UNIVERSIDADE FEDERAL DO TRIÂNGULO MINEIRO
DEPARTAMENTO DE MATEMÁTICA

Notas de aula de Teoria dos Números

Rafael Peixoto

O material que aqui se encontra são notas de aula para a disciplina de Teoria dos Números do curso de Matemática da UFTM. Todo seu conteúdo é baseado nos livros e arquivos citados na bibliografia. Estas notas de aula também podem ser utilizadas como material complementar a disciplina de Aritmética do PROFMAT.

1 Divisibilidade

1.1 Indução finita

Seja S um subconjunto de $\mathbb{N}$. Dizemos que um número a é o **menor elemento** de S se possui as seguintes propriedades:

i) $a \in S$

ii) Para todo $n \in S$, tem-se que $a \leq n$.

Disto, é imediato verificar que, se S possui um menor elemento, este é único. De fato, se a e b são menores elementos de S, então $a \leq b$ e $b \leq a$, o que implica que $a = b$.

Teorema 1.1 (P.B.O. - Princípio da Boa Ordem)**.** *Todo subconjunto não-vazio dos inteiros positivos* $\mathbb{N}$ *contém um menor elemento.*

Teorema 1.2 (Princípio de Indução Finita)**.** *Seja* B *um subconjunto dos inteiros positivos* $\mathbb{N}$ *com* B *possuindo as seguintes propriedades:*

i) $1 \in B$

ii) $k + 1 \in B$ *sempre que* $k \in B$.

Então, B *contém todos os inteiros positivos.*

Demonstração. Suponha que B não contenha todos os inteiros positivos e que denominamos por A o conjunto dos inteiros positivos não contidos em B, isto é, $A = \mathbb{N}^* \backslash B$. Observe que $A \neq \emptyset$. Assim, pelo P.B.O, existe um elemento mínimo $a \in A$. Agora observe que $a \notin B$ e $a > 1$. Então $a-1 \notin A$, ou seja, $a-1 \in B$. Logo, por (ii), $a = (a-1)+1 \in B$ contradição!. □

Exemplo 1.3. Mostre que $1 + x + x^2 + ... + x^{n-1} = \dfrac{x^n - 1}{x - 1}$, para todo $n \in \mathbb{N}^*$.

De fato, seja B o conjunto dos inteiros positivos para os quais a expressão acima seja verdadeira.

i) $n = 1 \in B$, pois $1 = \dfrac{x-1}{x-1}$

ii) Suponha que $n \in B$, então devemos mostrar que $n + 1 \in B$.

Assim,

$$1+x+x^2+...+x^{n-1}+x^n = \frac{x^n-1}{x-1}+x^n = \frac{x^n-1+x^n(x-1)}{x-1} = \frac{x^{n+1}-x^n+x^n-1}{x-1} = \frac{x^{n+1}-1}{x-1}$$

Portanto $n + 1 \in B$, e pelo princípio de indução, segue que $B = \mathbb{N}^*$, ou seja, a expressão acima é verdadeira para todo $n \in \mathbb{N}^*$.

Exercício 1.4. Mostre que $1 + 2 + 3 + ... + n = \dfrac{n(n+1)}{2}$, para todo $n \in \mathbb{N}$.

Existe outra forma de escrever o princípio de indução finita, esta pode ser dada como segue:

Teorema 1.5 (Princípio de Indução Finita - 2ª versão)**.** *Seja B um subconjunto de inteiros positivos com B possuindo as duas seguintes propriedades:*

i) $1 \in B$

ii) $k + 1 \in B$ *sempre que* $1, 2, ..., k \in B$.

Então B contém os inteiros positivos.

Demonstração. Suponha que B não contenha todos os inteiros positivos e seja A o conjunto dos inteiros positivos não contidos em B, isto é, $A = \mathbb{N}^* \backslash B$. Observe que $A \neq \emptyset$. Assim, pelo P.B.O, existe um elemento mínimo $a \in A$. Então, por (i) e (ii), $1, 2, ..., a-1 \in B$. Logo, por (ii), $a = (a-1)+1 \in B$ contradição!. □

Observação 1.6. O conjunto B no princípio de indução pode ser interpretado como uma afirmação $a(k)$ dependendo de $k \in \mathbb{N}^*$. Assim poderíamos reescrever o teorema acima da seguinte forma:

(Princípio de Indução Finita - 2ª versão) Suponhamos que seja dada uma afirmação $a(k)$ dependendo de $k \in \mathbb{N}^*$ tal que

i) $a(1)$ é verdadeira.

ii) Para cada inteiro $m > 0$, $a(m)$ é verdadeira sempre que $a(1), ..., a(m-1)$ for verdadeira. Então $a(k)$ é verdadeira para todo $k \in \mathbb{N}^*$.

Exemplo 1.7. Mostre que a expressão

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + ... + x + 1)$$

é verdadeira para todo $n \in \mathbb{N}^*$ e $x \geq 1$.

De fato, seja $a(n)$ a afirmação dada acima. Então

i) $a(1)$ é verdade, pois $x - 1 = (x-1)(1)$

ii) Suponha que seja verdadeira as afirmações $a(1), ..., a(k)$. Devemos mostrar que $a(k+1)$ é verdadeira.

De fato,

$$\begin{aligned} x^{k+1} - 1 = & \quad (x+1)(x^k - 1) - (x^k - x) = (x+1)\underbrace{(x^k - 1)}_{a(k)} - x(\underbrace{x^{k-1} - 1}_{a(k-1)}) \\ = & \quad (x+1)(x-1)(x^{k-1} + x^{k-2} + ... + x + 1) - x(x-1)(x^{k-2} + x^{k-3} + ... + x + 1) \\ = & \quad (x-1)(x^k + x^{k-1} + ... + x^2 + x + \underbrace{x^{k-1} + x^{k-2} + ... + x}_{} + 1 \underbrace{-x^{k-1} - x^{k-2} - ... - x^2 - x}_{}) \\ = & \quad (x-1)(x^k + x^{k-1} + ... + x + 1) \end{aligned}$$

ou seja, $a(k+1)$ é verdadeira. Pelo princípio de indução, segue que $a(n)$ é verdadeira para todo $n \in \mathbb{N}^*$.

Exercício 1.8. 1) Mostre que $1^2 + 2^2 + ... + n^2 = \dfrac{n(n+1)(2n+1)}{6}$, para todo $n \in \mathbb{N}^*$.

2) Mostre que $1 + 3 + 5 + ... + (2n-1) = n^2$, para todo $n \in \mathbb{N}^*$.

1.2 Binômio de Newton

Definição 1.9. Sejam $m, k \in \mathbb{N}$ com $k \leq m$. O **coeficiente binomial** $\binom{m}{k}$ é definido por

$$\binom{m}{k} = \frac{m!}{k!(m-k)!} = \frac{m \cdot (m-1) \cdots (m-k+1)}{1 \cdot 2 \cdots k}.$$

Exemplo 1.10. $\binom{5}{3} = \dfrac{5!}{3!2!} = \dfrac{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{3 \cdot 2 \cdot 1 \cdot 2 \cdot 1} = \dfrac{5 \cdot 4}{2 \cdot 1} = 10$

Proposição 1.11. *Sejam $m, k \in \mathbb{N}$ com $k \leq m$. Então,*

1. $\binom{m}{0} = \binom{m}{m} = 1.$
2. $\binom{m}{k} = \binom{m}{m-k}.$
3. $\binom{m}{k} + \binom{m}{k-1} = \binom{m+1}{k}.$

Demonstração. As propriedades (1) e (2) seguem diretamente da definição. Provemos a propriedade (3).

$$\begin{aligned}
\binom{m}{k} + \binom{m}{k-1} &= \frac{m!}{k!(m-k)!} + \frac{m!}{(k-1)!(m-k+1)!} \\
&= \frac{m!}{k!(m-k)!} \cdot \frac{(m-k+1)}{(m-k+1)} + \frac{m!}{(k-1)!(m-k+1)!} \cdot \frac{k}{k} \\
&= \frac{m!(m-k+1)}{k!(m-k+1)!} + \frac{m!k}{(k)!(m-k+1)!} \\
&= \frac{m!(m-k+1+k)}{k!(m-k+1)!} = \frac{m!(m+1)}{k!(m-k+1)!} \\
&= \frac{(m+1)!}{k!(m-k+1)!} = \binom{m+1}{k}
\end{aligned}$$

□

Teorema 1.12 (Binômio de Newton). *Sejam x e y duas variáveis e seja $n \in \mathbb{N}^*$. Então*

$$\begin{aligned}
(x+y)^n &= \tbinom{n}{0}x^n + \tbinom{n}{1}x^{n-1}y^1 + \tbinom{n}{2}x^{n-2}y^2 + ... + \tbinom{n}{n-2}x^2y^{n-2} + \tbinom{n}{n-1}x^1y^{n-1} + \tbinom{n}{n}y^n \\
&= \sum_{k=0}^{n} \binom{n}{k} x^{n-k}y^k.
\end{aligned}$$

Demonstração. Vamos demonstrar usando indução matemática. Para $n = 1$ a fórmula é válida, pois

$$(x+y)^1 = x+y = \binom{1}{0}x^1y^0 + \binom{1}{1}x^0y^1.$$

Vamos supor a validade da fórmula para um determinado n e prová-la para $(n+1)$. Note que

$$\begin{aligned}(x+y)^{n+1} &= (x+y)^n \cdot (x+y)\\ &= \left(\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k\right)\cdot(x+y)\\ &= \sum_{k=0}^{n}\binom{n}{k}x^{n-k+1}y^k + \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^{k+1}\\ &= x^{n+1} + \sum_{k=1}^{n}\binom{n}{k}x^{n-k+1}y^k + \sum_{k=0}^{n-1}\binom{n}{k}x^{n-k}y^{k+1} + y^{n+1}\end{aligned}$$

Note que

$$\sum_{k=0}^{n-1}\binom{n}{k}x^{n-k}y^{k+1} = \sum_{k=1}^{n}\binom{n}{k-1}x^{n-k+1}y^k.$$

Assim,

$$\begin{aligned}(x+y)^{n+1} &= x^{n+1} + \sum_{k=1}^{n}\binom{n}{k}x^{n-k+1}y^k + \sum_{k=1}^{n}\binom{n}{k-1}x^{n-k+1}y^k + y^{n+1}\\ &= x^{n+1} + \sum_{k=1}^{n}\left(\binom{n}{k} + \binom{n}{k-1}\right)x^{n-k+1}y^k + y^{n+1}\\ &= x^{n+1} + \sum_{k=1}^{n}\binom{n+1}{k}x^{n-k+1}y^k + y^{n+1}\\ &= \sum_{k=0}^{n+1}\binom{n+1}{k}x^{n+1-k}y^k.\end{aligned}$$

□

Exemplo 1.13. 1) $(x+y)^2 = x^2 + 2xy + y^2$

2) $(x+y)^3 = x^3 + 3x^2y + 3xy^2 + x^3$

3) $(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$

4) $2^n = \binom{n}{0} + \binom{n}{1} + ... + \binom{n}{n}$.

De fato, pois

$$2^n = (1+1)^n = \sum_{k=0}^{n}\binom{n}{k}1^{n-k}1^k = \binom{n}{0} + \binom{n}{1} + ... + \binom{n}{n}$$

Exercício 1.14. Mostre que $\binom{n}{0} + 2\binom{n}{1} + ... + 2^n\binom{n}{n} = 3^n$, para todo $n \geq 1$.

1.3 Divisibilidade

Definição 1.15. Dados dois números inteiros a e b, dizemos que a **divide** b, e denotamos por $a|b$, quando existir um número inteiro c tal que $b = a \cdot c$. Neste caso, dizemos também que a é um **divisor** de b, ou ainda, que b é um **múltiplo** de a. O número inteiro c é chamado de **quociente** de b por a e denotado por $c = \frac{b}{a}$.

Observe que a notação $a|b$ não representa nenhuma operação em $\mathbb{Z}$, nem representa uma fração. Trata-se de uma sentença que diz ser verdade que existe c tal que $b = ca$. A negação dessa sentença é representada por $a \nmid b$, significando que não existe nenhum número inteiro c tal que $b = ca$. Portanto, temos que $0 \nmid a$, se $a \neq 0$.

Exemplo 1.16. 1) $2|6$, pois $6 = 2 \cdot 3$

2) $-1|5$, pois $5 = (-1) \cdot (-5)$

3) $a|0$, $1|a$ e $a|a$ para todo $a \in \mathbb{Z}$, pois $0 = a \cdot 0$ e $a = a \cdot 1$

4) $3 \nmid 4$, pois não existe $c \in \mathbb{Z}$ tal que $4 = 3c$.

Propriedades 1.17. Sejam $a, b, c \in \mathbb{Z}$. Então,

1) se $a|b$ e $b|c$ então $a|c$.

2) se $a|b$ e $c|d$ então $ac|bd$.

3) se $a|b$ e $a|c$, então $a|(xb + yc)$, para todo $x, y \in \mathbb{Z}$.

4) se $a|b$ então $ac|bc$.

5) se $ab|ac$ e $a \neq 0$ então $b|c$.

6) se $a|b$ e $b \neq 0$ então $|a| \leq |b|$.

7) se $a|b$ e $b|a$ então $|a| = |b|$.

Demonstração. 1) Se $a|b$ e $b|c$ então existem $x, y \in \mathbb{Z}$, tais que $b = xa$ e $c = yb$. Assim, substituindo o valor de b da primeira equação na outra, obtemos $c = yb = y \cdot (xa) = (yx)a$, o que nos mostra que $a|c$.

2) Se $a|b$ e $c|d$, então existem $x, y \in \mathbb{Z}$ tais que $b = xa$ e $d = yc$. Portanto, $bd = (xa)(yc) = (xy)(ac)$. Logo, $ac|bd$.

3) Se $a|b$ e $a|c$ então existem $f, g \in \mathbb{Z}$ tais que $b = fa$ e $c = ga$. Logo,

$$xb + yc = x(fa) + y(ga) = (xf + yg)a,$$

o que prova o resultado.

4) Se $a|b$, então existe $x \in \mathbb{Z}$ tal que $b = xa$. Assim, multiplicando por c ambos os lados da igualdade, temos que $bc = (xa)c = x(ac)$. Portanto $ac|bc$.

5) Se $ab|ac$, então existe $x \in \mathbb{Z}$ tal que $ac = abx$. Logo, $ac - abx = 0$, ou seja, $a(c - bx) = 0$. Como $a \neq 0$, temos que $c - bx = 0$, ou seja, $c = bx$. Portanto, $b|c$.

6) Como $a|b$, existe $x \in \mathbb{Z}$ tal que $b = xa$. Como, por hipótese, $b \neq 0$, então segue que $x \neq 0$, e assim $|x| \geq 1$. Logo, $|b| = |xa| = |x||a| \geq 1 \cdot |a| = |a|$.

7) Suponha que $a|b$ e $b|a$. Se $a = 0$, naturalmente $b = 0$ e assim $|a| = |b| = 0$. Se $a \neq 0$ então $b \neq 0$, pois $b|a$, e da propriedade (4), temos que $|a| \leq |b|$ e $|b| \leq |a|$. Portanto $|a| = |b|$. □

Exemplo 1.18. Os únicos divisores de 1 são 1 e -1. De fato, pois suponha que existe $b \in \mathbb{Z}$ tais que $b|1$. Então segue que $b \neq 0$. Como $1|b$, pois $b = 1 \cdot b$, segue da propriedade (5) que $|b| = |1| = 1$. Logo, da definição de módulo, temos que $b = 1$ ou $b = -1$.

Proposição 1.19. *Sejam $a, b, c \in \mathbb{Z}$ tais que $a|(b \pm c)$. Então $a|b$ se, e somente se, $a|c$.*

Demonstração. Suponhamos que $a|(b + c)$. Logo, existe $x \in \mathbb{Z}$ tal que $b + c = xa$. Agora, se $a|b$, temos que existe $y \in \mathbb{Z}$ tal que $b = ya$. Juntando as duas igualdades acima, temos $ya + c = xa$, donde segue que $c = (x - y)a$. Portanto $a|c$.

A prova da implicação contrária é totalmente análoga.

Por outro lado, se $a|(b - c)$ e $a|b$, pelo caso anterior, temos $a|(-c)$, o que implica que $a|c$. Analogamente, prova-se que se $a|(b - c)$ e $a|c$ então $a|b$. □

Proposição 1.20. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Então*

1) $a - b$ divide $a^n - b^n$.

2) $a + b$ divide $a^{2n+1} + b^{2n+1}$.

3) $a + b$ divide $a^{2n} - b^{2n}$.

Demonstração. Vamos provar estes resultados por indução sobre n.

1) A afirmação é verdade para $n = 1$, pois $a - b$ divide $a^1 - b^1 = a - b$.

Suponhamos, agora, que $a-b|a^n-b^n$. Escrevamos

$$a^{n+1}-b^{n+1}=aa^n\underbrace{-ba^n+ba^n}_{=0}-bb^n=(a-b)a^n+b(a^n-b^n).$$

Como $a-b|a-b$ e, por hipótese de indução, $a-b|a^n-b^n$, decorre da igualdade acima e da Proposição 1.17(3) que $a-b|a^{n+1}-b^{n+1}$. Portanto o resultado segue para todo $n\in\mathbb{N}$.

2) A afirmação é, obviamente, verdade para $n=0$, pois $a+b$ divide $a^1+b^1=a+b$.

Suponhamos, agora, que $a+b|a^{2n+1}+b^{2n+1}$. Então

$$a^{2(n+1)+1}+b^{2(n+1)+1}=a^2a^{2n+1}\underbrace{-b^2a^{2n+1}+b^2a^{2n+1}}_{=0}+b^2b^{2n+1}=(a^2-b^2)a^{2n+1}+b^2(a^{2n+1}+b^{2n+1}).$$

Como $a+b$ divide $a^2-b^2=(a+b)(a-b)$ e, por hipótese de indução, $a+b|a^{2n+1}+b^{2n+1}$, decorre das igualdades acima e da Proposição 1.17(3) que $a+b|a^{2(n+1)+1}+b^{2(n+1)+1}$. Estabelecendo, assim, o resultado para todo $n\in\mathbb{N}$.

