $(0, 0, 2)$ é solução com $0 \leq a, b < c = 2$, o que dá origem às soluções $(2m, 2n, 2)$ para todos os m e n naturais. Se $c = 3$, temos que apenas $(1, 2, 3)$ e $(2, 1, 3)$ são soluções com $0 \leq a, b < c = 3$, o que nos fornece soluções $(1 + 3m, 2 + 3n, 3)$ e $(2+3m, 1+3n, 3)$ para todos os m e n naturais. Finalmente, para $c \geq 4$, temos que se $a < c - 1$ ou $b < c - 1$, então

$$3 \leq 2^a + 2^b + 1 \leq 2^{c-1} + 2^{c-2} + 1 = 3 \cdot 2^{c-2} + 1 < 2^c - 1$$

e assim $2^a + 2^b + 1$ não pode ser múltiplo de $2^c - 1$. Neste caso devemos ter $a = b = c - 1$ e $2^{c-1} + 2^{c-1} + 1 \equiv 0 \pmod{2^c - 1} \iff 2^c + 1 \equiv 0 \pmod{2^c - 1} \iff 2 \equiv 0 \pmod{2^c - 1}$, o que não ocorre pois $2^c - 1 \geq 15$ não pode dividir 2. Logo não há soluções neste último caso.

Resumindo, as ternas pedidas são $(m, n, 1)$, $(2m, 2n, 2)$, $(1 + 3m, 2 + 3n, 3)$ e $(2 + 3m, 1 + 3n, 3)$ onde m e n são naturais arbitrários. □

1.5 Bases

A notação usual para naturais é a chamada base 10, com dígitos $0, \ldots, 9$. Isto significa, por exemplo, que

$$196883 = 1 \cdot 10^5 + 9 \cdot 10^4 + 6 \cdot 10^3 + 8 \cdot 10^2 + 8 \cdot 10^1 + 3 \cdot 10^0.$$

O teorema abaixo mostra como escrever qualquer natural em qualquer base d.

Teorema 1.29. *Seja $n \geq 0$ e $d > 1$. Então existe uma única sequência (os "dígitos" de n na base d) $a_0, \ldots, a_k, \ldots$ com as seguintes propriedades:*

1. *para todo k, $0 \leq a_k < d$,*
2. *existe m tal que se $k \geq m$, então $a_k = 0$,*
3. *$n = \sum_{k \geq 0} a_k d^k$.*

Demonstração: Escrevemos $n = n_0 = n_1 d + a_0$, $0 \leq a_0 < d$, $n_1 = n_2 d + a_1$, $0 \leq a_1 < d$ e em geral $n_k = n_{k+1} d + a_k$, $0 \leq a_k < d$. Nossa primeira afirmação é que $n_k = 0$ para algum valor de k. De fato, se

$n_0 < d^m$, então $n_1 = \lfloor \frac{n_0}{d} \rfloor < d^{m-1}$ e mais geralmente, por indução, $n_k < d^{m-k}$; fazendo $k \geq m$ temos $n_k < 1$ donde $n_k = 0$. Segue daí que $a_k = 0$ para $k \geq m$. A identidade do item *3* é facilmente demonstrada por indução.

Para a unicidade, suponha $\sum_{k\geq 0} a_k d^k = \sum_{k\geq 0} b_k d^k$. Se as sequências a_k e b_k são distintas existe um menor índice, digamos j, para o qual $a_j \neq b_j$. Podemos escrever $a_j + \sum_{k>j} a_k d^{k-j} = b_j + \sum_{k>j} b_k d^{k-j}$ donde $a_j \equiv b_j \pmod{d}$, o que é uma contradição, pois $0 < |a_j - b_j| < d$ e portanto $a_j - b_j$ não pode ser um múltiplo de d. □

Ignorando os dígitos 0's iniciais, denotamos por $(a_n a_{n-1} \cdots a_1 a_0)_d$ o natural cuja representação na base d tem algarismos a_k como no teorema acima:

$$(a_n a_{n-1} \cdots a_1 a_0)_d \stackrel{\text{def}}{=} \sum_{0\leq k\leq n} a_k d^k.$$