3) A afirmação é verdadeira para $n=1$, pois claramente $a+b$ divide $a^2-b^2=(a+b)(a-b)$.

Suponhamos, agora, que $a+b|a^{2n}-b^{2n}$. Então

$$a^{2(n+1)}-b^{2(n+1)}=a^2a^{2n}\underbrace{-b^2a^{2n}+b^2a^{2n}}_{=0}-b^2b^{2n}=(a^2-b^2)a^{2n}+b^2(a^{2n}-b^{2n}).$$

Como $a+b|a^2-b^2$ e, por hipótese de indução, $a+b|a^{2n}-b^{2n}$, decorre das igualdades acima e da Proposição 1.17(3) que $a+b|a^{2(n+1)}+b^{2(n+1)}$. Portanto o resultado segue para todo $n\in\mathbb{N}$. □

Exemplo 1.21. 1) Para todo $n\in\mathbb{N}$, temos que $3|10^n-7^n$, pois $3=10-7$ e da Proposição 1.20(1) $10-7|10^n-7^n$, para todo $n\in\mathbb{N}$.

2) Para todo $n\in\mathbb{N}$, temos que $19|3^{2n+1}+4^{4n+2}$. De fato, $19=3+4^2$ e

$$3^{2n+1}+4^{4n+2}=3^{2n+1}+4^{2(2n+1)}=3^{2n+1}+(4^2)^{2n+1}.$$

Então da Proposição 1.20(2), segue que $3+4^2|3^{2n+1}+(4^2)^{2n+1}$, ou seja, $19|3^{2n+1}+4^{4n+2}$.

3) Para todo $n\in\mathbb{N}$, temos que $53|7^{4n}-2^{4n}$. De fato, $53=7^2+2^2$ e

$$7^{4n}-2^{4n}=7^{2(2n)}-2^{2(2n)}=(7^2)^{2n}-(2^2)^{2n}.$$

Então da Proposição 1.20(3), segue que $7^2+2^2|(7^2)^{2n}-(2^2)^{2n}$, ou seja, $53|7^{4n}-2^{4n}$.

Teorema 1.22 (Algoritmo da Divisão ou Divisão Euclidiana)**.** *Sejam a e b dois números inteiros com $a \neq 0$. Existem dois únicos números inteiros q e r tais que*

$$b = aq + r, \text{ com } 0 \leq r < |a|.$$

Demonstração. Considere o conjunto

$$S = \{b - ay \mid y \in \mathbb{Z}\} \cap \mathbb{N}.$$

Existência: Pela Propriedade Arquimediana, existe $n \in \mathbb{Z}$ tal que $n(-a) > -b$, logo $b - na > 0$, o que mostra que S é não vazio. Pelo princípio da boa ordenação, o conjunto S possui um menor elemento r. Suponhamos então que $r = b - aq$, $q \in \mathbb{Z}$. Sabemos que $r \geq 0$. Vamos mostrar que $r < |a|$. Suponhamos por absurdo que $r \geq |a|$. Então, existe $s \in \mathbb{N}$ tal que $r = |a| + s$, logo $0 \leq s < r$. Mas

$$s = r - |a| = b - aq - |a| = b - (q \pm 1)a \in S,$$

contradizendo o fato de r ser o menor elemento de S. Portanto $r < |a|$, e logo $b = aq + r$, com $0 \leq r < |a|$.

Unicidade: Suponha que $b = aq + r = aq_0 + r_0$, onde $q, q_0, r, r_0 \in \mathbb{Z}$, $0 \leq r < |a|$ e $0 \leq r_0 < |a|$. Assim, temos que $-|a| < -r \leq r_0 - r < |a|$. Logo, $|r_0 - r| < |a|$. Por outro lado, $a(q - q_0) = r_0 - r$, o que implica que

$$|a||q - q_0| = |a(q - q_0)| = |r_0 - r| < |a|,$$

o que só é possível se $q = q_0$ e consequentemente, $r = r_0$. □

Nas condições do teorema acima, os números q e r são chamados, respectivamente, de **quociente** e de **resto** da divisão de b por a.

Do algoritmo da divisão, temos que o resto da divisão de b por a é zero se, e somente se, $a|b$.

Exemplo 1.23. 1) O quociente e o resto da divisão de 19 por 5 são $q = 3$ e $r = 4$, isto é, $19 = 5 \cdot 3 + 4$. O quociente e o resto da divisão de -19 por 5 são $q = -4$ e $r = 1$, isto é, $-19 = 5 \cdot (-4) + 1$.

2) O resto da divisão de 10^n por 9 é sempre 1, qualquer que seja o número natural n.

De fato, pois $9 = 10 - 1$ e da Proposição 1.20(1), $10 - 1 | 10^n - 1^n$, ou seja, existe $q \in \mathbb{Z}$ tal que $10^n - 1 = 9q$. Logo $10^n = 9q + 1$, para todo $n \in \mathbb{N}$.

Observação 1.24. 1) Todo número inteiro n pode ser escrito em uma, e somente uma, das seguintes formas: $2q$ ou $2q + 1$, pois do algoritmo da divisão, existem $q, r \in \mathbb{Z}$ tais que $n = 2q + r$, com $0 \leq r < 2$, ou seja, $r = 0$ ou $r = 1$.

Portanto, os números inteiros se dividem em duas classes, a dos números da forma $2q$ para algum $q \in \mathbb{Z}$, chamados de números **pares**, e a dos números da forma $2q + 1$, chamados de números **ímpares**. A paridade de um número inteiro é o caráter do número ser par ou ímpar. 2) Mais geralmente, fixado um número natural $m > 1$, pode-se sempre escrever um número qualquer n, de modo único, na forma $n = mk + r$, onde $k, r \in \mathbb{Z}$ e $0 \leq r < m$.

Por exemplo, todo número inteiro n pode ser escrito em uma, e somente uma, das seguintes formas: $3k$, $3k + 1$ ou $3k + 2$.

Ou ainda, todo número inteiro n pode ser escrito em uma, e somente uma, das seguintes formas: $4k$, $4k + 1$, $4k + 2$ ou $4k + 3$.

Corolário 1.25 (Teorema de Eudóxius)**.** *Dados dois números inteiros a e b com $a > 0$, existe um número inteiro n tal que*

$$na \leq b < (n + 1)a.$$

Demonstração. Pela divisão euclidiana, temos que existem únicos $q, r \in \mathbb{Z}$ com $0 \leq r < a$, tais que $b = aq + r$. Assim, basta agora tomar $n = q$, pois

$$aq \leq b = aq + r < aq + a = a(q + 1).$$

□

Exemplo 1.26. Determine os múltiplos de 5 que se encontram entre 1 e 253.

Pelo algoritmo da divisão temos que $253 = 5 \cdot 50 + 3$, ou seja, o maior múltiplo de 5 que cabe em 253 é $5 \cdot 50$, onde 50 é o quociente da divisão de 253 por 5. Portanto, os múltiplos de 5 ente 1 e 253 são

$$1 \cdot 5, 2 \cdot 5, 3 \cdot 5, ..., 50 \cdot 5,$$

e, consequentemente, são em número de 50.

Mais geralmente, dados $a, b \in \mathbb{N}$ com $a < b$, o número de múltiplos não nulos de a menores ou iguais a b é igual ao quociente da divisão de b por a.

Exercício 1.27. 1) O resto da divisão do inteiro N por 20 é 8. Qual é o resto da divisão de N por 5?

2) Seja N um número natural. Prove que a divisão de N^2 por 6 nunca deixa resto 2.

Teorema 1.28. *Dados $a, b \in \mathbb{N}$, com $b > 1$, existem únicos números naturais $c_0, c_1, ..., c_n$ menores do que b tais que*

$$a = c_n b^n + c_{n-1} b^{n-1} + ... + c_2 b^2 + c_1 b + c_0$$

Demonstração. Vamos demonstrar o teorema usando a segunda forma do Princípio de Indução Matemática sobre a. Se $a = 0$, ou se $a = 1$, basta tomar $n = 0$ e $c_0 = a$. Supondo o resultado válido para todo natural menor do que a, vamos prová-lo para a. Pela divisão euclidiana, existem únicos q e r únicos tais que $a = bq + r$, com $0 \leq r < b$. Como $q < a$ (verifique!), pela hipótese de indução, segue-se que existem números naturais m e $d_0, d_1, ..., d_m$, com $d_j < b$, para todo $j = 1, ..., m$, tais que

$$q = d_m b^m + ... + d_2 b^2 + d_1 b + d_0.$$

Assim, temos que

$$\begin{aligned} a = & \ bq + r \\ = & \ b(d_m b^m + ... + d_2 b^2 + d_1 b + d_0) + r \\ = & \ d_m b^{m+1} + ... + d_2 b^3 + d_1 b^2 + d_0 b + r, \end{aligned}$$

donde o resultado segue-se pondo $c_0 = r$, $n = m + 1$ e $c_j = d_{j-1}$ para $j = 1, ..., n$.

A unicidade segue-se facilmente das unicidades acima estabelecidas. □

A representação dada no teorema acima é chamada de **expansão relativa à base** b. Quando $b = 10$, essa expansão é chamada **expansão decimal**, e quando $b = 2$, ela toma o nome de **expansão binária**.

Exemplo 1.29. 1) O número 12019, na base 10, é representado por

$$12019 = 1 \cdot 10^4 + 2 \cdot 10^3 + 0 \cdot 10^2 + 1 \cdot 10 + 9$$

2) O número 13, na base 2, é representado por

$$13 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 1$$

A demonstração do Teorema anterior também nos fornece um algoritmo para determinar a expansão de um número qualquer relativamente à base b. Trata-se de aplicar, sucessivamente, a divisão euclidiana, como segue:

$$a = bq_0 + r_0, \quad r_0 < b,$$
$$q_0 = bq_1 + r_1, \quad r_1 < b,$$
$$q_1 = bq_2 + r_2, \quad r_2 < b,$$

e assim por diante. Como $a > q_0 > q_1 > ...$, pelo princípio da boa ordenação, deveremos, em um certo ponto, ter $q_{n-1} < b$ e, portanto, de

$$q_{n-1} = bq_n + r_n,$$

decorre que $q_n = 0$, o que implica $0 = q_n = q_{n+1} = q_{n+2} = ...$, e, portanto, $0 = r_{n+1} = r_{n+2} = ...$

Temos, então, que

$$a = r_n b^n + ... + r_2 b^2 + r_1 b + r_0$$

Utilizamos o símbolo $(r_n r_{n-1} ... r_1 r_0)_b$ para representar a expressão de a na base b. Naturalmente, omitiremos mencioná-la explicitamente, quando trabalharmos com números na base 10. Vamos também denotar $[a]_b = r_n r_{n-1} ... r_1 r_0$.

Exemplo 1.30. 1) Na base 2, temos que $13 = (1101)_2$ e $[13]_2 = 1101$.
O sistema na base 2 é habitualmente utilizado nos computadores

2) Vamos escrever o número 1329 na base 5

$$1329 = 5(265) + 4$$
$$265 = 5(53) + 0$$
$$53 = 5(10) + 3$$
$$10 = 5(2) + 0$$
$$2 = 5(0) + 2$$

Portanto,

$$1329 = 2 \cdot 5^4 + 0 \cdot 5^3 + 3 \cdot 5^2 + 0 \cdot 5^1 + 4 = (20304)_5,$$

isto é, $[1329]_5 = 20304$.

3) Vamos escrever $(1235)_6$ na base 10. Temos

$$(1235)_6 = 1 \cdot 6^3 + 2 \cdot 6^2 + 3 \cdot 6 + 5 = 216 + 72 + 18 + 5 = 311$$

Exercício 1.31. 1) Escreva 855 na base 12.

2) Escreva $(532)_6$ na base 8.

Proposição 1.32 (Critérios de divisibilidade)**.** *Seja $a = r_n r_{n-1}...r_1 r_0$ um número representado no sistema decimal. Então*

a) $2|a$ *se, e somente se* $2|r_0$.

b) $3|a$ *se, e somente se* $3|(r_0 + r_1 + ... + r_n)$.

c) $5|a$ *se, e somente se* $5|r_0$.

d) $9|a$ *se, e somente se* $9|(r_0 + r_1 + ... + r_n)$.

e) $11|a$ *se, e somente se* $11|(r_0 - r_1 + r_2 - ... + (-1)^n r_n)$.

Demonstração. a) Observe que $a = 10(r_n...r_1) + r_0$. Assim, se $2|a$, como $2|10$, segue das propriedades de divisibilidade, que $2|r_0$. Reciprocamente, se $2|r_0$, como $2|10$, segue das propriedades de divisibilidade, que $2|a$.

b) Temos que

$$\begin{aligned} a - (r_n + ... + r_1 + r_0) &= r_n 10^n + ... + r_1 10 + r_0 - (r_n + ... + r_1 + r_0) \\ &= r_n(10^n - 1) + ... + r_1(10 - 1). \end{aligned}$$

Como o termo à direita nas igualdades acima é divisível por 9, via Proposição 1.20, temos, para algum número q, que

$$a = (r_n + ... + r_1 + r_0) + 9q$$

Assim, das propriedades de divisibilidade, segue que $3|a$ se, e somente se $3|(r_0 + r_1 + ... + r_n)$.

c) Análogo ao (a).

d) Análogo ao (b).

e) Temos que

$$a - (r_0 - r_1 + r_2 - ... + (-1)^n r_n) = r_n 10^n + ... + r_1 10 + r_0 - (r_0 - r_1 + r_2 - ... + (-1)^n r_n)$$
$$= r_n(10^n - (-1)^n) + r_{n-1}(10^{n-1} - (-1)^{n-1}) + ... + r_3(10^3 + 1) + r_2(10^2 - 1) + r_1(10 + 1)$$

Da Proposição 1.20 temos que $11|10^{2q} - 1$ e $11|10^{2q+1} + 1$, e logo, das propriedades de divisibilidade, 11 divide o termo à direita nas igualdades acima. Desta forma, existe $k \in \mathbb{Z}$ tal que

$$a = (r_0 - r_1 + r_2 - ... + (-1)^n r_n) + 11k$$

Logo, das propriedades de divisibilidade, segue que $11|a$ se, e somente se $11|(r_0 - r_1 + r_2 - ... + (-1)^n r_n)$. □

Exemplo 1.33. 1) O número 990 é divisível por $2, 3, 5, 9$ e 11, pois $2|0$, $3|(9 + 9 + 0)$, $5|0$, $9|(9 + 9 + 0)$ e $11|(0 - 9 + 9)$.

2) O número 9075 é divisível por 3, 5 e 11, pois $3|(9 + 0 + 7 + 5)$, $5|5$ e $11|(5 - 7 + 0 - 9)$. Porém, nem 2 e nem 9 divide 9075, uma vez que $2 \nmid 5$ e $9 \nmid (9 + 0 + 7 + 5)$.

1.4 Máximo Divisor Comum

Definição 1.34. Dados dois números inteiros a e b, não simultaneamente nulos, diremos que o número inteiro $d \in \mathbb{Z}$ é um **divisor comum** de a e b se $d|a$ e $d|b$.

Exemplo 1.35. Os números $\pm 1, \pm 2, \pm 3$ e ± 6 são os divisores comuns de 12 e 18.

Definição 1.36. Diremos que um número natural d é um **máximo divisor comum** de a e b, não simultaneamente nulos, e indicaremos por $d = \text{mdc}(a, b)$, se possuir as seguintes

propriedades:

i) d é um divisor comum de a e de b, e

ii) d é divisível por todo divisor comum de a e b.

A condição (ii) acima pode ser reescrita como segue:

ii') Se c é um divisor comum de a e b, então $c|d$.

Observação 1.37. Se $d = \text{mdc}(a, b)$ e c é um divisor comum desses números, então $|c|$ divide d e, portanto, $c \leq |c| \leq d$. Isto nos mostra que o máximo divisor comum de dois números é efetivamente o maior dentre todos os divisores comuns desses números.

Em particular, isto nos mostra que, se d e d' são dois mdc de um mesmo par de números, então $d|d'$ e $d'|d$. Da Proposição 1.17 (6), temos que $d \leq d'$ e $d' \leq d$, e, consequentemente, $d = d'$. Ou seja, o mdc de dois números é único.

Exemplo 1.38. 1) $\text{mdc}(12, 18) = 6$;

2) $\text{mdc}(0, a) = |a|$, para todo $a \in \mathbb{Z}^*$.

3) $\text{mdc}(1, a) = 1$, para todo $a \in \mathbb{Z}$.

4) $\text{mdc}(a, a) = |a|$, para todo $a \in \mathbb{Z}^*$.

5) Para todo $a, b \in \mathbb{Z}$, $a \neq 0$, tem-se que $a|b$ se, e somente se, $\text{mdc}(a, b) = |a|$.

De fato, se $a|b$ temos que $|a|$ é um divisor comum de a e b, e, se c é um divisor comum de a e b, então c divide $|a|$, o que mostra que $|a| = \text{mdc}(a, b)$.

Reciprocamente, se $\text{mdc}(a, b) = |a|$, segue-se que $|a|$ divide b, e logo $a|b$.

Exercício 1.39. Dados $a, b \in \mathbb{Z}$ não ambos nulos, mostre que

$$\text{mdc}(a, b) = \text{mdc}(-a, b) = \text{mdc}(a, -b) = \text{mdc}(-a, -b).$$

Teorema 1.40 (Teorema de Bézout)**.** *Se $d = mdc(a, b)$ então existem $x_0, y_0 \in \mathbb{Z}$ tais que $d = ax_0 + by_0$.*

Demonstração. Considere o conjunto

$$I(a, b) = \{ax + by \,|x, y \in \mathbb{Z}\}.$$

Note que se a e b não são simultaneamente nulos, então $I(a,b) \neq \emptyset$, pois temos que $a^2 + b^2 = a \cdot a + b \cdot b \in I(a,b)$. Vamos mostrar que d é o menor elemento positivo de $I(a,b)$, isto é, $d = min\{I(a,b) \cap \mathbb{N}^*\}$..

Sejam $x_0, y_0 \in \mathbb{Z}$ tais que $d' = ax_0 + by_0$ seja o menor inteiro positivo pertencente a $I(a,b)$, isto é, $d' = min\{I(a,b) \cap \mathbb{N}^*\}$. A existência $x_0, y_0 \in \mathbb{Z}$ é garantida pelo Princípio da Boa Ordenação. Vamos provar que $d'|a$ e $d'|b$. Suponha, por absurdo, que $d' \nmid a$. Pelo Divisão Euclidiana, existem $q, r \in \mathbb{Z}$ tais que

$$a = d'q + r, \text{ com } 0 < r < d'.$$

Logo,

$$r = a - d'q = a - (ax_0 + by_0)q = a(\underbrace{1 - qx_0}_{\in\mathbb{Z}}) + (\underbrace{-qy_0}_{\in\mathbb{Z}})b \in I(a,b) \cap \mathbb{N} * .$$

Contradição, pois $0 < r < d'$ e $d' = min\{I(a,b) \cap \mathbb{N}^*\}$. Portanto $d'|a$. De forma análoga se prova que $d'|b$.

Agora, como d é um divisor comum de a e b, existem inteiros $m, n \in \mathbb{Z}$ tais que $a = m \cdot d$ e $b = n \cdot d$. Logo

$$d' = ax_0 + by_0 = (md)x_0 + (nd)y_0 = d(mx_0 + ny_0)$$

o que implica que $d|d'$. Logo, da Proposição 1.17 (6), temos que $0 < d \leq d'$. Mas como $d = \text{mdc}(a,b)$ e $d'|a$ e $d'|b$, segue da definição de mdc, que $d'|d$, e portanto, $d' \leq d$. Logo $d = d'$. □

Observação 1.41. O Teorema acima nos dá uma demonstração da existência do mdc de dois números. Mais ainda, na demostração deste teorema mostramos não apenas que o $\text{mdc}(a,b)$ pode ser expresso como uma combinação linear de a e b, mas que este número é o menor valor positivo dentre todas combinações lineares de a e b.

Lema 1.42 (Lema de Euclides)**.** *Sejam $a, b, n \in \mathbb{Z}$. Então $mdc(a,b) = mdc(a, b - na)$.*

Demonstração. Seja $d = \text{mdc}(a, b - na)$. Como $d|a$ e $d|(b - na)$, segue, das propriedades de divisibilidade, que d divide $b = b - na + na$. Logo, d é um divisor comum de a e b. Suponha agora que c seja um divisor comum de a e b. Logo, c é um divisor comum de a e $b - na$ e, portanto, $c|d$. Isso prova que $d = \text{mdc}(a,b)$. □

Exemplo 1.43. 1) $\text{mdc}(15,12) \overset{LE}{=} \text{mdc}(12, 15-12) = \text{mdc}(12,3) \overset{3|12}{=} 3$

2)
$$\begin{aligned} \text{mdc}(34,14) &\overset{LE}{=} \text{mdc}(14, 34 - 2\cdot 14) = \text{mdc}(14,6) \\ &\overset{LE}{=} \text{mdc}(6, 14 - 2\cdot 6) = \text{mdc}(6,2) \overset{2|6}{=} 2 \end{aligned}$$

3) Dados $a, m \in \mathbb{N}^*$ com $a > 1$, temos que $\text{mdc}\left(\dfrac{a^m-1}{a-1}, a-1\right) = \text{mdc}(a-1, m)$.

De fato, para $m = 1$ igualdade acima é trivialmente verificada. Suponhamos então que $m > 2$. Seja $d = \text{mdc}\left(\dfrac{a^m-1}{a-1}, a-1\right)$. Do exemplo 1.3 temos

$$\frac{a^m-1}{a-1} = a^{m-1} + a^{m-2} + ... + a^2 + a + 1$$

e logo,

$$\begin{aligned} d = &\ \text{mdc}(a^{m-1} + a^{m-2} + ... + a^2 + a + 1, a-1) \\ = &\ \text{mdc}\left((a^{m-1}-1) + (a^{m-2}-1) + ... + (a^2-1) + (a-1) + m, a-1\right). \end{aligned}$$

Como, pela Proposição 1.20 (a), temos que

$$a-1 | (a^{m-1}-1) + (a^{m-2}-1) + ... + (a-1),$$

segue-se que $(a^{m-1}-1) + (a^{m-2}-1) + ... + (a-1) = n(a-1)$ para algum $n \in \mathbb{Z}$, e, portanto, pelo Lema de Euclides, tem-se que

$$d = \text{mdc}(n(a-1)+m, a-1) = \text{mdc}(a-1, n(a-1)+m) \overset{LE}{=} \text{mdc}(a-1, m).$$

Teorema 1.44. *Sejam $a, b, q, r \in \mathbb{Z}$ tais que $b = aq + r$. Então $mdc(a,b) = mdc(a,r)$.*

Demonstração. Como $b = aq + r$, segue do Lema de Euclides que

$$\text{mdc}(a,b) = \text{mdc}(a, r + aq) \overset{LE}{=} \text{mdc}(a,r).$$

□

Segue do teorema acima que se q e r são respectivamente o quociente e o resto da divisão de b por a, então o problema de se encontrar o $\text{mdc}(a,b)$ reduz-se a encontrar o $\text{mdc}(a,r)$.

Naturalmente, pode-se repetir este processo, fazendo divisões sucessivas, isto é,

$$\begin{aligned}
b &= aq_1 + r_1, & 0 \leq r_1 < |a| \\
a &= r_1q_2 + r_2, & 0 \leq r_2 < r_1 \\
r_1 &= r_2q_3 + r_3, & 0 \leq r_3 < r_2 \\
&\vdots & \vdots \\
r_{n-2} &= r_{n-1}q_n + r_n, & 0 \leq r_n < r_{n-1} \\
r_{n-1} &= r_nq_{n+1}
\end{aligned}$$

Como o resto diminui a cada passo, pelo Princípio da Boa Ordem, o processo não pode cair indefinidamente. Logo, para algum n, temos que $r_n|r_{n-1}$. Assim,

$$\text{mdc}(a,b) = \text{mdc}(a,r_1) = \text{mdc}(r_1,r_2) = ... = \text{mdc}(r_{n-2},r_{n-1}) = \text{mdc}(r_{n-1},r_n) = r_n,$$

pois $r_n|r_{n-1}$. Portanto, $\text{mdc}(a,b) = r_n$, ou seja, o máximo divisor comum de a e b é o último resto diferente de zero. Tal método é chamado de **Algoritmo de Euclides**.

O algoritmo acima pode ser sintetizado e realizado na prática, como mostraremos a seguir.

Inicialmente, efetuamos a divisão $b = aq_1 + r_1$ e colocamos os números envolvidos no seguinte diagrama:

	q_1	
b	a	
r_1		

A seguir, continuamos efetuando a divisão $a = r_1q_2 + r_2$ e colocamos os números envolvidos no diagrama

	q_1	q_2	
b	a	r_1	
r_1	r_2		

Prosseguindo, enquanto for possível, teremos

	q_1	q_2	q_3	$\cdots$	q_{n-1}	q_n	q_{n+1}
b	a	r_1	r_2	$\cdots$	r_{n-2}	r_{n-1}	$r_n = \text{mdc}(a,b)$
r_1	r_2	r_3	r_4	$\cdots$	r_n	0	

Exemplo 1.45. Calcule o mdc$(1128, 336)$.

Utilizando o Algoritmo de Euclides, temos

	3	2	1	4
1128	336	120	96	24
120	96	24	0	

Portanto, mdc$(1128, 336) = 24$.

Observe também que o Algoritmo de Euclides nos fornece um meio prático de escrever o mdc de dois números como soma de dois múltiplos dos números em questão, isto é, este algoritmo possibilita encontrarmos $x_0, y_0 \in \mathbb{Z}$ tais que $\text{mdc}(a, b) = ax_0 + by_0$. De fato, pois isolando os restos na primeira coluna, obtemos a segunda:

$$\begin{aligned}
b = aq_1 + r_1 \quad &\Rightarrow \quad r_1 = b - aq_1 \\
a = r_1q_2 + r_2 \quad &\Rightarrow \quad r_2 = a - r_1q_2 \\
r_1 = r_2q_3 + r_3 \quad &\Rightarrow \quad r_3 = r_1 - r_2q_3 \\
\vdots \quad &\qquad \vdots \\
r_{n-3} = r_{n-2}q_{n-1} + r_{n-1} \quad &\Rightarrow \quad r_{n-1} = r_{n-3} - r_{n-2}q_{n-1} \\
r_{n-2} = r_{n-1}q_n + r_n \quad &\Rightarrow \quad r_n = r_{n-2} - r_{n-1}q_n
\end{aligned}$$

Agora, substituindo cada um dos restos na equação acima, obteremos x_0 e y_0. Por exemplo, suponha que $\text{mdc}(a, b) = r_3$. Então

$$\begin{aligned}
\text{mdc}(a, b) \quad &= \quad r_3 = r_1 - r_2q_3 \overset{r_2=a-r_1q_2}{=} r_1 - (a - r_1q_2)q_3 = r_1(1 + q_2q_3) - aq_3 \\
&\overset{r_1=b-aq_1}{=} (b - aq_1)(1 + q_2q_3) - aq_3 = b(1 + q_2q_3) - a(q_1(1 + q_2q_3) + q_3) \\
&= \quad a(\underbrace{-q_1 - q_1q_2q_3 - q_3}_{x_0}) + b(\underbrace{1 + q_2q_3}_{y_0})
\end{aligned}$$

Exemplo 1.46. Vimos que mdc$(1128, 336) = 24$. Do algoritmo de Euclides, temos

$$\begin{aligned}
1128 = 3 \cdot 336 + 120 \quad &\Rightarrow \quad 120 = 1128 - 3 \cdot 336 \quad (3) \\
336 = 2 \cdot 120 + 96 \quad &\Rightarrow \quad 96 = 336 - 2 \cdot 120 \quad (2) \\
120 = 1 \cdot 96 + 24 \quad &\Rightarrow \quad 24 = 120 - 1 \cdot 96 \quad (1) \\
96 = 4 \cdot 24 &
\end{aligned}$$

Assim,

$$\begin{aligned}\text{mdc}(1128, 336) = \; & 24 \overset{(1)}{=} 120 - 1 \cdot 96 \overset{(2)}{=} 120 - 1 \cdot (336 - 2 \cdot 120) = 120(1 + 2) - 1 \cdot 336 \\ = \; & 3 \cdot 120 - 1 \cdot 336 \overset{(3)}{=} 3 \cdot (1128 - 3 \cdot 336) - 1 \cdot 336 \\ = \; & 3 \cdot 1128 + 336(3 \cdot (-3) - 1) = 1128(\underbrace{3}_{x_0}) + 336(\underbrace{-10}_{y_0})\end{aligned}$$

Exercício 1.47. Para cada par de números naturais a e b dados abaixo, ache $\text{mdc}(a, b)$ e determine números inteiros m e n tais que $\text{mdc}(a, b) = na + mb$.

a) 56 e 72

b) 372 e 162

Vejamos agora algumas propriedades para mdc.

Proposição 1.48. *Quaisquer que sejam $a, b \in \mathbb{Z}$, não ambos nulos e $n \in \mathbb{N}$, temos que $mdc(na, nb) = n \cdot mdc(a, b)$.*

Demonstração. Suponha que $d = \text{mdc}(a, b)$. Então $d|a$ e $d|b$. Logo, das propriedades de divisibilidade, $nd|na$ e $nd|nb$.

Seja $c \in \mathbb{Z}$ tal que $c|na$ e $c|nb$. Como $d = \text{mdc}(a, b)$, do Teorema de Bezout, existem $x, y \in \mathbb{Z}$ tais que $d = ax + by$. Multiplicando esta igualdade por n, temos

$$nd = n(ax + by) = (na)x + (nb)y$$

Como $c|na$ e $c|nb$, das propriedades de divisibilidade, $c|nd$. Portanto, da definição de mdc, temos que $\text{mdc}(na, nb) = nd = n \cdot \text{mdc}(a, b)$. □

Exemplo 1.49. $\text{mdc}(56, 72) = \text{mdc}(8 \cdot 7, 8 \cdot 9) = 8 \cdot \text{mdc}(7, 9) = 8 \cdot 1 = 8$.

Corolário 1.50. *Sejam $a, b \in \mathbb{Z}$ não ambos nulos. Se $mdc(a, b) = d$ então $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.*

Demonstração. Pela proposição anterior, temos

$$d = \text{mdc}(a, b) = \text{mdc}\left(\frac{ad}{d}, \frac{bd}{d}\right) = \text{mdc}\left(d\frac{a}{d}, d\frac{b}{d}\right) = d \cdot \text{mdc}\left(\frac{a}{d}, \frac{b}{d}\right).$$

Logo $\text{mdc}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. □

Definição 1.51. Dois números inteiros a e b são ditos **primos entre si**, ou **coprimos**, se $\text{mdc}(a, b) = 1$, ou seja, se o único divisor comum positivo de ambos é 1.

Exemplo 1.52. 1) 3 e 5 são coprimos, pois $\text{mdc}(3, 5) = 1$.

2) 40 e 27 são coprimos, pois $\text{mdc}(40, 27) = 1$

Proposição 1.53. *Dois números inteiros a e b são primos entre si se, e somente se, existem números inteiros n e m tais que $na + mb = 1$.*

Demonstração. ($\Rightarrow$) Segue imediatamente da definição de coprimos e do teorema de Bézout. ($\Leftarrow$) Suponha que existam números inteiros n e m tais que $na + mb = 1$. Se $d = \text{mdc}(a, b)$, temos que $d|(na + mb)$, o que mostra que $d|1$, e, portanto, $d = 1$. □

Teorema 1.54. *Sejam $a, b, c \in \mathbb{Z}$. Se $a|bc$ e $mdc(a, b) = 1$, então $a|c$.*

Demonstração. Se $a|bc$, então existe $k \in \mathbb{Z}$ tal que $bc = ak$. Como $\text{mdc}(a, b) = 1$, pela proposição anterior, temos que existem $m, n \in \mathbb{Z}$ tais que $na + mb = 1$. Assim, multiplicando por c ambos os lados da igualdade, temos que $c = nac + mbc$. Substituindo bc por ak nesta última igualdade, temos

$$c = nac + mak = a(nc + mk)$$

Portanto $a|c$. □

Exemplo 1.55. Suponha que $4|7x$, para algum $x \in \mathbb{Z}$. Como $\text{mdc}(4, 7) = 1$, então temos que $4|x$.

Corolário 1.56. *Sejam $a, b, c \in \mathbb{Z}$, com a e b não ambos nulos, e seja $d = mdc(a, b)$. Então $a|c$ e $b|c$ se, e somente se, $\frac{ab}{d}|c$.*

Demonstração. ($\Rightarrow$) Como $a|c$ e $b|c$, então existem $m, n \in \mathbb{Z}$ tais que $c = am$ e $c = bn$. Logo $am = bn$. Como $d|a$ e $d|b$, temos que $\frac{a}{d}m = \frac{b}{d}n$. Logo $\frac{b}{d}|\frac{a}{d}m$. Mas, do corolário 1.50, temos $\text{mdc}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Assim, do teorema anterior, segue que $\frac{b}{d}|m$, o que implica que $a\frac{b}{d}|am$, isto é, $\frac{ab}{d}|c$.
($\Leftarrow$) Como $\frac{ab}{d}|c$ e, $d|a$ e $d|b$, existe $m \in \mathbb{Z}$ tal que $c = \frac{ab}{d}m$. Logo $c = a\left(\frac{b}{d}m\right)$ e portanto $a|c$. Temos também que $c = b\left(\frac{a}{d}m\right)$ e, portanto $b|c$. □

Observação 1.57. Observe que se $\text{mdc}(a, b) = 1$, então pelo resultado anterior, temos

$$a|c \text{ e } b|c \Longleftrightarrow ab|c.$$

A noção de mdc pode ser generalizada.

Definição 1.58. Um número natural d será dito **máximo divisor comum** de dados números inteiros $a_1, ..., a_n$, não todos nulos, se possuir as seguintes propriedades:

i) d é um divisor comum de $a_1, ..., a_n$.

ii) Se c é um divisor comum de $a_1, ..., a_n$, então $c|d$.

O mdc, quando existe, é certamente único e será representado por

$$\text{mdc}(a_1, ..., a_n).$$

Proposição 1.59. *Dados números inteiros $a_1, ..., a_n$, não todos nulos, existe o seu mdc e*

$$mdc(a_1, ..., a_n) = mdc(a_1, ..., a_{n-2}, mdc(a_{n-1}, a_n)).$$

Demonstração. Vamos provar a proposição por indução sobre n ($n \geq 2$). Para $n = 2$, sabemos que o resultado é válido. Suponha que o resultado vale para n, isto é, que se pode encontrar o mdc de n números. Para provar que o resultado é válido para $n + 1$, basta mostrar que

$$\text{mdc}(a_1, ..., a_n, a_{n+1}) = \text{mdc}(a_1, ..., a_{n-1}, \text{mdc}(a_n, a_{n+1})),$$

pois isso provará também a existência.