Muitos dos famosos critérios de divisibilidade que aprendemos na escola decorrem diretamente da representação acima. Por exemplo, se $N = (a_n a_{n-1} \cdots a_1 a_0)_{10}$, como $10 \equiv 1 \pmod{9}$, temos que $10^k \equiv 1 \pmod{9}$, donde

$$N = \sum_{0\leq k\leq n} a_k 10^k \equiv \sum_{0\leq k\leq n} a_k \pmod{9}.$$

Segue que N e a soma de seus dígitos na base 10 possuem o mesmo resto na divisão por 9; em particular N é divisível por 9 se, e só se, a soma de seus dígitos $a_0 + \cdots + a_n$ é divisível por 9.

De forma similar, para o critério de divisibilidade por 11, observemos que $10 \equiv -1 \pmod{11}$, logo

$$N = \sum_{0\leq k\leq n} a_k 10^k \equiv \sum_{0\leq k\leq n} (-1)^k a_k \pmod{11}$$

e assim um número é divisível por 11 se, e só se, a soma dos dígitos em posição par menos a soma dos dígitos em posição ímpar é divisível por 11. De igual forma, podemos encontrar critérios de divisibilidade por 7, 13 e 37, que deixamos como exercício para o leitor enunciá-los e demonstrá-los (utilize o fato que $10^3 \equiv -1 \pmod{7}$, $10^3 \equiv -1 \pmod{13}$ e $10^3 \equiv 1 \pmod{37}$).

Cópia eletrônica

Exemplo 1.30. *Encontrar os últimos dois dígitos na representação decimal de* 3^{200}.

SOLUÇÃO: Como

$$\begin{aligned}(a_n a_{n-1} \cdots a_1 a_0)_{10} &= 10^2 \cdot (a_n \cdot 10^{n-2} + \cdots + a_2) + (10 \cdot a_1 + a_0) \\ &= 100 \cdot (a_n \ldots a_2)_{10} + (a_1 a_0)_{10}\end{aligned}$$

temos que o número formado pelos dois últimos dígitos de $(a_n \cdots a_1 a_0)_{10}$ é o resto da divisão deste número por 100, logo o problema se resume a calcular 3^{200} módulo 100. Podemos utilizar o binômio de Newton para simplificar as contas:

$$3^{200} = 9^{100} = (10-1)^{100} = \sum_{0 \le k \le 100} \binom{100}{k} 10^{100-k} (-1)^k,$$

logo $3^{200} \equiv -\binom{100}{99}10 + \binom{100}{100} \pmod{100} \iff 3^{200} \equiv 1 \pmod{100}$ e assim os dois últimos dígitos de 3^{200} são 01. □

Exemplo 1.31. *Demonstrar que, para todo* n *natural ímpar,*

$$s_n = 2^{2n} \cdot (2^{2n+1} - 1)$$

termina em 28 *quando escrito em notação decimal.*

SOLUÇÃO: Vamos mostrar por indução em n que s_n termina em 28. Para $n = 1$ temos que $s_1 = 28$. Suponhamos que para algum $n \ge 1$ ímpar s_n termina em 28 e vamos mostrar que s_{n+2} termina em 28 ou, equivalentemente, que $100 \mid s_{n+2} - s_n$. Temos

$$\begin{aligned}s_{n+2} - s_n &= 2^{2(n+2)} \cdot (2^{2(n+2)+1} - 1) - 2^{2n} \cdot (2^{2n+1} - 1) \\ &= 2^{2n} \cdot (16 \cdot 2^{2n+5} - 16 - 2^{2n+1} + 1) \\ &= 5 \cdot 2^{2n} \cdot (51 \cdot 2^{2n+1} - 3).\end{aligned}$$