Pela hipótese de indução, seja $d = \text{mdc}(a_1, ..., a_{n-1}, \text{mdc}(a_n, a_{n+1}))$. Logo, $d|a_1, ..., d|a_{n-1}$ e $d|\text{mdc}(a_n, a_{n+1})$. Portanto, $d|a_1, ..., d|a_{n-1}$, $d|a_n$ e $d|a_{n+1}$. Por outro lado, seja c um divisor comum de $a_1, ..., a_n, a_{n+1}$. Logo, c é um divisor comum de $a_1, ..., a_{n-1}$ e $\text{mdc}(a_n, a_{n+1})$; e, portanto, $c|d$. Logo $d = \text{mdc}(a_1, ..., a_n, a_{n+1})$.

Assim, o resultado segue do Princípio de Indução Finita. □

Observação 1.60. Para calcular o número $\text{mdc}(a_1, ..., a_n)$, pode-se usar recursivamente o Algoritmo de Euclides.

Exemplo 1.61. Calcule $\text{mdc}(1128, 852, 336)$.

Pelo resultado anterior, temos que

$$\mathrm{mdc}(1128, 852, 336) = \mathrm{mdc}(\underbrace{\mathrm{mdc}(1128, 336)}_{24}, 852) = \mathrm{mdc}(24, 852) = 12.$$

	35	2
852	24	12
12	0	

Exercício 1.62. Verifique que $\mathrm{mdc}(96, 1974, 858) = 6$.

1.5 Mínimo Múltiplo Comum

Definição 1.63. Sejam a e b inteiros não-nulos. Dizemos que um inteiro c é um **múltiplo comum** de a e b se $a|c$ e $b|c$.

Em qualquer caso, os números ab e 0 são sempre múltiplos comuns de a e b.

Definição 1.64. Diremos que um número natural m é um **mínimo múltiplo comum** dos números inteiros a e b, ambos não-nulos, e indicaremos por $m = \mathrm{mmc}(a, b)$, se possuir as seguintes propriedades:

i) m é um múltiplo comum de a e b, e

ii) se c é um múltiplo comum de a e b, então $m|c$.

Exemplo 1.65. 12 é um múltiplo comum de 2 e 3, mas não é um mmc destes números. O número 6 é um mmc de 2 e 3.

Observação 1.66. Se m e m' são dois mínimos múltiplos comuns de a e b, então, do item (ii) da definição acima, temos que $m|m'$ e $m'|m$. Como m e m' são números naturais, temos que $m \leq m'$ e $m' \leq m$. Logo $m = m'$, o que mostra que o mínimo múltiplo comum, se existe, é único e é o menor dos múltiplos comuns positivos de a e b.

Proposição 1.67. *Sejam a e b dois números inteiros, ambos não nulos. Então $mmc(a, b)$ existe e*

$$mmc(a, b) \cdot mdc(a, b) = |ab|.$$

Demonstração. Seja $m = \dfrac{|ab|}{d}$, onde $d = \text{mdc}(a, b)$. Como $m = |a|\dfrac{|b|}{d} = |b|\dfrac{|a|}{d}$, temos que $a|m$ e $b|m$. Agora, seja c um múltiplo comum de a e b, isto é, $a|c$ e $b|c$. Então, do Corolário 1.56, temos que $\dfrac{ab}{d}|c$. Logo $m|c$. Portanto, da definição de mmc, temos que $m = \text{mmc}(a, b)$. □

Exemplo 1.68. Calcule $\text{mmc}(1128, 336)$.

Por um exemplo anterior, vimos que $\text{mdc}(1128, 336) = 24$. Assim, da Proposição anterior, temos

$$\text{mmc}(1128, 336) = \frac{1128 \cdot 336}{\text{mdc}(1128, 336)} = \frac{379008}{24} = 15792$$

Exercício 1.69. Calcule $\text{mmc}(56, 72)$ e $\text{mmc}(372, 162)$.

Corolário 1.70. *Se a e b são números inteiros primos entre si, então $mmc(a, b) = |ab|$.*

Demonstração. Se a e b são números inteiros primos entre si, então $\text{mdc}(a, b) = 1$, e da proposição anterior, segue que $\text{mmc}(a, b) \cdot 1 = |ab|$. □

Exemplo 1.71. Para todo $n \in \mathbb{Z}$, $n \neq 0, -1$, calcule $\text{mmc}(n, n + 1)$ e $\text{mmc}(2n - 1, 2n + 1)$.

Vamos calcular o $\text{mmc}(n, n + 1)$. Pela Proposição 1.67, temos que

$$\text{mmc}(n, n + 1) = \frac{|n \cdot (n + 1)|}{\text{mdc}(n, n + 1)}$$

Mas, pelo lema de Euclides, $\text{mdc}(n, n+1) = \text{mdc}(n, 1) = 1$. Logo, $\text{mmc}(n, n+1) = n \cdot (n+1)$.

Vamos agora calcular $\text{mmc}(2n - 1, 2n + 1)$. Pela Proposição 1.67, temos que

$$\text{mmc}(2n - 1, 2n + 1) = \frac{|(2n - 1) \cdot (2n + 1)|}{\text{mdc}(2n - 1, 2n + 1)}$$

Mas, pelo lema de Euclides,

$$\text{mdc}(2n - 1, 2n + 1) = \text{mdc}(2n - 1, 2n - 1 + 2) = \text{mdc}(2n - 1, 2) = \text{mdc}(-1, 2) = 1,$$

logo $\text{mmc}(2n - 1, 2n + 1) = |(2n - 1) \cdot (2n + 1)| = 4n^2 - 1$.

Exercício 1.72. Para todo $n \in \mathbb{Z}$, $n \neq 0, -1$, calcule $\text{mmc}(2n, 2n + 2)$ e $\text{mmc}(kn, k(n + 1))$, onde $k \in \mathbb{Z}^*$.

Podemos também estender a noção de mmc para vários números.

Definição 1.73. Um número natural m é o **mínimo múltiplo comum** de dados números inteiros $a_1, ..., a_n$, não todos nulos, se possuir as seguintes propriedades:

i) m é um múltiplo comum de $a_1, ..., a_n$.

ii) Se c é um múltiplo comum de $a_1, ..., a_n$, então $m|c$.

O mmc de $a_1, ..., a_n$ será representado por $\text{mmc}(a_1, ..., a_n)$.

Proposição 1.74. *Dados números inteiros $a_1, ..., a_n$, não todos nulos, existe o seu mmc e*

$$mmc(a_1, ..., a_n) = mmc(a_1, ..., a_{n-2}, mmc(a_{n-1}, a_n)).$$

Demonstração. Vamos provar a proposição por indução sobre n ($n \geq 2$). Para $n = 2$, sabemos que o resultado é válido. Suponha que o resultado vale para n, isto é, que se pode encontrar o mmc de n números. Para provar que o resultado é válido para $n + 1$, basta mostrar que

$$\text{mmc}(a_1, ..., a_n, a_{n+1}) = \text{mmc}(a_1, ..., a_{n-1}, \text{mmc}(a_n, a_{n+1})),$$

pois isso provará também a existência.

Pela hipótese de indução, seja $m = \text{mmc}(a_1, ..., a_{n-1}, \text{mmc}(a_n, a_{n+1}))$. Logo, $a_1, ..., a_{n-1}$ e $\text{mmc}(a_n, a_{n+1})$ dividem m. Como $a_n|\text{mmc}(a_n, a_{n+1})$ e $a_{n+1}|\text{mmc}(a_n, a_{n+1})$, segue que m é um múltiplo comum de $a_1, ..., a_n, a_{n+1}$.

Por outro lado, suponha que c seja um múltiplo comum de $a_1, ..., a_n, a_{n+1}$. Logo, $a_1|c$,...,$a_{n-1}|c$ e da definição de mmc, $\text{mmc}(a_n, a_{n+1})|c$. Daí segue, da definição de mmc, que c é múltiplo de m. Portanto $m = \text{mmc}(a_1, ..., a_n, a_{n+1})$.

Logo o resultado segue do Princípio de Indução Finita. □

Exercício 1.75. Verifique que $\text{mmc}(1128, 852, 336) = 1.121.232$ e $\text{mmc}(96, 1974, 858) = 4.516.512$.

2 Números Primos

2.1 Números Primos

Definição 2.1. Um número inteiro p que só possui como divisores positivos 1 e $|p|$ é chamado de **número primo**.

Note que a definição exclui o 0 (zero), pois este possui infinitos divisores positivos, e também -1 e 1, que possui apenas um divisor positivo. Assim, um número diferente de $-1, 0$ e 1 e que não seja primo é chamado de **composto**.

Exemplo 2.2. Os números $2, 3, 5, 7, 11, 13, 17$ são números primos enquanto os números $4, 6, 8, 9, 10, 12$ são compostos.

Observação 2.3. 1) Da definição, se um número $a \in \mathbb{Z}^*$ é composto, então ele admite um divisor $b \in \mathbb{Z}$ tal que $|b|$ seja diferente de 1 e $|a|$, isto é, um divisor b tal que $1 < |b| < |a|$. Um divisor nestas condições diz-se um **divisor próprio** de a.

2) Dados dois números primos p e q, se $p|q$ então $|p| = |q|$. De fato, como $p|q$ e sendo q primo, temos que $|p| = 1$ ou $|p| = |q|$. Sendo p primo, tem-se que $|p| > 1$, o que acarreta que $|p| = |q|$.

Proposição 2.4. *Sejam $a, b, p \in \mathbb{Z}$, com p primo.*

1) Se $p \nmid a$ então $mdc(a, p) = 1$.

2) Se $p|ab$, então $p|a$ ou $p|b$.

Demonstração. 1) Suponha que $\text{mdc}(a, p) = d$. Então temos que $d|a$ e $d|p$. Como p é primo, temos que $d = |p|$ ou $d = 1$. Mas $d \neq |p|$, pois $p \nmid a$ e, consequentemente, $d = 1$.

2) Suponha que $p|ab$. Se $p|a$ então o resultado segue. Se $p \nmid a$ então $\text{mdc}(a, p) = 1$. Assim, do teorema de Bezout, existem $m, n \in \mathbb{Z}$ tais que $am + np = 1$. Multiplicando por b esta última igualdade, temos que $b = (ab)m + p(bn)$. Como $p|ab$ e $p|p$ segue da propriedades de divisibilidade que $p|b$. □

Corolário 2.5. *Se um número primo p divide um produto $a_1 \cdots a_n$ de números inteiros, então $p|a_k$ para algum $k = 1, ..., n$.*

Demonstração. Segue imediatamente da proposição anterior, usando indução (exercício!). □

Teorema 2.6 (Teorema Fundamental da Aritmética - T.F.A.)**.** *Todo número natural n maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos positivos.*

Demonstração. Usaremos a segunda forma do Princípio de Indução. Se $n = 2$, o resultado é obviamente verificado, pois 2 é primo.

Suponhamos o resultado válido para todo número natural menor do que n e vamos provar que vale para n. Se o número n é primo, nada temos a demonstrar.

Suponhamos, então, que n seja composto. Logo, existem números naturais n_1 e n_2 tais que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1, ..., p_r$ e $q_1, ..., q_s$ tais que $n_1 = p_1 \cdots p_r$ e $n_2 = q_1 \cdots q_s$. Portanto, $n = p_1 \cdots p_r \cdot q_1 \cdots q_s$.

Vamos, agora, provar a unicidade. Suponha que tenhamos $n = p_1 \cdots p_r = q_1 \cdots q_s$, onde os p_i e q_j, $i = 1, ..., r$ e $j = 1, ..., s$, são números primos. Como $p_1 | q_1 \cdots q_s$, segue, do corolário acima, que $p_1 | q_j$ para algum j, e logo, da observação 2.3 (2), $p_1 = q_j$, que, após um reordenamento de $q_1, ..., q_s$, podemos supor que $p_1 = q_1$. Portanto,

$$p_2 \cdots p_r = q_2 \cdots q_s.$$

Como $p_2 \cdots p_r < n$, a hipótese de indução acarreta que $r = s$ e os p_i e q_j são iguais aos pares. □

Teorema 2.7. *Dado um número inteiro $a \neq 0, 1, -1$, existem primos $0 < p_1 < ... < p_r$ e $n_1, ..., n_r \in \mathbb{N}$, univocamente determinados, tais que*

$$a = \pm p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}.$$

Demonstração. Basta observar que $a = \pm|a|$. Como $|a| > 1$, do T.F.A., existem únicos primos $p_1 < ... < p_t$ tais que $|a| = p_1 p_2 \cdots p_t$. Logo,

$$a = \pm|a| = \pm p_1 p_2 \cdots p_t.$$

Agora, agrupando os primos eventualmente repetidos, podemos escrever

$$a = \pm p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}.$$

□

Exemplo 2.8. 1) $42 = 2 \cdot 3 \cdot 7$

2) $-232925 = -(5^2 \cdot 7 \cdot 11^3)$

Observação 2.9. Numa decomposição em fatores primos de dois, ou mais, números inteiros, usaremos o recurso de acrescentar fatores da forma p^0 $(= 1)$, onde p é um número primo qualquer. Assim, dados $a, b \in \mathbb{Z}\backslash\{-1, 0, 1\}$ quaisquer, podemos escrever

$$a = \pm p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r} \text{ e } b = \pm p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r},$$

usando o mesmo conjunto de primos $p_1, ..., p_r$, onde $n_1, ..., n_r, m_1, ..., m_r \in \mathbb{N}$. Por exemplo, os números $2^3 \cdot 3^2 \cdot 7$ e $2^2 \cdot 5 \cdot 13^3$ pode ser escritos respectivamente $2^3 \cdot 3^2 \cdot 5^0 \cdot 7 \cdot 13^0$ e $2^2 \cdot 3^0 \cdot 5 \cdot 7^0 \cdot 13^3$.

Proposição 2.10. *Seja $a = \pm p_1^{n_1} \cdots p_r^{n_r} \in \mathbb{Z}$, com $p_i > 0$, $n_i \in \mathbb{N}, i = 1, ..., r$. Se b é um divisor de a, então*

$$b = \pm p_1^{m_1} \cdots p_r^{m_r},$$

onde $0 \leq m_i \leq n_i$, para $i = 1, ..., r$.

Demonstração. Seja b um divisor de a, e seja p^m a potência de um primo p que figura na decomposição de b em fatores primos. Como $p^m | b$ e $b | a$ temos que $p^m | a$. Logo, da corolário 2.5, p^m divide algum $p_i^{n_i}$, e consequentemente, $p = p_i$ e $m \leq n_i$. □

Exemplo 2.11. Os divisores de $60 = 2^2 \cdot 3 \cdot 5$ são $\pm 2^0 \cdot 3^0 \cdot 5^0 (= \pm 1)$, $2^1 \cdot 3^0 \cdot 5^0 (= \pm 2)$, $\pm 2^2 \cdot 3^0 \cdot 5^0 (= \pm 4)$, $\pm 2^0 \cdot 3^1 \cdot 5^0 (= \pm 3)$, $\pm 2^0 \cdot 3^0 \cdot 5^1 (= \pm 5)$, $\pm 2^1 \cdot 3^1 \cdot 5^0 (= \pm 6)$, $\pm 2^1 \cdot 3^0 \cdot 5^1 (= \pm 10)$, $\pm 2^2 \cdot 3^1 \cdot 5^0 (= \pm 12)$, $\pm 2^0 \cdot 3^1 \cdot 5^1 (= \pm 15)$, $\pm 2^2 \cdot 3^0 \cdot 5^1 (= \pm 20)$, $\pm 2^1 \cdot 3^1 \cdot 5^1 (= \pm 30)$, $\pm 2^2 \cdot 3^1 \cdot 5^1 (\pm 60)$.

Exercício 2.12. Mostre que um número natural $a > 1$ escrito na forma $a = p_1^{n_1} \cdots p_r^{n_r}$ é um quadrado perfeito se, e somente se, cada expoente n_i é par.

Uma maneira de determinar o número de divisores positivos de um dado número, é dado a seguir:

Proposição 2.13. *Seja $a = \pm p_1^{n_1} \cdots p_r^{n_r}$ a decomposição em primos de $a \in \mathbb{Z}$. Então o número de divisores positivos de a é dado por*

$$d(a) = (n_1 + 1) \cdot (n_2 + 1) \cdots (n_r + 1).$$

Demonstração. Pela proposição 2.10, temos que todos os divisores positivos de a são da forma

$$b = p_1^{m_1} \cdots p_r^{m_r}, \text{ onde } 0 \leq m_i \leq n_i,\ i = 1, ..., n.$$

Note que, conforme esse critério, os divisores positivos de a são todos os termos do desenvolvimento do produto

$$S = (P_1^0 + P_1^1 + ... + P_1^{n_1}) \cdot (P_2^0 + P_2^1 + ... + P_2^{n_2}) \cdots (P_r^0 + P_r^1 + ... + P_r^{n_r}) = \sum_{0 \leq m_i \leq n_i} p_1^{m_1} \cdots p_r^{m_r}.$$

Como cada parenteses contém $n_i + 1$ termos, $i = 1, ..., r$, temos que o número total de termos no desenvolvimento é

$$d(a) = (n_1 + 1) \cdot (n_2 + 1) \cdots (n_r + 1).$$

□

Exemplo 2.14. O número $60 = 2^2 \cdot 3 \cdot 5$ possui $d(60) = (2+1) \cdot (1+1) \cdot (1+1) = 12$ divisores positivos.

Exercício 2.15. Determine o número de divisores dos números 96 e 260.

Uma maneira mais simples de se determinar o mdc e o mmc de dois números é dada a seguir.

Teorema 2.16. *Sejam $a = \pm p_1^{n_1} \cdots p_r^{n_r}$ e $b = \pm p_1^{k_1} \cdots p_r^{k_r}$, com $p_i > 0,\ n_i, k_i \in \mathbb{N},\ i = 1, ..., r$. Então*

$$mdc(a, b) = p_1^{\alpha_1} \cdots p_r^{\alpha_r},\ onde\ \alpha_i = min\{n_i, k_i\},$$

$$e$$

$$mmc(a, b) = p_1^{\beta_1} \cdots p_r^{\beta_r},\ onde\ \beta_i = max\{n_i, k_i\}.$$

Demonstração. Provemos primeiro que $\text{mdc}(a, b) = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, onde $\alpha_i = min\{n_i, k_i\}$.

Pelo proposição 2.10, segue $p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ é um divisor comum de a e b. Assim seja c um divisor comum de a e b. Então da proposição 2.10, $c = \pm p_1^{\gamma_1} \cdots p_r^{\gamma_r}$, onde $\gamma_i \leq min\{n_i, k_i\} = \alpha_i$, e portanto, $c | p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Assim, da definição de mdc, segue que $\text{mdc}(a, b) = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.

Agora, provemos que $\text{mmc}(a, b) = p_1^{\beta_1} \cdots p_r^{\beta_r}$, onde $\beta_i = max\{n_i, k_i\}$.

Pelo proposição 2.10, segue $p_1^{\beta_1} \cdots p_r^{\beta_r}$ é um múltiplo comum de a e b. Agora, seja m um múltiplo comum de a e b. Então da proposição 2.10, $m = \pm p_1^{\theta_1} \cdots p_r^{\theta_r}$, onde $\theta_i \geq max\{n_i, k_i\} = \beta_i$, e portanto, $p_1^{\beta_1} \cdots p_r^{\beta_r} | m$. Portanto, da definição de mmc, segue que $\text{mmc}(a, b) = p_1^{\beta_1} \cdots p_r^{\beta_r}$

□

Exemplo 2.17. 1) Calcule $\text{mdc}(1128, 336)$ e $\text{mmc}(1128, 336)$.

Como $1128 = 2^3 \cdot 3 \cdot 47$ e $336 = 2^4 \cdot 3 \cdot 7$, segue do teorema anterior que

$$\text{mdc}(1128, 336) = 2^3 \cdot 3 \cdot 7^0 \cdot 47^0 = 24$$

$$\text{mmc}(1128, 336) = 2^4 \cdot 3 \cdot 7^1 \cdot 47^1 = 15792$$

2) Determine $a, b \in \mathbb{N}$ tais que $\text{mdc}(a, b) = 8$ e $\text{mmc}(a, b) = 48$.

Como $\text{mdc}(a, b) = 8 = 2^3 \cdot 3^0$ e $\text{mmc}(a, b) = 48 = 2^4 \cdot 3$, temos que

$$a = 2^m \cdot 3^n \text{ e } b = 2^p \cdot 3^q, \text{ com } 3 \leq m, p \leq 4 \text{ e } 0 \leq n, q \leq 1$$

Pelo Teorema anterior, $3 = min\{m, p\}$ e $4 = max\{m, p\}$, e $0 = min\{n, q\}$ e $1 = max\{n, q\}$. Assim, temos

- $m = 3 \Rightarrow p = 4$ $\begin{cases} n = 0 \Rightarrow q = 1 \Rightarrow a = 2^3 = 8 \text{ e } b = 2^4 \cdot 3 = 48 \\ \text{ou} \\ n = 1 \Rightarrow q = 0 \Rightarrow a = 2^3 \cdot 3 = 24 \text{ e } b = 2^4 = 16 \end{cases}$
- $m = 4 \Rightarrow p = 3$ $\begin{cases} n = 0 \Rightarrow q = 1 \Rightarrow a = 2^4 = 16 \text{ e } b = 2^3 \cdot 3 = 24 \\ \text{ou} \\ n = 1 \Rightarrow q = 0 \Rightarrow a = 2^4 \cdot 3 = 48 \text{ e } b = 2^3 = 8 \end{cases}$

Exercício 2.18. Usando a caracterização de mdc e mmc de dois números naturais a e b através da fatoração em primos desses números, prove que

$$\text{mdc}(a,b) \cdot \text{mmc}(a,b) = ab.$$

Vamos provar agora que existem infinitos números primos. A prova deste resultado, dada por Euclides, registra, pela primeira vez, o uso de uma demonstração por redução ao absurdo em matemática.

Teorema 2.19. *Existem infinitos números primos*

Demonstração. Suponha que exista apenas um número finito de números primos $p_1, ..., p_r$. Considere agora o número

$$n = p_1 \cdot p_2 \cdots p_r + 1.$$

Pelo T.F.A., o número n possui um fator primo p que, portanto, deve ser um dos $p_1, ..., p_r$ e, consequentemente, divide o produto $p_1 \cdot p_2 \cdots p_r$. Mas, das propriedades de divisibilidade, isto implica que p divide 1, o que é absurdo. □

Proposição 2.20. *Se um número natural $n > 1$ não é divisível por nenhum número primo p tal que $p^2 \leq n$, então ele é primo.*

Demonstração. Suponhamos que n não seja divisível por nenhum número primo p tal que $p^2 \leq n$ e, suponha por absurdo, que n não seja primo. Seja q o menor número primo que divide n. Então $n = q \cdot n_1$, com $q \leq n_1$. Segue daí que $q^2 \leq q \cdot n_1 = n$. Logo, n é divisível por um número primo q tal que $q^2 \leq n$, contradição. □

Este resultado tem uma importante aplicação prática. Ele nos diz que, para testarmos se um número é primo, é suficiente testarmos sua divisibilidade apenas pelos primos menores ou iguais a $\sqrt{n}$. Por exemplo, para verificar se 91 é primo, basta verificar se este é divisível por algum primo menor que $\sqrt{91} \approx 9,54$, ou seja, se 91 é divisível por $2, 3, 5$ ou 7. Neste caso temos que 91 não é primo, pois $91 = 7 \cdot 13$.

Agora, se desejarmos obter uma lista de todos os primos menores que um determinado número, por exemplo 120, devemos excluir dentre os números 2 a 120 aqueles que são múltiplos

dos primos menores que $\sqrt{120} \approx 10,95$, ou seja, devemos excluir os múltiplos de $2, 3, 5$ e 7. Este processo é chamado **Crivo de Eratóstenes**.

	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	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104	105	106	107	108
109	110	111	112	113	114	115	116	117	118	119	120

Todos os números não riscados na lista acima são números primos.

2.2 O Pequeno Teorema de Fermat

Lema 2.21. *Seja $p > 0$ um número primo. Os números binomiais $\binom{p}{i}$, onde $0 < i < p$, são todos divisíveis por p.*

Demonstração. O resultado vale trivialmente para $i = 1$. Portanto, podemos supor que $1 < i < p$. Neste caso,

$$i!|p(p-1)\cdots(p-i+1).$$

Como, $\text{mdc}(i!, p) = 1$, então que $i!|(p-1)\cdots(p-i+1)$. Logo,

$$\binom{p}{i} = p \cdot \frac{(p-1)\cdots(p-i+1)}{i!}.$$

□

Teorema 2.22 (Pequeno Teorema de Fermat)**.** *Dado um número primo $p > 0$, tem-se que p divide o número $a^p - a$, para todo $a \in \mathbb{Z}$.*

Demonstração. Se $p = 2$, temos que $a^2 - a = a(a-1)$ e portanto $2|a^2 - a$. Suponhamos que p é ímpar. Mostremos o caso em que $a \geq 0$, pois se $a < 0$, então $a = -b$, para algum inteiro $b > 0$, e $a^p - a = (-b)^p - (-b) = (-1)^p(b^p) - (-1)(b) = (-1)(b^p - b)$. Neste caso, $p|a^p - a \Leftrightarrow p|b^p - b$. Faremos a demostração por indução sobre a. Se $a = 0$ ou $a = 1$ o resultado segue claramente. Por hipótese de indução, suponha que o resultado seja válido para a, i.e,

$p|a^p - a$ para algum $a > 0$. Mostremos que vale para $a+1$, isto é, $p|(a+1)^p - (a+1)$. Pelo Binômio de Newton, temos

$$\begin{aligned}(a+1)^p - (a+1) &= \binom{p}{0}a^p + \binom{p}{1}a^{p-1} + ... + \binom{p}{p-1}a + \binom{p}{p}1 - (a+1) \\ &(a^p - a) + \binom{p}{1}a^{p-1} + ... + \binom{p}{p-1}a\end{aligned}$$

Como, pelo lema anterior, $p|\binom{p}{i}$, com $1 \leq i \leq p-1$, e pela hipótese de indução, $p|a^p - a$, segue, pelas propriedades de divisibilidade, que $p|(a+1)^p - (a+1)$. □

Exemplo 2.23. Seja $n \in \mathbb{N}$. Então n^9 e n tem o mesmo algarismo da unidade.

De fato, A afirmação acima é equivalente a $10|n^9 - n$. Como $10 = 2 \cdot 5$, e $\text{mdc}(2,5) = 1$, pela observação 1.57, basta mostrar que $2|n^9 - n$ e $5|n^9 - n$.

Como n^9 e n têm a mesma paridade, segue-se que $n^9 - n$ é par. Logo $2|n^9 - n$.

Por outro lado,

$$n^9 - n = n(n^8 - 1) = n(n^4 - 1)(n^4 + 1) = (n^5 - n)(n^4 + 1).$$

Como, pelo P.T.F, $5|n^5 - n$, segue então que $5|n^9 - n$. Portanto, $10|n^9 - n$.

Corolário 2.24. *Sejam $p > 0$ um número primo e $a \in \mathbb{Z}$ tal que $mdc(p,a) = 1$. Então p divide $a^{p-1} - 1$.*

Demonstração. Pelo P.T.F., temos que $p|a^p - a$, isto é, $p|a(a^{p-1} - 1)$. Como $\text{mdc}(a,p) = 1$, segue, das propriedades de mdc, que $p|a^{p-1} - 1$. □

Exercício 2.25. Sejam $a, k \in \mathbb{N}$ tais que $\text{mdc}(a,7) = 1$. Mostre que $7|a^{6k} - 1$.

2.3 Decomposição do Fatorial em Primos

Veremos agora como encontrar a fatoração em números primos de $n!$, onde n é um número natural arbitrário.

Sejam a e b números naturais. Pelo algoritmo da divisão, existem inteiros q e r tais que $a = bq + r$, com $0 \leq r < b$. Vamos designar pelo símbolo $\left[\frac{a}{b}\right]$ o quociente da divisão de a por b, isto é, $\left[\frac{a}{b}\right] = q$.

Observe que se $a < b$ então $\left[\frac{a}{b}\right] = 0$.

Lema 2.26. *Sejam $a, b, c \in \mathbb{N}$. Então*

$$\left\lfloor \frac{\left\lfloor \frac{a}{b} \right\rfloor}{c} \right\rfloor = \left\lfloor \frac{a}{bc} \right\rfloor .$$

Demonstração. Sejam

$$q_1 = \left\lfloor \frac{a}{b} \right\rfloor \text{ e } q_2 = \left\lfloor \frac{\left\lfloor \frac{a}{b} \right\rfloor}{c} \right\rfloor .$$

Logo, $a = bq_1 + r_1$, com $0 \leq r_1 \leq b-1$ e pelo algoritmo da divisão, $\left\lfloor \frac{a}{b} \right\rfloor = q_1 = cq_2 + r_2$, com $0 \leq r_2 \leq c-1$. Assim,

$$a = bq_1 + r_1 = b(cq_2 + r_2) + r_1 = (bc)q_2 + br_2 + r_1.$$

Como $r_1 \leq b-1$ e $r_2 \leq c-1$, temos

$$br_2 + r_1 \leq b(c-1) + b - 1 = bc - 1.$$

Logo, segue que q_2 é o quociente da divisão de a por bc, ou seja, $q_2 = \left\lfloor \frac{a}{bc} \right\rfloor$. □

Dados um número primo p e um número natural m, vamos denotar por $E_p(m)$ o expoente da maior potência de p que divide m, ou seja, o expoente da potência de p que aparece na fatoração de m em fatores primos. Por exemplo, temos que $144 = 2^4 3^2$, assim $E_2(144) = 4$ e $E_3(144) = 2$.

Em particular, $E_p(n!)$ representará a potência de p que aparece na fatoração de $n!$ em fatores primos.

Teorema 2.27. *Sejam n um número natural e p um número primo. Então,*

$$E_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

Demonstração. Note, inicialmente, que a soma acima é finita , pois existe $r \in \mathbb{N}$ tal que $p^i > n$ para todo $i \geq r$. Assim, $\left\lfloor \frac{n}{p^i} \right\rfloor = 0$, se $i \geq r$.

Vamos demonstrar o resultado por indução sobre n. A fórmula vale trivialmente para $n = 1$. Suponha que o resultado vale para qualquer natural m com $m < n$, isto é, $E_p(m!) =$

$\left[\frac{m}{p}\right] + \left[\frac{m}{p^2}\right] + \left[\frac{m}{p^3}\right] + \cdots$. Sabemos que os múltiplos de p entre 1 e n são $p, 2p, 3p, ..., \left[\frac{n}{p}\right] p$, e

$$n! = 1 \cdot 2 \cdot 3 \cdot ... \cdot p \cdot ... \cdot 2p \cdot ... \cdot \left[\frac{n}{p}\right] p \cdot ... \cdot n.$$

Agrupando todos os múltiplos de p e chamando de K o produto restante em $n!$, temos

$$n! = p \cdot 2p \cdot 3p \cdot ... \cdot \left[\frac{n}{p}\right] p \cdot K = p^{\left[\frac{n}{p}\right]} \left(1 \cdot 2 \cdot 3 \cdot ... \cdot \left[\frac{n}{p}\right]\right) \cdot K = K \cdot p^{\left[\frac{n}{p}\right]} \cdot \left[\frac{n}{p}\right]!$$

Assim, como $p \nmid K$, temos

$$E_p(n!) = \left[\frac{n}{p}\right] + E_p(\left[\frac{n}{p}\right]!).$$

Por hipótese de indução, e Lema 2.26 temos que

$$E_p(\left[\frac{n}{p}\right]!) = \left[\frac{\left[\frac{n}{p}\right]}{p}\right] + \left[\frac{\left[\frac{n}{p}\right]}{p^2}\right] + \cdots = \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots,$$

e portanto,

$$E_p(n!) = \left[\frac{n}{p}\right] + E_p(\left[\frac{n}{p}\right]!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

provando o resultado. □

Exemplo 2.28. Determine a decomposição de 10! em fatores primos e descubra com quantos zeros termina a representação decimal desse número.

Para resolvermos o problema, deveremos achar $E_p(10!)$ para todo primo $p < 10$. Assim,

$$\begin{aligned}
E_2(10!) &= \left[\frac{10}{2}\right] + \left[\frac{10}{2^2}\right] + \left[\frac{10}{2^3}\right] + \left[\frac{10}{2^4}\right] = 5 + 2 + 1 + 0 = 8 \\
E_3(10!) &= \left[\frac{10}{3}\right] + \left[\frac{10}{3^2}\right] + \left[\frac{10}{3^3}\right] = 3 + 1 + 0 = 4 \\
E_5(10!) &= \left[\frac{10}{5}\right] + \left[\frac{10}{5^2}\right] = 2 + 0 = 2 \\
E_7(10!) &= \left[\frac{10}{7}\right] + \left[\frac{10}{7^2}\right] = 1 + 0 = 1
\end{aligned}$$

Logo, $10! = 2^8 3^4 5^2 7$.

Agora, como a quantidade de zeros que aparece na representação decimal de 10! é determinada pela quantidade de $2 \cdot 5$ que aparecem na decomposição de 10!, e como há dois fatores iguais a 5 e oito fatores iguais a 2 na decomposição de 10! em fatores primos, vê-se, imediatamente, que 10! termina com dois zeros.

3 Equações Diofantinas Lineares

A resolução de vários problemas de aritmética recai na resolução, em números inteiros, de equações do tipo

$$aX + bY = c, \quad \text{com } a, b, c \in \mathbb{Z}.$$

Tais equações são chamadas **equações diofantinas lineares** em homenagem a Diofanto de Alexandria (aprox. 250 DC).

Nem sempre estas equações possuem solução. Por exemplo, a equação $4X + 6Y = 3$ não possui nenhuma solução nos números inteiros pois, caso contrário, se $a, b \in \mathbb{Z}$ fosse uma solução então teríamos $4a + 6b = 3$, isto é, $2(2a + 3b) = 3$ e logo $2|3$, absurdo!

Assim, começaremos o estudo procurando condições para a existência de soluções.

Proposição 3.1. *Sejam $a, b, c \in \mathbb{Z}$, com a e b não-nulos. A equação $aX + bY = c$ admite solução em $\mathbb{Z}$ se, e somente se, $mdc(a, b)|c$.*

Demonstração. Seja $d = \text{mdc}(a, b)$. Do teorema de Bezout, temos que

$$I(a, b) = \{ax + by \mid x, y \in \mathbb{Z}\} = d\mathbb{Z} \qquad \text{(Exercício!)}$$

onde $d\mathbb{Z} = \{dt \mid t \in \mathbb{Z}\}$. Assim, temos que a equação $aX + bY = c$ possui solução se, e somente se, $c \in I(a, b)$, o que é equivalente a $c \in d\mathbb{Z}$, que por sua vez, é equivalente a $d|c$. □

Observação 3.2. Observe que a equação $aX + bY = c$ é equivalente à equação

$$\frac{a}{d}X + \frac{b}{d}Y = \frac{c}{d},$$

onde $d = \text{mdc}(a, b)$. Note também, do corolário 1.50, que $\text{mdc}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Portanto, podemos nos restringir às equações do tipo

$$aX + bY = c, \text{ com } \text{mdc}(a, b) = 1,$$

que sempre têm soluções.

Teorema 3.3. *Sejam $x_0, y_0 \in \mathbb{Z}$ uma solução da equação $aX + bY = c$, onde $mdc(a, b) = 1$. Então, as soluções x, y em $\mathbb{Z}$ da equação são*

$$x = x_0 + tb, \quad y = y_0 - ta, \quad t \in \mathbb{Z}.$$

Reciprocamente, para todo $t \in \mathbb{Z}$, os valores x, y dados pelas fórmulas acima são soluções da equação.