Como, para n ímpar,

$$\begin{aligned}2^2 \equiv -1 \pmod 5 &\implies 2^{2n} \equiv -1 \pmod 5 \\ &\implies 2^{2n+1} \equiv -2 \pmod 5,\end{aligned}$$

temos que $51 \cdot 2^{2n+1} - 3 \equiv 1 \cdot (-2) - 3 \pmod 5 \iff 51 \cdot 2^{2n+1} - 3 \equiv 0 \pmod 5$. Assim, $s_{n+2} - s_n$ é divisível por $5 \cdot 4 \cdot 5 = 100$. □

1.6 O Anel de Inteiros Módulo n

As semelhanças entre as relações de congruência módulo n e igualdade não são mero fruto do acaso, ambas são instâncias de *relações de equivalência* em $\mathbb{Z}$. Em geral, uma relação $\sim$ sobre um conjunto X é dita de *equivalência* se ela é reflexiva ($x \sim x$ para todo $x \in X$), simétrica ($x \sim y \iff y \sim x$) e transitiva ($x \sim y$ e $y \sim z \implies x \sim z$).

Dar uma relação de equivalência em X é o mesmo que dar uma *partição* $X = \bigsqcup_{\lambda \in \Lambda} X_\lambda$ de X, i.e., uma coleção de subconjuntos $X_\lambda \neq \emptyset$, dois a dois disjuntos, cuja união é X. De fato, dada a partição acima, podemos definir uma relação de equivalência $\sim$ declarando que $x \sim y$ se, e somente se, x e y pertencem a um mesmo X_λ. Reciprocamente, se $\sim$ é uma relação de equivalência, dado um elemento $x \in X$ podemos definir a *classe de equivalência* $\overline{x}$ de x como o conjunto de todos os elementos equivalentes a x:

$$\overline{x} = \{y \in X \mid y \sim x\}.$$

Observe que ou $\overline{x} \cap \overline{y} = \emptyset$ (se $x \not\sim y$) ou $\overline{x} = \overline{y}$ (se $x \sim y$). Assim, as distintas classes de equivalência $\overline{x}$ formam uma partição de X. O conjunto $\{\overline{x} \mid x \in X\}$ das classes de equivalência de $\sim$ é chamado de *quociente* de X por $\sim$ e é denotado por $X/{\sim}$. Intuitivamente, $X/{\sim}$ é o conjunto obtido "igualando-se" elementos equivalentes entre si.

Agora aplicamos esta construção geral ao nosso caso. O quociente de $\mathbb{Z}$ pela relação $\equiv \pmod{n}$ é chamado de *anel de inteiros módulo* n e é denotado por uma das notações $\mathbb{Z}/(n)$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}/n$ ou às vezes $\mathbb{Z}_n$. Por exemplo, para $n = 2$, temos que $\mathbb{Z}/2\mathbb{Z}$ possui apenas dois elementos, $\overline{0}$ e $\overline{1}$ (popularmente conhecidos como conjunto dos pares e ímpares, respectivamente).

A definição de $\overline{a}$ como um subconjunto de $\mathbb{Z}$ raramente será importante, sendo apenas uma maneira de formalizar o fato de que estamos "identificando" todos os inteiros que deixam o mesmo resto na divisão por n (como no exemplo dos pares e ímpares acima). Assim, o importante é sabermos que

$$\begin{aligned} \overline{a} = \overline{a'} &\iff a \equiv a' \pmod{n} \\ &\iff a \text{ e } a' \text{ deixam o mesmo resto na divisão por } n. \end{aligned}$$

Se $n > 0$, a divisão euclidiana diz que todo inteiro a é côngruo a um único inteiro a' com $0 \leq a' < n$; podemos reescrever este fato na nossa

nova linguagem como

$$\mathbb{Z}/(n) = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Os itens *(4)* e *(5)* da proposição 1.24 dizem que as operações de soma, diferença e produto são compatíveis com a relação de congruência. Uma formulação mais abstrata da mesma ideia é dizer que as operações $+$, $-$ e $\cdot$ *passam ao quociente*, i.e., que podemos definir a soma, subtração e o produto de classes de congruência por