Demonstração. Sejam $x, y \in \mathbb{Z}$ uma solução de $aX + bY = c$, logo,

$$ax + by = c = ax_0 + by_0.$$

Consequentemente,

$$a(x - x_0) = b(y_0 - y). \qquad (*)$$

Como $\text{mdc}(a, b) = 1$, segue-se que $b|(x - x_0)$. Logo,

$$x - x_0 = bt, \;\; t \in \mathbb{Z} \Rightarrow x = x_0 + bt, \quad t \in \mathbb{Z}.$$

Substituindo a expressão de $x - x_0$ acima em $(*)$, segue-se que

$$a(x - x_0) = b(y_0 - y) \Rightarrow abt = b(y_0 - y) \Rightarrow at = y_0 - y \Rightarrow y = y_0 - at, \;\; t \in \mathbb{Z}.$$

Reciprocamente, $x = x_0 + tb$, $y = y_0 - ta$, com $t \in \mathbb{Z}$, é solução da equação $aX + bY = c$, pois

$$ax + by = a(x_0 + tb) + b(y_0 - ta) = ax_0 + atb + by_0 - bat = ax_0 + by_0 = c.$$

□

Segue do teorema anterior que a equação diofantina $aX + bY = c$, com $\text{mdc}(a, b) = 1$, admite infinitas soluções em $\mathbb{Z}$.

Exemplo 3.4. Resolva a equação $24X + 14Y = 18$.

Como $\text{mdc}(24, 14) = 2$ e $2|18$, segue da proposição 3.1 que a equação $24X + 14Y = 18$ possui solução. Agora, dividindo ambos os membros por $2 = \text{mdc}(24, 14)$, obtemos a equação equivalente $12X + 7Y = 9$.

Vamos então achar uma solução particular $x_0, y_0 \in \mathbb{Z}$ desta última equação. Pelo algoritmo euclidiano, temos

$$\begin{aligned} 12 = 7(1) + 5 \quad &\Rightarrow \quad 5 = 12 - 7(1) \\ 7 = 5(1) + 2 \quad &\Rightarrow \quad 2 = 7 - 5(1) \\ 5 = 2(2) + 1 \quad &\Rightarrow \quad 1 = 5 - 2(2) \end{aligned}$$

Substituindo as equações acima umas nas outras, obtemos

$$1 = 5 - 2(2) = 5 - (7 - 5(1))(2) = 7(-2) + 5(3) = 7(-2) + (3)(12 - 7(1)) = 12(3) + 7(-5)$$

ou seja

$$12(3) + 7(-5) = 1.$$

Multiplicando a última equação por 9, obtemos

$$12(27) + 7(-45) = 9,$$

Logo, $x_0 = 27$ e $y_0 = -45$ é uma solução particular da equação, e consequentemente, do teorema 3.3,l as soluções são

$$x = 27 + 7t, \;\; y = -45 - 12t, \text{ com } t \in \mathbb{Z}.$$

Exemplo 3.5. Encontre as soluções positivas da equação $11X + 7Y = 58$.

Como $\text{mdc}(11, 7) = 1$ temos que a equação dada admite soluções. Para encontra-las, considere o algoritmo euclidiano,

$$\begin{aligned} 11 = 7(1) + 4 &\;\Rightarrow\; 4 = 11 - 7(1) \\ 7 = 4(1) + 3 &\;\Rightarrow\; 3 = 7 - 4(1) \\ 4 = 3(1) + 1 &\;\Rightarrow\; 1 = 4 - 3(1) \end{aligned}$$

Substituindo as equações acima umas nas outras, obtemos

$$1 = 4 - 3 = 4 - (7 - 4) = 4(2) - 7 = (2)(11 - 7) - 7 = 11(2) + 7(-3).$$

Portanto, multiplicando por 58, temos

$$58 = 11(116) + 7(-174)$$

Logo $x_0 = 116$ e $y_0 = -174$ são soluções particulares da equação dada, e portanto, são soluções

$$x = 116 + 7t, \;\; y = -174 - 11t, \text{ com } t \in \mathbb{Z}.$$

Como estamos interessados nas soluções positivas, então

$$x = 116 + 7t > 0 \text{ e } y = -174 - 11t > 0.$$

Logo, $t > -\dfrac{116}{7} \geq -17$ e $t < -\dfrac{174}{11} \leq -15$, ou seja, $t = -16$. Assim, $x = 4$ e $y = 2$ é a única solução positiva.

Observação 3.6. Seja $d = \text{mdc}(a, b)$, como a equação diofantina $aX + bY = c$ é equivalente à equação

$$\frac{a}{d}X + \frac{b}{d}Y = \frac{c}{d}, \tag{1}$$

e que $\text{mdc}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, segue do teorema 3.3, que a equação (1), possui solução da forma

$$x = x_0 + t\left(\frac{b}{d}\right), \quad y = y_0 - t\left(\frac{a}{d}\right), \quad t \in \mathbb{Z}.$$

as quais também é solução da equação $aX + bY = c$.

Exercício 3.7. Resolva as equações $15X + 12Y = 14$ e $56X + 72Y = 40$.

4 Congruências

4.1 Congruências

Definição 4.1. Seja m um número natural diferente de zero. Diremos que dois números inteiros a e b são **congruentes** módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se

$$a \equiv b \mod m.$$

Para indicar que a e b não são congruentes, ou que são *incongruentes*, módulo m, escreveremos, $a \not\equiv b \mod m$.

Exemplo 4.2. 1) $7 \equiv 11 \mod 4$, pois $7 = 4(1) + 3$ e $11 = 4(2) + 3$.

2) $10 \equiv 0 \mod 5$, pois $10 = 5(2) + 0$ e $0 = 5(0) + 0$.

3) $6 \not\equiv 4 \mod 3$, pois $6 = 3(2) + 0$ e $4 = 3(1) + 1$.

Observação 4.3. Como o resto da divisão de um número inteiro qualquer por 1 é sempre nulo, temos que $a \equiv b \mod 1$, quaisquer que sejam $a, b \in \mathbb{Z}$. Isto torna desinteressante a aritmética dos restos módulo 1. Portanto, doravante, consideraremos sempre $m > 1$.

Proposição 4.4. *Sejam $a, b, m \in \mathbb{Z}$, com $m > 1$. Então $a \equiv b \mod m$ se, e somente se, $m|b - a$.*

Demonstração. Sejam $a = mq + r$, com $0 \leq r < m$ e $b = mt + s$, com $0 \leq s < m$, as divisões euclidianas de a e b por m, respectivamente. Logo,

$$a - b = mq + r - (mt + s) = m(q - t) + (r - s).$$

Portanto, se $a \equiv b \mod m$ então $r = s$ e logo $r - s = 0$, e portanto, $m|a - b$. Agora, se $m|a - b$, como $m|m(q - t)$, segue das propriedades de divisibilidade que $m|r - s$, mas como $0 \leq |r - s| < m$, segue que $r - s = 0$. Logo $r = s$, e portanto $a \equiv b \mod m$. □

Observação 4.5. Note que todo número inteiro é congruente módulo m ao seu resto pela divisão euclidiana por m, isto é,

$$a \equiv r \mod m \Leftrightarrow a = mq + r, \text{ com } 0 \leq r < m.$$

Logo, r é chamado de **resíduo** de a módulo m. Note que todo número inteiro é congruente módulo m a um dos números $0, 1, ..., m-1$. Além disso, dois quaisquer desses números inteiros não são congruentes módulo m.

Proposição 4.6. *Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$. Então valem as seguintes propriedades:*

1. $a \equiv a \mod m$.
2. *Se* $a \equiv b \mod m$ *então* $b \equiv a \mod m$.
3. *Se* $a \equiv b \mod m$ *e* $b \equiv c \mod m$ *então* $a \equiv c \mod m$.
4. *Se* $a \equiv b \mod m$ *e* $c \equiv d \mod m$ *então* $a + c \equiv b + d \mod m$.
5. $a \equiv b \mod m$ *se, e somente se,* $a + c \equiv b + c \mod m$.
6. *Se* $a \equiv b \mod m$ *e* $c \equiv d \mod m$ *então* $ac \equiv bd \mod m$.
7. *Se* $a \equiv b \mod m$ *então* $a^n \equiv b^n \mod m$, *para todo* $n \in \mathbb{N}$.

Demonstração. As propriedades (1) e (2) são de demostração imediata e ficam de exercício.

3) Se $a \equiv b \mod m$ e $b \equiv c \mod m$ então $m|a - b$ e $m|b - c$. Logo, $m|(a - b) + (b - c)$, ou seja, $m|a - c$. Portanto, $a \equiv c \mod m$.

4) Se $a \equiv b \mod m$ e $c \equiv d \mod m$ então $m|a-b$ e $m|c-d$. Logo, $m|(a-b)+(c-d)$, ou seja, $m|(a+c)-(b+d)$. Logo, $a+c \equiv b+d \mod m$.

5) ($\Rightarrow$) Segue dos itens (4) e (1).

($\Leftarrow$) Se $a+c \equiv b+c \mod m$, então $m|(a+c)-(b+c)$. Logo $m|a-b$, isto é, $a \equiv b \mod m$.

6) Se $a \equiv b \mod m$ e $c \equiv d \mod m$ então $m|a-b$ e $m|c-d$. Agora, note que

$$bd - ac = d(b-a) + a(d-c).$$

Então, das propriedades de divisibilidade, temos que $m|ac-bd$. Logo, $ac \equiv bd \mod m$.

7) Se $a \equiv b \mod m$ então $m|a-b$. Mas das propriedades de divisibilidade, $a-b|a^n-b^n$ para todo $n \in \mathbb{N}$, logo, $m|a^n-b^n$ para todo $n \in \mathbb{N}$. Portanto, $a^n \equiv b^n \mod m$, para todo $n \in \mathbb{N}$.

□

Exemplo 4.7. 1) Vamos determinar o resto da divisão de 5^{60} por 26.

Do algorítmo da divisão, temos que $5^{60} = 26q + r$, com $0 \leq r < 26$. Assim, basta encontrarmos o inteiro r com $0 \leq r \leq 25$ tal que $5^{60} \equiv r \mod 26$.
Observe que $5^2 = 25 \equiv (-1) \mod 26$. Logo $5^4 = (25)^2 \equiv (-1)^2 \mod 26$, isto é, $5^4 \equiv 1 \mod 26$.
Agora, note que $60 = 4 \cdot 15$, assim,

$$5^{60} = 5^{4 \cdot 15} = (5^4)^{15} \equiv (1)^{15} \equiv 1 \mod 26.$$

Portanto, o resto da divisão de 5^{60} por 26 é 1.

2) Vamos determinar o algarismo das unidades de 9^{100}.

Note que se um número a possui representação decimal

$$a = a_n a_{n-1} ... a_1 a_0 = a_n 10^n + a_{n-1} 10^{n-1} + ... + a_1 10 + a_0$$

então $a \equiv a_0 \mod 10$. Assim, para determinar o algarismo das unidades de 9^{100}, basta determinar um número r com $0 \leq r \leq 9$ tal que $9^{100} \equiv r \mod 10$.

Observe que $9^2 = 81 \equiv 1 \mod 10$, e $100 = 2 \cdot 50$. Assim,

$$9^{100} = 9^{2 \cdot 50} = (9^2)^{50} \equiv 1^{50} \equiv 1 \mod 10$$

Portanto, o algarismo das unidades de 9^{100} é 1.

Exercício 4.8. 1) Mostre que $89|(2^{44} - 1)$.

2) Sejam $a, b, m, n \in \mathbb{Z}$, com $m > 1$ e $n > 1$. Mostre que se $a \equiv b \mod m$ e $n|m$, então $a \equiv b \mod n$.

Proposição 4.9. *Sejam $a, b, m, n \in \mathbb{Z}$, com $m > 1$ e $n > 1$. Se $k = mmc(m, n)$ então*

$$a \equiv b \mod k \text{ se, e somente se, } a \equiv b \mod m \text{ e } a \equiv b \mod n$$

Demonstração. ($\Rightarrow$) Se $a \equiv b \mod k$, como $k = \text{mmc}(m, n)$, então $m|k$ e $n|k$. Logo, do exercício (2) anterior, segue que $a \equiv b \mod m$ e $a \equiv b \mod n$.

($\Leftarrow$) Se $a \equiv b \mod m$ e $a \equiv b \mod n$, então $m|a - b$ e $n|a - b$. Sendo $a - b$ um múltiplo de m e n, segue, da definição de mmc, que $k|a - b$, o que prova que $a \equiv b \mod k$.

□

Exemplo 4.10. Determine o menor múltiplo positivo de 7 que deixa resto 1 quando dividido por 5 e 6.

Observe que resolver este problema é o mesmo que encontrar o menor elemento $x \in \mathbb{N}$ tal que

$$7x \equiv 1 \mod 5 \text{ e } 7x \equiv 1 \mod 6$$

Mas, da proposição anterior, como $\text{mmc}(5, 6) = 30$, basta resolver

$$7x \equiv 1 \mod 30 \Leftrightarrow 30|7x - 1 \Leftrightarrow 7x - 30y = 1,\ y \in \mathbb{Z}.$$

Uma solução particular para a equação diofantina dada acima é $x = 13$ e $y = 3$.

Logo uma solução geral é dada por

$$x = 13 + t(-30),\ \text{e}\ y = 3 - 7t,\ t \in \mathbb{Z}$$

Para $x > 0$, temos $t < \dfrac{13}{30} < 1$. Porém, se $t < 0$ então $x > 13$. Logo, para $t = 0$, temos que $x = 13$ é a menor solução.

Observação 4.11. Da Proposição 4.6 (6), temos que se $a \equiv b \mod m$ e como $c \equiv c \mod m$ então $ac \equiv bc \mod m$. Porém, a recíproca deste resultado, em geral é falsa, por exemplo: $3 \equiv 3 \mod 6$ e $3 \cdot 3 \equiv 3 \cdot 5 \mod 6$, mas $3 \not\equiv 5 \mod 6$.

Mais precisamente, temos o seguinte resultado.

Proposição 4.12. *Sejam $a, b, c, m \in \mathbb{Z}$, com $c \neq 0$ e $m > 1$. Se $d = mdc(c, m)$ então*

$$ac \equiv bc \mod m \text{ se, e somente se, } a \equiv b \mod \frac{m}{d}$$

Demonstração. Temos que se $ac \equiv bc \mod m$ então $m|(a-b)c$, ou seja, $(a-b)c = km$. Dividindo os dois lados por d, temos que $(a-b)\frac{c}{d} = k\frac{m}{d}$. Mas como $\frac{m}{d}$ e $\frac{c}{d}$ são coprimos, então do Teorema 1.54, $\frac{m}{d}|(a-b)$, e portanto $a \equiv b \mod \frac{m}{d}$.

Reciprocamente, se $a \equiv b \mod \frac{m}{d}$, então $\frac{m}{d}|(a-b)$, e como mdc $\left(\frac{m}{d}, \frac{c}{d}\right) = 1$, $\frac{m}{d}|(a-b)\frac{c}{d}$, ou seja, $(a-b)\frac{c}{d} = k\frac{m}{d}$. Agora, multiplicando por d ambos os lados, segue que $(a-b)c = km$, e portanto, $ac \equiv bc \mod m$. □

Corolário 4.13. *Sejam $a, b, c, m \in \mathbb{Z}$, com $c \neq 0$ e $m > 1$. Se $mdc(c, m) = 1$ então*

$$ac \equiv bc \mod m \text{ se, e somente se, } a \equiv b \mod m$$

Definição 4.14. Uma coleção de m números inteiros $\{a_1, ..., a_m\}$ é chamado um **sistema completo de resíduos** módulo m se

i) $a_i \not\equiv a_j \mod m$ para $i \neq j$

ii) Para todo $n \in \mathbb{Z}$ existe a_i tal que $n \equiv a_i \mod m$

Exemplo 4.15. 1) Da observação 4.5, temos que $\{0, 1, ..., m-1\}$ é um sistema completo de resíduos módulo m. Desta forma, $\{m, m+1, ..., 2m-1\}$ também é um sistema completo de resíduos módulo m.

2) $\{0, 1, 2, 3, 4\}$, $\{5, 6, 7, 8, 9\}$, $\{12, 24, 35, -4, 18\}$ são sistemas completo de resíduos módulo 5.

Teorema 4.16. *Se* $\{a_1, ..., a_m\}$ *é um sistema completo de resíduos módulo* m *e* a *e* k *são inteiros tais que* $mdc(k, m) = 1$*, então*

$$a + ka_1, a + ka_2, ..., \ a + ka_m$$

também é um sistema de completo de resíduos módulo m*.*

Demonstração. Para $i, j = 0, ...m - 1$, temos que se $a + ka_i \equiv a + ka_j \mod m$ então, da Proposição 4.6 (5), temos que $ka_i \equiv ka_j \mod m$. Como $\text{mdc}(k, m) = 1$, segue, do corolário acima, que $a_i = a_j \mod m$. Mas como $\{a_1, ..., a_m\}$ é um sistema completo de resíduos módulo m, então temos que $i = j$. Isto mostra que $\{a + ka_1, a + ka_2, ..., \ a + ka_m\}$ são, dois a dois, não congruentes módulo m.

Agora dado $n \in \mathbb{Z}$, como $\{a_1, ..., a_m\}$ é um sistema completo de resíduos módulo m, existe a_i tal que $n \equiv a_i \mod m$. Por outro lado, como $\{a + ka_1, a + ka_2, ..., \ a + ka_m\}$ são, dois a dois, não congruentes módulo m, existe $a + ka_j$ tal que $a + ka_j \equiv a_i \mod m$. Portanto, da Proposição 4.6 (3), temos que $n \equiv a + ka_j \mod m$.

Portanto, $\{a+ka_1, a+ka_2, ..., \ a+ka_m\}$ formam um sistema completo de resíduos módulo m. □

Exemplo 4.17. $\{7, 11, 15, 19, 23\}$ é um sistema completo de resíduos módulo 5, pois $7 = 7+4\cdot 0$, $11 = 7+4\cdot 1$, $15 = 7+4\cdot 2$, $19 = 7+4\cdot 3$ e $23 = 7+4\cdot 4$, $\text{mdc}(4, 5) = 1$ e $\{0, 1, 2, 3, 4\}$ é um sistema completo de resíduos módulo 5.

4.2 Os Teoremas de Euler, Fermat e Wilson

Definição 4.18. Sejam $a, m \in \mathbb{Z}$, com $m > 1$. Um número $b \in \mathbb{Z}$ é chamado de um **inverso** de a módulo m se satisfaz $ab \equiv 1 \mod m$.

Note que se $\text{mdc}(a, m) = 1$ então a possui um inverso módulo m, pois pelo Teorema de Bezout, existem $b, c \in \mathbb{Z}$ tais que $ab + mc = 1$, isto é, $m|ab - 1$, ou ainda, $ab \equiv 1 \mod m$. O próximo resultado nos diz quando um inteiro a é o seu próprio inverso módulo p, onde p é um número primo.

Proposição 4.19. *Seja p um número primo. O inteiro positivo a é o seu próprio inverso módulo p se, e somente se, $a \equiv 1 \mod p$ ou $a \equiv -1 \mod p$.*

Demonstração. ($\Rightarrow$) Se a é o seu próprio inverso, então $a^2 \equiv 1 \mod p$, que implica que $p|a^2 - 1$, ou seja, $p|(a-1)(a+1)$. Como p é primo, temos que $p|a-1$ ou $p|a+1$, e portanto, $a \equiv 1 \mod p$ ou $a \equiv -1 \mod p$.
($\Leftarrow$) Se $a \equiv 1 \mod p$ ou $a \equiv -1 \mod p$, então $p|a-1$ ou $p|a+1$, o que implica que $p|(a-1)(a+1)$. Logo $p|a^2-1$, e portanto $a^2 \equiv 1 \mod p$, concluindo a demonstração. □

Exercício 4.20. Seja p primo. Mostre que se $i \in \{1, ..., p-1\}$ existe um único $j \in \{1, ..., p-1\}$ tal que $ij \equiv 1 \mod p$.

Teorema 4.21 (Teorema de Wilson)**.** *Se p é um número primo, então*

$$(p-1)! \equiv -1 \mod p.$$

Demonstração. Suponha que p seja primo. Para cada $i \in \{1, ..., p-1\}$, pelo exercício 4.20 existe um único $j \in \{1, ..., p-1\}$ tal que $ij \equiv 1 \mod p$. Por outro lado, da Proposição 4.19, 1 e $p-1$ são seus próprios inversos módulo p. Logo,

$$2 \cdot 3 \cdots (p-2) \equiv 1 \mod p,$$

Multiplicando-se ambos os lados da congruência por $p-1$ teremos,

$$2 \cdot 3 \cdots (p-2) \cdot (p-1) \equiv (p-1) \equiv -1 \mod p.$$

Portanto, $(p-1)! \equiv -1 \mod p$. □

Vale a recíproca do Teorema de Wilson.

Teorema 4.22. *Se $n \in \mathbb{Z}$ é tal que $(n-1)! \equiv -1 \mod n$ então n é primo.*

Demonstração. Suponha, por absurdo, que $(n-1)! \equiv -1 \mod n$ e que n não seja primo. Como n não é primo, existem $r, s \in \mathbb{Z}$, com $1 < |r| < n$ e $1 < |s| < n$ tais que $n = rs$. Logo $r|n$ e $r|(n-1)!$. Como $n|(n-1)!+1$, segue das propriedades de divisibilidade que $r|(n-1)!+1$ e portanto, $r|1$, contradição, pois $|r| > 1$. Portanto segue o resultado. □

Exemplo 4.23. 1) Encontre o resto da divisão de $6 \cdot 7 \cdot 8 \cdot 9$ por 5.

Devemos encontrar r tal que $6 \cdot 7 \cdot 8 \cdot 9 \equiv r \mod 5$. Observe que, $6 \equiv 1 \mod 5$, $7 \equiv 2 \mod 5$, $8 \equiv 3 \mod 5$ e $9 \equiv 4 \mod 5$. Assim,

$$6 \cdot 7 \cdot 8 \cdot 9 \equiv 1 \cdot 2 \cdot 3 \cdot 4 \equiv 4! \mod 5$$

Mas, do Teorema de Wilson, $4! \equiv -1 \mod 5$, portanto,

$$6 \cdot 7 \cdot 8 \cdot 9 \equiv -1 \equiv 4 \mod 5.$$

2) Seja $p > 3$ um número primo. Mostre que $p!$ e $(p-1)! - 1$ são primos entre si.

Mostremos que $\text{mdc}(p!\,, (p-1)! - 1) = 1$. Note que

$$\begin{aligned}\text{mdc}(p!\,, (p-1)! - 1) &= \text{mdc}(p(p-1)! - p + p\,, (p-1)! - 1) = \text{mdc}(p((p-1)! - 1) + p\,, (p-1)! - 1 \\ &\overset{\text{Lema de Euclides}}{=} \text{mdc}(p\,, (p-1)! - 1)\end{aligned}$$

Mas, do Teorema de Wilson, $(p-1)! \equiv -1 \mod p$, logo, $(p-1)! - 1 \equiv -2 \equiv p-2 \mod p$, ou seja, $p \nmid (p-1)! - 1$. Como $p > 3$, segue que,

$$\text{mdc}(p!\,, (p-1)! - 1) = \text{mdc}(p\,, (p-1)! - 1) = 1.$$

Definição 4.24. Um **sistema reduzido de resíduos** módulo m é um conjunto de números inteiros $r_1, ..., r_s$ tais que

a) $\text{mdc}(r_i, m) = 1$, para todo $i = 1, ..., s$

b) $r_i \not\equiv r_j \mod m$, se $i \neq j$

c) Para cada $n \in \mathbb{Z}$ tal que $\text{mdc}(n, m) = 1$, existe r_i tal que $n \equiv r_i \mod m$.

Observação 4.25. Pode-se obter um sistema reduzido de resíduos $r_1, ..., r_s$, módulo m, a partir de um sistema completo qualquer de resíduos $a_1, ..., a_m$, módulo m, eliminando os elementos a_i que não são primos com m.

Por exemplo, $\{0, 1, 2, 3, 4, 5, 6, 7\}$ é um sistema completo de resíduos módulo 8. Logo, $\{1, 3, 5, 7\}$ é um sistema reduzido de de resíduos módulo 8.

Designaremos por $\varphi(m)$ o número de elementos de um sistema reduzido de resíduos módulo $m > 1$, que corresponde à quantidade de números naturais entre 0 e $m-1$ que são primos com m. Pondo $\varphi(1) = 1$, isto define uma importante função $\varphi : \mathbb{N}^* \to \mathbb{N}^*$, chamada **função φ de Euler**.

Observe que $\varphi(m) \leq m-1$, para todo $m > 1$. Mais ainda, $\varphi(m) = m-1$ se, e somente se, m é primo. De fato, m é primo se, e somente se, $1, 2, ..., m-1$ formam um sistema reduzido de resíduos módulo m, o que equivale a dizer que $\varphi(m) = m-1$.

Exemplo 4.26. 1) $\varphi(8) = 4$

2) $\varphi(7) = 7 - 1 = 6$

3) $\varphi(12) = 4$, pois $\{1, 5, 7, 11\}$ é um sistema reduzido de resíduos módulo 12.

Proposição 4.27. *Seja $r_1, ..., r_{\varphi(m)}$ um sistema reduzido de resíduos módulo m e seja $a \in \mathbb{Z}$ tal que $mdc(a, m) = 1$. Então, $ar_1, ..., ar_{\varphi(m)}$ é um sistema reduzido de resíduos módulo m.*

Demonstração. Como na sequencia $ar_1, ..., ar_{\varphi(m)}$ temos $\varphi(m)$ elementos, vamos mostrar que todos eles são coprimos com m e, dois a dois, incongruentes módulo m.

Como $\text{mdc}(a, m) = 1$ e $\text{mdc}(r_i, m) = 1$ então $\text{mdc}(ar_i, m) = 1$, para todo i (Verifique!). Por outro lado, se $ar_i \equiv ar_j \mod m$, então, como $\text{mdc}(a, m) = 1$, temos que $r_i \equiv r_j \mod m$, e portanto $i = j$, uma vez que $r_1, ..., r_{\varphi(m)}$ é um sistema reduzido de resíduos módulo m, o que conclui a demonstração. □

Teorema 4.28 (Teorema de Euler)**.** *Sejam $m, a \in \mathbb{Z}$ com $m > 1$ e $mdc(a, m) = 1$. Então,*

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

Demonstração. Seja $r_1, ..., r_{\varphi(m)}$ um sistema reduzido de resíduos módulo m. Logo, pela proposição anterior, $ar_1, ..., ar_{\varphi(m)}$ formam um sistema reduzido de resíduos módulo m, pois $\text{mdc}(a, m) = 1$. Logo, ar_i é congruente a exatamente um dos r_j, $j = 1, ..., \varphi(m)$. Portanto, o produto dos ar_i é congruente ao produto dos r_j módulo m, isto é,

$$ar_1 \cdot ... \cdot ar_{\varphi(m)} \equiv r_1 \cdot ... \cdot r_{\varphi(m)} \mod m,$$

ou seja,

$$a^{\varphi(m)} r_1 \cdot ... \cdot r_{\varphi(m)} \equiv r_1 \cdot ... \cdot r_{\varphi(m)} \mod m.$$

Como $\text{mdc}(r_1 \cdot ... \cdot r_{\varphi(m)}, m) = 1$, pois $\text{mdc}(r_i, m) = 1$ para todo i, segue-se, pelo Corolário 4.13, que

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

□

Exemplo 4.29. 1) Como $\text{mdc}(15, 8) = 1$ e $\varphi(8) = 4$, segue do teorema de Euler, $15^4 \equiv 1 \mod 8$.

2) Encontre um inverso de 7 módulo 12.

Como $\text{mdc}(7, 12) = 1$ e $\varphi(12) = 4$, segue do teorema de Euler, $7^4 \equiv 1 \mod 12$. Logo $b = 7^3$ é um inverso de 7 módulo 12. Note também que

$$b = 7^3 \equiv 7 \cdot 49 \equiv 7 \cdot 1 \mod 12.$$

Logo, 7 também é um inverso de 7 módulo 12.

3) Determine o algarismo das unidades de 7^{9999}.

Sendo $7^{9999} = a_n...a_2a_1a_0$, temos que $7^{9999} \equiv a_0 \mod 10$. Como $\text{mdc}(7, 10) = 1$, então do Teorema de Euler,

$$7^{\varphi(10)} \equiv 1 \mod 10 \quad \overset{\varphi(10)=4}{\Longleftrightarrow} \quad 7^4 \equiv 1 \mod 10.$$

Por outro lado, do algoritmo da divisão, temos $9999 = 4 \cdot 2499 + 3$. Assim,

$$7^{9999} = 7^{4 \cdot 2499 + 3} = \left(7^4\right)^{2499} \cdot 7^3 \equiv 1 \cdot 7^3 \equiv 3 \mod 10$$

Portanto, o algarismo das unidades de 7^{9999} é 3.

Corolário 4.30 (Pequeno Teorema de Fermat)**.** *Sejam $a \in \mathbb{Z}$ e p um número primo tais que $mdc(a, p) = 1$. Então*

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

Demonstração. Como $\text{mdc}(a, p) = 1$, segue do Teorema de Euler, que $a^{\varphi(p)} \equiv 1 \mod p$. Mas p é primo, logo $\varphi(p) = p - 1$. Portanto $a^{p-1} \equiv 1 \mod p$. □

Observação 4.31. Se p é número primo e $a \in \mathbb{Z}$, então

$$a^p \equiv a \mod p.$$

De fato, pois se $p|a$ então $p|a(a^{p-1} - 1)$, o que implica que $a^p \equiv a \mod p$. Agora, se $p \nmid a$, então $\text{mdc}(a, p) = 1$, e do Pequeno Teorema de Fermat, $a^{p-1} \equiv 1 \mod p$. Multiplicando por a em ambos os lados, obtemos $a^p \equiv a \mod p$.

Exemplo 4.32. 1) Vamos achar o resto da divisão de 237^{28} por 13.

Observe que $237 \equiv 3 \mod 13$. Como $\text{mdc}(237, 13) = 1$, pelo Pequeno Teorema de Fermat, $237^{12} \equiv 1 \mod 13$, logo

$$(237^{12})^2 = 237^{24} \equiv 1 \mod 13.$$

Mas $237^4 \equiv 3^4 \equiv 81 \equiv 3 \, mod \, 7$, logo

$$237^{28} = 237^{24} \cdot 237^4 \equiv 1 \cdot 3 = 3 \mod 13$$

Portanto o resto da divisão de 237^{28} por 13 é 3.

2) Sejam p um número primo e $a, b \in \mathbb{Z}$. Então $(a + b)^p \equiv a^p + b^p \mod p$.

De fato, pois do PTF, $a^p \equiv a \mod p$, $b^p \equiv b \mod p$ e $(a + b)^p \equiv a + b \mod p$. Assim,

$$(a + b)^p \equiv a + b \equiv a^p + b^p \mod p.$$

Observação 4.33. Em geral, para o cálculo de $\varphi(m)$, temos os seguintes resultados:

1. Sejam $m, n \in \mathbb{N}$ tais que $\text{mdc}(m, n) = 1$. Então

$$\varphi(mn) = \varphi(m) \cdot \varphi(n).$$

2. Seja $m > 1$ e seja $m = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ a decomposição de m em fatores primos. Então,

$$\begin{aligned} \varphi(m) = & \; p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_n}\right) \\ = & \; p_1^{a_1 - 1} p_2^{a_2 - 1} \cdots p_n^{a_n - 1} \cdot (p_1 - 1) \cdot (p_2 - 1) \cdots (p_n - 1) \end{aligned}$$

Exemplo 4.34. Encontre os dois últimos algarismos de 9^{9^9}.

Tomando $9^{9^9} = a_n...a_1a_0$, então devemos ter que $9^{9^9} \equiv a_1a_0 \mod 100$. Como $\text{mdc}(9, 100) = 1$, do Teorema de Euler, temos $9^{\varphi(100)} \equiv 1 \mod 100$. Mas,

$$\varphi(100) = \varphi(2^2 \cdot 5^2) = 2^2 \cdot 5^2 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$$

Logo, $9^{40} \equiv 1 \mod 100$. Por outro lado, $81 = 9^2 \equiv 1 \mod 40$, então

$$9^9 = \left(9^2\right)^4 \cdot 9 \equiv 1 \cdot 9 \mod 40 \iff 40|9^9 - 9 \iff 9^9 = 40k + 9.$$

Logo,

$$9^{9^9} = 9^{40k+9} = \left(9^{40}\right)^k \cdot 9^9 \equiv 1 \cdot 9^9 \mod 100$$

Mas $9^3 = 729 \equiv 29 \mod 100$, então

$$9^9 = \left(9^3\right)^3 \equiv 29^3 \equiv 24389 \equiv 89 \mod 100.$$

Portanto, os dois últimos algarismos de 9^{9^9} é 89.

4.3 Congruências Lineares

Nesta seção, vamos estudar a resolução de congruências da forma:

$$aX \equiv b \mod m, \text{ onde } a, b, m \in \mathbb{Z},\ m > 1.$$

Para isto, vamos, inicialmente, dar um critério para decidir se tais congruências admitem solução.

Proposição 4.35. *Dados $a, b, m \in \mathbb{Z}$, com $m > 1$, a congruência*

$$aX \equiv b \mod m$$

possui solução se, e somente se, $mdc(a, m)$ divide b.

Demonstração. ($\Rightarrow$) Suponhamos que a congruência $aX \equiv b \mod m$ tenha uma solução x. Logo, temos que $m|ax - b$, ou seja, existe $y \in \mathbb{Z}$ tal que $ax - b = my$. Portanto, a equação $aX - mY = b$ admite solução. Logo, da proposição 3.1, segue que $\text{mdc}(a, m)$ divide b.

($\Leftarrow$) Suponha que $\text{mdc}(a, m)$ divide b. Logo, da proposição 3.1, segue que a equação $aX - mY = b$ admite uma solução $x, y \in \mathbb{Z}$. Portanto, $ax = b + my$ e, consequentemente, x é solução da congruência pois, $ax \equiv b \mod m$. □

Exemplo 4.36. Resolva a congruência $8X \equiv 4 \mod 12$.

Como $\text{mdc}(8, 12) = 4$ divide 4, temos da proposição anterior que a congruência dada admite solução, e

$$8X \equiv 4 \mod 12 \Leftrightarrow 8X + 12Y = 4 \overset{\div 4 = \text{mdc}(8,12)}{\Leftrightarrow} 2X + 3Y = 1$$

Observe que $x_0 = 2$ e $y_0 = -1$ é uma solução particular da equação $2X + 3Y = 1$. Portanto, $x_0 = 2$ é uma solução da congruência dada. Logo,

$$x = 2 + 3t,\ t \in \mathbb{Z}$$

são todas as soluções da congruência.

Observação 4.37. Note que se x_0 é solução da congruência $aX \equiv b \mod m$, então todo x tal que $x \equiv x_0 \mod m$ é também solução da congruência pois,

$$ax \equiv ax_0 \equiv b \mod m.$$

Portanto, toda solução particular determina, automaticamente, uma infinidade de soluções da congruência. Essas soluções serão identificadas (módulo m), já que são congruentes entre si, e, consequentemente, se determinam mutuamente.

Estaremos, portanto, interessados em determinar uma coleção completa de soluções duas a duas incongruentes módulo m, as quais serão chamadas de **sistema completo de soluções incongruentes** da congruência.