$$\begin{aligned} \overline{a} + \overline{b} &= \overline{a+b} \\ \overline{a} - \overline{b} &= \overline{a-b} \\ \overline{a} \cdot \overline{b} &= \overline{a \cdot b} \end{aligned}$$

respectivamente. A dúvida à primeira vista seria se a escolha de a e b não afeta a resposta: afinal existem infinitos inteiros a' e b' com $\overline{a} = \overline{a'}$ e $\overline{b} = \overline{b'}$. Os itens *(4)* e *(5)* da proposição são exatamente o que precisamos: eles nos dizem que nestas condições $\overline{a \pm b} = \overline{a' \pm b'}$ e $\overline{a \cdot b} = \overline{a' \cdot b'}$, de modo que as operações acima estão bem definidas.

Por exemplo, em $\mathbb{Z}/6\mathbb{Z}$ temos as seguintes tabelas de soma e produto:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

e

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

A próxima proposição diz quando podemos "dividir" por a módulo n, isto é, quando o "inverso multiplicativo" de a módulo n está definido:

Proposição 1.32. *Sejam $a, n \in \mathbb{Z}$, $n > 0$. Então existe $b \in \mathbb{Z}$ com $ab \equiv 1 \pmod{n}$ se, e somente se,* $\mathrm{mdc}(a, n) = 1$.

Demonstração: Temos que $ab \equiv 1 \pmod{n}$ admite solução na variável b se, e somente se, existem $b, k \in \mathbb{Z}$ tais que $ab - 1 = nk \iff ab - nk = 1$. Pelo corolário 1.8 do teorema de Bachet-Bézout, isto ocorre se, e só se, $\mathrm{mdc}(a, n) = 1$. $\square$

Cópia eletrônica

Dizemos portanto que a é *invertível* módulo n quando $\mathrm{mdc}(a,n)=1$ e chamamos b com $ab \equiv 1 \pmod{n}$ de *inverso multiplicativo* de a módulo n. O inverso é sempre único módulo n: se $ab \equiv ab' \equiv 1 \pmod{n}$ temos

$$b \equiv b \cdot 1 \equiv b \cdot (ab') \equiv (ba) \cdot b \equiv 1 \cdot b' \equiv b' \pmod{n}.$$

Assim, $\overline{b}$ está bem definido e, em termos de classes de congruência, temos que $\overline{a} \cdot \overline{b} = \overline{1}$; denotamos $\overline{b}$ por $(\overline{a})^{-1}$. Note que pela demonstração da proposição acima calcular $(\overline{a})^{-1}$ é equivalente a resolver a equação diofantina linear $ax + ny = 1$ e para isto podemos utilizar o método do exemplo 1.14.

Definimos o *grupo de unidades* $(\mathbb{Z}/n\mathbb{Z})^\times \subset \mathbb{Z}/n\mathbb{Z}$ do anel de inteiros módulo n como o subconjunto formado pelos elementos invertíveis de $\mathbb{Z}/n\mathbb{Z}$:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{mdc}(a,n) = 1\}.$$

Observe que o produto de elementos de $(\mathbb{Z}/n\mathbb{Z})^\times$ é sempre um elemento de $(\mathbb{Z}/n\mathbb{Z})^\times$. Por exemplo, temos a seguinte tabela de multiplicação em $(\mathbb{Z}/15\mathbb{Z})^\times$:

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{7}$	$\overline{8}$	$\overline{11}$	$\overline{13}$	$\overline{14}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{7}$	$\overline{8}$	$\overline{11}$	$\overline{13}$	$\overline{14}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{8}$	$\overline{14}$	$\overline{1}$	$\overline{7}$	$\overline{11}$	$\overline{13}$
$\overline{4}$	$\overline{4}$	$\overline{8}$	$\overline{1}$	$\overline{13}$	$\overline{2}$	$\overline{14}$	$\overline{7}$	$\overline{11}$
$\overline{7}$	$\overline{7}$	$\overline{14}$	$\overline{13}$	$\overline{4}$	$\overline{11}$	$\overline{2}$	$\overline{1}$	$\overline{8}$
$\overline{8}$	$\overline{8}$	$\overline{1}$	$\overline{2}$	$\overline{11}$	$\overline{4}$	$\overline{13}$	$\overline{14}$	$\overline{7}$
$\overline{11}$	$\overline{11}$	$\overline{7}$	$\overline{14}$	$\overline{2}$	$\overline{13}$	$\overline{1}$	$\overline{8}$	$\overline{4}$
$\overline{13}$	$\overline{13}$	$\overline{11}$	$\overline{7}$	$\overline{1}$	$\overline{14}$	$\overline{8}$	$\overline{4}$	$\overline{2}$
$\overline{14}$	$\overline{14}$	$\overline{13}$	$\overline{11}$	$\overline{8}$	$\overline{7}$	$\overline{4}$	$\overline{2}$	$\overline{1}$

Uma aplicação do inverso multiplicativo é o famoso *teorema de Wilson*. Primeiramente precisamos de um lema.

Lema 1.33. *Se p é primo, então as únicas soluções de $x^2 = \overline{1}$ em $\mathbb{Z}/(p)$ são $\overline{1}$ e $-\overline{1}$. Em particular, se $x \in (\mathbb{Z}/(p))^\times - \{1,-1\}$, então $x^{-1} \neq x$ em $\mathbb{Z}/(p)$.*

Demonstração: Temos

$$\begin{aligned} x^2 \equiv 1 \pmod{p} &\iff p \mid (x^2-1) \iff p \mid (x-1)(x+1) \\ &\iff p \mid x-1 \text{ ou } p \mid x+1 \\ &\iff x \equiv 1 \pmod{p} \text{ ou } x \equiv -1 \pmod{p} \end{aligned}$$

donde o resultado segue. □

Teorema 1.34 (Wilson)**.** *Seja $n > 1$. Então $n \mid (n-1)!+1$ se, e só se, n é primo. Mais precisamente,*

$$(n-1)! \equiv \begin{cases} -1 \pmod{n} & \textit{se } n \textit{ é primo} \\ 0 \pmod{n} & \textit{se } n \textit{ é composto e } n \neq 4. \end{cases}$$

Demonstração: Se n é composto mas não é o quadrado de um primo podemos escrever $n = ab$ com $1 < a < b < n$. Neste caso tanto a quanto b são fatores de $(n-1)!$ e portanto $(n-1)! \equiv 0 \pmod{n}$. Se $n = p^2$, $p > 2$, então p e $2p$ são fatores de $(n-1)!$ e novamente $(n-1)! \equiv 0 \pmod{n}$; isto demonstra que para todo $n \neq 4$ composto temos $(n-1)! \equiv 0 \pmod{n}$.

Se n é primo podemos escrever $(n-1)! \equiv -2 \cdot 3 \cdot \ldots \cdot (n-2) \pmod{n}$; mas pelo lema anterior podemos juntar os inversos aos pares no produto do lado direito, donde $(n-1)! \equiv -1 \pmod{n}$. □

Vejamos uma aplicação do teorema de Wilson.

Teorema 1.35 (Teorema de Wolstenholme)**.** *Seja $p > 3$ um número primo. Então o numerador do número*

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

é divisível por p^2.

Demonstração: Note que somando os "extremos" temos

$$\sum_{1 \leq i \leq p-1} \frac{1}{i} = \sum_{1 \leq i \leq \frac{p-1}{2}} \left(\frac{1}{i} + \frac{1}{p-i} \right) = p \sum_{1 \leq i \leq \frac{p-1}{2}} \frac{1}{i(p-i)}.$$

Como o mmc dos números de 1 a $p-1$ não é divisível por p, basta mostrar que o numerador da última soma é múltiplo de p. Equivalentemente, como $p \nmid (p-1)!$, devemos mostrar que o inteiro

$$S \stackrel{\text{def}}{=} \sum_{1 \leq i \leq \frac{p-1}{2}} \frac{(p-1)!}{i(p-i)}$$

é um múltiplo de p. Para $1 \leq i \leq p-1$, denote por r_i o inverso de i mod p, ou seja, $ir_i \equiv 1 \pmod{p}$. Note que $r_{p-i} \equiv -r_i \pmod{p}$, assim

$$\begin{aligned} S &\equiv \sum_{1 \leq i \leq \frac{p-1}{2}} \frac{(p-1)!}{i(p-i)} \cdot ir_i(p-i)r_{p-i} \\ &\equiv \sum_{1 \leq i \leq \frac{p-1}{2}} (p-1)! r_i r_{p-i} \equiv \sum_{1 \leq i \leq \frac{p-1}{2}} r_i^2 \pmod{p} \end{aligned}$$

pelo teorema de Wilson. Note que como cada r_i é congruente a um dos números $\pm 1, \pm 2, \ldots, \pm \frac{p-1}{2}$, temos que os r_i^2 são congruentes a um dos números $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ módulo p. Vamos mostrar que todos eles aparecem. De fato, se $r_i^2 \equiv r_j^2 \pmod{p}$, então $p \mid (r_i - r_j)(r_i + r_j)$, isto é, $r_i \equiv \pm r_j \pmod{p}$. Multiplicando por ij, temos que $j \equiv \pm i \pmod{p}$, o implica $i = j$ pois $1 \leq i, j \leq \frac{p-1}{2}$.

Assim, $S \equiv \sum_{1 \leq i \leq \frac{p-1}{2}} i^2 \pmod{p}$ e como $\sum_{1 \leq i \leq \frac{p-1}{2}} i^2 = \frac{p(p^2-1)}{24}$ é um múltiplo de p (pois $\text{mdc}(p, 24) = 1$), o resultado segue. □

O teorema de Wilson produz ainda resultados interessantes sobre os coeficientes binomiais. Suponhamos que k e h são inteiros positivos tais que $k + h = p - 1$ onde p é primo. Então

$$\begin{aligned} h!k! &\equiv (-1)^h (p-1)(p-2)\cdots(p-h)k! = (-1)^k (p-1)! \\ &\equiv (-1)^{k+1} \pmod{p}. \end{aligned}$$

Portanto

$$\begin{aligned} & h!k!\binom{p-1}{k} \equiv (p-1)! \pmod{p} \\ \iff & (-1)^{k+1}\binom{p-1}{k} \equiv -1 \pmod{p} \\ \iff & \binom{p-1}{k} \equiv (-1)^k \pmod{p}. \end{aligned}$$

Exemplo 1.36. *Demonstrar que se $p > 3$ é primo, então $p^3 \mid \binom{2p}{p} - 2$.*

Solução: Primeiramente, vamos relembrar algumas identidades com coeficientes binomiais bem conhecidas. Para todo $1 \leq i \leq p-1$, temos

que $\binom{p}{i} = \frac{p}{i}\binom{p-1}{i-1}$ (basta utilizar a definição) enquanto que

$$\binom{2p}{p} = \binom{p}{0}^2 + \binom{p}{1}^2 + \cdots + \binom{p}{p}^2$$

pois podemos escolher p objetos dentre $2p$ escolhendo i objetos dentre os p primeiros e $p-i$ dos p últimos para todo i entre 0 e p, logo

$$\binom{2p}{p} = \sum_{0\le i\le p}\binom{p}{i}\binom{p}{p-i} = \sum_{0\le i\le p}\binom{p}{i}^2.$$

Utilizando estas identidades, temos que

$$\binom{2p}{p} - 2 = \sum_{1\le i\le p-1}\frac{p^2}{i^2}\binom{p-1}{i-1}^2 = p^2\sum_{1\le i\le p-1}\frac{1}{i^2}\binom{p-1}{i-1}^2.$$

Note que $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ é um múltiplo de p para $1 \le i \le p-1$ pois o denominador desta fração não é divisível por p. Assim, $\frac{1}{i^2}\binom{p-1}{i-1}^2 = \frac{1}{p^2}\binom{p}{i}^2$ é inteiro e portanto a soma $\sum_{1\le i\le p-1}\frac{1}{i^2}\binom{p-1}{i-1}^2$ é inteira e devemos mostrar que ela é um múltiplo de p. Para isto observemos que cada $1 \le i \le p-1$ é invertível módulo p; seja r_i tal que $1 \le r_i \le p-1$ e $ir_i \equiv 1 \pmod p$. Pela unicidade de r_i módulo p, temos que os r_i's formam uma permutação de $1, 2, \ldots, p-1$. Assim, como $\binom{p-1}{i-1} \equiv (-1)^{i-1} \pmod p$, temos

$$\begin{aligned}
&\sum_{1\le i\le p-1}\frac{1}{i^2}\binom{p-1}{i-1}^2 \equiv \sum_{1\le i\le p-1}\frac{(ir_i)^2}{i^2}\binom{p-1}{i-1}^2 \pmod p\\
\iff &\sum_{1\le i\le p-1}\frac{1}{i^2}\binom{p-1}{i-1}^2 \equiv \sum_{1\le i\le p-1} r_i^2 = \sum_{1\le i\le p-1} i^2 \pmod p.
\end{aligned}$$

Como $\sum_{1\le i\le p-1} i^2 = \frac{p(p-1)(2p-1)}{6}$ é um múltiplo de p (pois $\mathrm{mdc}(p,6)=1$), a prova acaba. □

Os termos grupo e anel empregados nesta seção estão em conformidade com o jargão usualmente utilizado em Álgebra. *Grupo* é o nome emprestado a um conjunto G juntamente com uma operação binária $\cdot$ (produto) que satisfaz os seguintes três axiomas:

Cópia eletrônica

1. (Associatividade) Para quaisquer $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

2. (Existência de elemento neutro) Existe um elemento $e \in G$ tal que, para todo $a \in G$, $a \cdot e = e \cdot a = a$.

3. (Existência de inverso) Para qualquer elemento $a \in G$ existe um elemento $a^{-1} \in G$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Se, além dos três axiomas acima, o grupo G satisfaz

4. (Comutatividade) Para quaisquer $a, b \in G$, $a \cdot b = b \cdot a$.

então G é chamado de *grupo abeliano*.

Um *anel* é um conjunto A com duas operações binárias $+$ (soma) e $\cdot$ (produto) satisfazendo axiomas que abstraem as propriedades usuais dos inteiros (por exemplo). Estes axiomas são

1. $(A, +)$ é um grupo abeliano com elemento neutro 0.

2. (Associatividade do produto) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ para todo $a, b, c \in A$.

3. (Elemento neutro do produto) Existe um elemento $1 \in A$ tal que $1 \cdot a = a \cdot 1 = a$ para todo $a \in A$.

4. (Distributividade) $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(b + c) \cdot a = b \cdot a + c \cdot a$ para todo $a, b, c \in A$.

Se $a \cdot b = b \cdot a$ para todo $a, b \in A$, dizemos que o anel A é *comutativo*. Um anel comutativo $A \neq 0$ (isto é, $0 \neq 1$ em A) é chamado de *domínio* se, para $a, b \in A$, $a \cdot b = 0 \implies a = 0$ ou $b = 0$. Por outro lado, se um anel comutativo $A \neq 0$ é tal que todo elemento não nulo possui inverso multiplicativo (ou seja, $(A \setminus \{0\}, \cdot)$ é um grupo) então dizemos que o anel A é um *corpo*. Um importante resultado é a seguinte

Proposição 1.37. *O anel $\mathbb{Z}/n\mathbb{Z}$ é um corpo se, e só se, n é primo.*

Demonstração: Temos que $\mathbb{Z}/n\mathbb{Z}$ é um corpo se, e somente se, todo elemento $\overline{a} \neq \overline{0}$ é invertível, ou seja, se e somente se, $\mathrm{mdc}(a, n) = 1$ para todo a com $0 < a < n$. Mas isto é equivalente a n ser primo, pois se n é composto e $a \mid n$ com $1 < a < n$, então $\mathrm{mdc}(a, n) = a \neq 1$. $\square$

Cópia eletrônica