Teorema 4.38. *Sejam $a, b, m \in \mathbb{Z}$, com $m > 1$, $d = mdc(a, m)$ e $d|b$. Se x_0 é uma solução da congruência $aX \equiv b \mod m$, então*

$$x_0,\ x_0 + \frac{m}{d},\ x_0 + 2\frac{m}{d}, ...,\ x_0 + (d-1)\frac{m}{d},$$

formam um sistema completo de soluções incongruentes da congruência.

Demonstração. Como $d = \text{mdc}(a, m)$ e $d|b$, segue da proposição anterior, que a congruência admite solução.

Vamos mostrar que os números $x_0 + i\frac{m}{d}$, com $i \in \mathbb{N}$, são soluções da congruência. De fato,

$$a\left(x_0 + i\frac{m}{d}\right) = ax_0 + \underbrace{i\frac{a}{d}m}_{\equiv 0} \equiv ax_0 \equiv b \mod m.$$

Além disso, esses números são dois a dois incongruentes módulo m, pois, para $i, j \in \{0, 1, ..., d-1\}$, se

$$x_0 + i\frac{m}{d} \equiv x_0 + j\frac{m}{d} \mod m,$$

então, das propriedades de congruência e da Proposição 4.12, temos

$$i\frac{m}{d} \equiv j\frac{m}{d} \mod m \Leftrightarrow i \equiv j \mod \frac{m}{\text{mdc}(\frac{m}{d}, m)}$$

Mas, como $\frac{m}{\text{mdc}(\frac{m}{d}, m)} = d$ (Verifique!), logo $i \equiv j \mod d$, o que implica que $i = j$.

Finalmente, mostraremos que toda solução x da congruência $aX \equiv b \mod m$ é congruente, módulo m, $ax_0 + i\frac{m}{d}$, para algum $0 \leq i < d$.

De fato, seja x uma solução qualquer da congruência $aX \equiv b \mod m$. Então,

$$ax \equiv ax_0 \equiv b \mod m \overset{Prop.4.12}{\Leftrightarrow} x \equiv x_0 \mod \frac{m}{d}$$

Logo, existe $k \in \mathbb{Z}$ tal que $x - x_0 = k\frac{m}{d}$. Porém, do algoritmo da divisão, existem $i, q \in \mathbb{Z}$ tais que $k = qd + i$, com $0 \leq i < d$. Assim, $x = x_0 + (qd + i)\frac{m}{d}$, ou seja,

$$x = x_0 + qm + i\frac{m}{d} \equiv x_0 + i\frac{m}{d} \mod m.$$

□

Exemplo 4.39. Do exemplo 4.36, vinos que $x_0 = 2$ é uma solução da congruência $8X \equiv 4 \mod 12$. Logo, do teorema anterior, temos que a congruência $8X \equiv 4 \mod 12$ tem 4 soluções incongruentes módulo 12, a saber,

$$2,\ 2 + \frac{12}{4} = 5,\ 2 + 2\frac{12}{4} = 8,\ 2 + 3\frac{12}{4} = 11.$$

Exercício 4.40. Resolva a congruência $6X \equiv 14 \mod 4$.

Corolário 4.41. *Se $mdc(a, m) = 1$, então a congruência $aX \equiv b \mod m$ possui uma única solução módulo m.*

Exercício 4.42. Resolva a congruência $25X \equiv 15 \mod 29$.

4.4 Teorema Chinês dos Restos

Aproximadamente no primeiro século da nossa era, o matemático chinês Sun-Tsu propôs o seguinte problema:

Qual é o número que deixa restos 2, 3 e 2 quando dividido, respectivamente, por 3, 5 e 7?

A resposta dada por Sun-Tsu para este problema foi 23.

Traduzido em linguagem matemática, o problema de Sun-Tsu equivale a procurar as soluções do seguinte sistema de congruências:

$$\begin{aligned} X &\equiv 2 \mod 3 \\ X &\equiv 3 \mod 5 \\ X &\equiv 2 \mod 7. \end{aligned}$$

Mais geralmente, estudaremos sistemas de congruências da forma:

$$\begin{aligned} a_1X &\equiv b_1 \mod m_1 \\ a_2X &\equiv b_2 \mod m_2 \\ &\vdots \\ a_kX &\equiv b_k \mod m_k. \end{aligned} \tag{2}$$

Para que tal sistema possua solução, é necessário que $\text{mdc}(a_i, m_i)|b_i$, para todo $i = 1, ..., k$, via Proposição 4.35. Porém, observe que se uma congruência da forma $aX \equiv b \mod m$ possui solução, então $d = \text{mdc}(a, m)$ divide b. Assim, pondo

$$a' = \frac{a}{d},\ b' = \frac{b}{d},\ n = \frac{m}{d},$$

temos, pela Proposição 4.12, que a congruência $aX \equiv b \mod m$ é equivalente a

$$a'X \equiv b' \mod n,$$

onde $\text{mdc}(a', n) = 1$. Logo, da observação feita após a Definição 4.18, segue que a' possui um único inverso multiplicativo a'' módulo n, e daí segue que a congruência $a'X \equiv b' \mod n$ é equivalente à congruência

$$X \equiv c \mod n,$$

onde $c = b' \cdot a''$. Disto, segue que o sistema de congruências (2) é equivalente a um sistema da forma

$$X \equiv c_1 \mod n_1$$
$$X \equiv c_2 \mod n_2$$
$$\vdots$$
$$X \equiv c_k \mod n_k.$$

Teorema 4.43 (Teorema Chinês dos Restos)**.** *Sejam $n_1, n_2, ..., n_k \in \mathbb{Z}$ tais que $mdc(n_i, n_j) = 1$, para todo $i, j = 1, ..., k$, com $i \neq j$, e sejam $c_1, c_2, ..., c_k$ inteiros arbitrários. Então o sistema de congruências lineares*

$$\begin{aligned} X &\equiv c_1 \mod n_1 \\ X &\equiv c_2 \mod n_2 \\ &\vdots \\ X &\equiv c_k \mod n_k. \end{aligned} \tag{3}$$

possui uma única solução módulo $N = n_1 \cdot n_2 \cdots n_k$. Tal solução pode ser obtida como segue:

$$x = N_1 y_1 c_1 + N_2 y_2 c_2 + ... + N_k y_k c_k, \tag{4}$$

onde $N_i = \dfrac{N}{n_i}$ e y_i é o inverso multiplicativo de N_i módulo n_i, $i = 1, ..., k$.

Demonstração. Vamos, inicialmente, provar que x como dado em (4) é uma solução simultânea do sistema (3).

De fato, como $\text{mdc}(n_i, n_j) = 1$, $i \neq j$, e $n_i \nmid N_i$, segue que $\text{mdc}(n_i, N_i) = 1$ e logo N_i possui um inverso multiplicativo y_i módulo n_i. Assim, como $n_i | N_j$, se $i \neq j$, e $N_i y_i \equiv 1 \mod n_i$, segue-se que

$$x = N_1 y_1 c_1 + N_2 y_2 c_2 + ... + N_k y_k c_k \equiv N_i y_i c_i \equiv c_i \mod n_i.$$

Por outro lado, se x_0 é outra solução do sistema (3), então

$$x \equiv x_0 \; mod \; n_i, \; \forall i = 1, ..., k.$$

Como $\text{mdc}(n_i, n_j) = 1$, para $i \neq j$, segue que $\text{mmc}(n_1, ..., n_k) = n_1 \cdots n_k = N$ e, consequentemente, pela Proposição 4.9, temos que

$$x \equiv x_0 \mod N.$$

□

Exemplo 4.44. 1) Vamos determinar a solução do problema de Sun-Tsu.

$$X \equiv 2 \mod 3$$

$$X \equiv 3 \mod 5$$

$$X \equiv 2 \mod 7.$$

Observe que $3, 5$ e 7 são coprimos entre si, logo temos que $N = 3 \cdot 5 \cdot 7 = 105$. Assim, $N_1 = 5 \cdot 7 = 35$, $N_2 = 3 \cdot 7 = 21$ e $N_3 = 3. \cdot 5 = 15$. Disto, devemos encontrar os inversos multiplicativos de N_1, N_2 e N_3, módulo $3, 5$ e 7, respectivamente, ou seja, encontrar as soluções das congruências:

$$35Y \equiv 1 \mod 3, \quad 21Y \equiv 1 \mod 5, \quad 15Y \equiv 1 \mod 7.$$

Resolvendo estas congruências, obtemos, respectivamente, as soluções $y_1 = 2$, $y_2 = 1$ e $y_3 = 1$. Portanto, uma solução módulo $N = 105$ é dada por

$$x = N_1 y_1 c_1 + N_2 y_2 c_2 + N_3 y_3 c_3 = 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 = 233 \equiv 23 \mod 105.$$

Logo, 23 é uma solução, única módulo 105, do problema. Qualquer outra solução é da forma $23 + 105t$, com $t \in \mathbb{Z}$.

Exercício 4.45. Resolva o sistema:

$$3X \equiv 1 \mod 7$$

$$5X \equiv 2 \mod 11$$

$$4X \equiv 3 \mod 13.$$

Solução: 810

Vários sistemas de congruências lineares que não se encaixam nas hipóteses do Teorema Chines dos Restos ainda podem ter solução.

Proposição 4.46. *O sistema de congruências* $X \equiv c_1 \mod m_1$ *e* $X \equiv c_2 \mod m_2$ *admite solução se, e somente se,* $c_2 \equiv c_1 \mod (mdc(m_1, m_2))$. *Além disso, dada uma solução a dos sistema, um número* a' *é também uma solução se, e somente se,* $a' \equiv a \mod (mmc(m_1, m_2))$. *Logo, se a é uma solução do sistema, então uma solução geral é dada por*

$$a' = a + mmc(m_1, m_2)t, \ t \in \mathbb{Z}.$$

Demonstração. ($\Rightarrow$) Suponha que $X \equiv c_1 \mod m_1$ e $X \equiv c_2 \mod m_2$ admite uma solução a. Então $a \equiv c_1 \mod m_1$ e $a \equiv c_2 \mod m_2$. Logo existem $x, y \in \mathbb{Z}$ tais que $a = m_1x + c_1$ e $a = m_2y + c_2$. Logo

$$m_1x + c_1 = m_2y + c_2 \Longrightarrow m_1x - m_2y = c_2 - c_1,$$

ou seja, a segunda equação possui solução, o que implica que $\text{mdc}(m_1, m_2)|c_2 - c_1$, ou seja, $c_2 \equiv c_1 \mod (\text{mdc}(m_1, m_2))$.

($\Leftarrow$) Suponha que $c_2 \equiv c_1 \mod (\text{mdc}(m_1, m_2))$. Então $\text{mdc}(m_1, m_2)|c_2 - c_1$, o que implica que a equação diofantina

$$m_1X + m_2Y = c_2 - c_1$$

possui solução x_0 e y_0. Tome $a = m_1x_0 + c_1 = m_2(-y_0) + c_2$. Então $a \equiv c_1 \mod m_1$ e $a \equiv c_2 \mod m_2$, e portanto $X \equiv c_1 \mod m_1$ e $X \equiv c_2 \mod m_2$ admite solução.

A outra parte segue diretamente da proposição 4.9, pois

$$\begin{array}{l} a' \equiv c_1 \equiv a \mod m_1 \\ a' \equiv c_2 \equiv a \mod m_2 \end{array} \iff a' \equiv a \mod (\text{mmc}(m_1, m_2))$$

□

Exemplo 4.47. Encontre os termos comuns das progressões aritméticas (a_n) de primeiro termo 5 e razão 14, e (b_n) de primeiro termo 12 e razão 21.

Observe que $a_n = 5 + 14n$ e $b_n = 12 + 21n$, $n \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Assim, os termos comuns a ambas as PAs satisfazem

$$X \equiv 5 \mod 14$$

$$X \equiv 12 \mod 21$$

a qual possui solução, pois $\text{mdc}(14, 21) = 7$ e $12 \equiv 5 \mod 7$. Assim, para determinarmos uma solução para o sistema acima, basta resolver a equação diofantina

$$14x + 21y = 21 - 5 \iff 14x + 21y = 7$$

que possui solução $x_0 = -1$ e $y_0 = 1$. Logo $a = 14(-1) + 5 = -9$ é solução do sistema. Assim, os termos comuns são dados por

$$a' \equiv -9 \mod \text{mmc}(14, 21) \iff a' \equiv -9 \equiv 33 \mod 42$$

Logo, os termos comuns entre as PAs são dados por $c_n = 33 + 42n$, para todo $n \in \mathbb{N}_0$

Exercício 4.48. Encontre o menor número natural que deixa resto 380 quando dividido por 1512 e deixa resto 68 quando dividido por 1650.

4.5 Resíduos Quadráticos

Sejam p um primo ímpar e $a, b, c \in \mathbb{Z}$ tal que $\text{mdc}(a, p) = 1$. Estamos interessados em encontrar soluções para a equação quadrática

$$ax^2 + bx + c \equiv 0 \mod p$$

Porém, esta equação é equivalente a

$$4a(ax^2 + bx + c) \equiv 0 \mod p.$$

Como $4a(ax^2 + bx + c) = (2ax + b)^2 - (b^2 - 4ac)$, segue que a equação acima é equivalente a

$$(2ax + b)^2 \equiv b^2 - 4ac \mod p.$$

Tomando $X = 2ax + b$ e $A = b^2 - 4ac$, temos

$$X^2 \equiv A \mod p.$$

Observação 4.49. 1) O fato de que os números naturais são produtos de seus divisores primos nos leva a querer estudar resíduo quadrático módulo primo, pois se x_0 é uma solução da congruência $x^2 \equiv a \mod m$, $m > 1$ e se $p|m$ então x_0 é solução de $x^2 \equiv a \mod p$.

2) A equação $x^2 \equiv a \mod 2$ sempre possui solução para todo inteiro a, pois se a é par, então $a = 2k$, para algum $k \in \mathbb{Z}$, e neste caso, $x^2 \equiv 2k \equiv 0 \mod 2$, onde $x = 0$ é uma solução. Agora se a é ímpar, então $a = 2k + 1$, para algum $k \in \mathbb{Z}$, e logo $x^2 \equiv 2k + 1 \equiv 1 \mod 2$, e portanto $x = 1$ é solução.

Disto conclui-se que todo inteiro é resíduo quadrático módulo 2. Portanto, basta estudar resíduo quadrático módulo números primos ímpares.

3) Se $p|a$ então a congruência quadrática $x^2 \equiv a \mod p$ tem $x = 0$ como única solução.

Então para evitar trivialidades, vamos sempre assumir que $\text{mdc}(a, p) = 1$.

Portanto, estamos interessados no estudo das soluções para as congruências da forma

$$x^2 \equiv a \mod p,$$

onde p é um primo ímpar e $\text{mdc}(a, p) = 1$.

Definição 4.50. Sejam $a \in \mathbb{Z}$ e p um primo ímpar tal que $\text{mdc}(a, p) = 1$. Dizemos que a é um **resíduo quadrático** módulo p se a congruência $x^2 \equiv a \mod p$ possui solução. Caso contrário, dizemos que a não é um resíduo quadrático módulo p.

Exemplo 4.51. 4 é um resíduo quadrático módulo 5, pois $3^2 \equiv 4 \mod 5$. Mas 2 não é um resíduo quadrático módulo 5, pois esta congruência $x^2 \equiv 2 \mod 5$ não possui solução. De fato, pois se x_0 fosse uma solução de $x^2 \equiv 2 \mod 5$, pelo algoritmo da divisão, $x_0 = 5q + r$ com $0 \leq r < 5$. Assim, $r^2 \equiv (x_0)^2 \equiv 2 \mod 5$, o que é impossível.

Teorema 4.52. *Para p primo ímpar e $a \in \mathbb{Z}$ tal que $mdc(a, p) = 1$, a congruência $x^2 \equiv a \mod p$, caso tenha solução, tem exatamente duas soluções incongruentes módulo p.*

Demonstração. Se esta congruência possui uma solução x_0 então $-x_0$ também é uma solução, pois $(-x_0)^2 = (x_0)^2 \equiv a \mod p$. Mostremos então que estas duas soluções x_0 e $-x_0$ são incongruentes módulo p. Suponha que $x_0 \equiv -x_0 \mod p$ então $2x_0 \equiv 0 \mod p$, isto é, $p|2x_0$. Mas como $p > 2$ primo, então $p|x_0$. Como $p|(x_0)^2 - a$, das propriedades de divisibilidade, segue que $p|a$, contradição, pois $\text{mdc}(a, p) = 1$. Mostremos agora que existem apenas duas soluções incongruentes. Seja $y \in \mathbb{Z}$ uma solução de $x^2 \equiv a \mod p$, isto é, $y^2 \equiv a \mod p$. Como x_0 é solução, temos que $(x_0)^2 \equiv y^2 \equiv a \mod p$, ou seja, $(x_0 - y)(x_0 + y) \equiv 0 \mod p$. Logo $p|x_0 - y$ ou $p|x_0 + y$, o que implica que $y \equiv x_0 \mod p$ ou $y \equiv -x_0 \mod p$. □

Exemplo 4.53. Vamos determinar todos os resíduos quadráticos módulo 13. Para isto, é suficiente considerarmos os quadrados dos números $1, 2, ..., 12$ que formam um sistema reduzido

de resíduos módulo 13.

$$\begin{array}{ll} 1^2 \equiv 1 \mod 13 & 7^2 \equiv 10 \mod 13 \\ 2^2 \equiv 4 \mod 13 & 8^2 \equiv 12 \mod 13 \\ 3^2 \equiv 9 \mod 13 & 9^2 \equiv 3 \mod 13 \\ 4^2 \equiv 3 \mod 13 & 10^2 \equiv 9 \mod 13 \\ 5^2 \equiv 12 \mod 13 & 11^2 \equiv 4 \mod 13 \\ 6^2 \equiv 10 \mod 13 & 12^2 \equiv 1 \mod 13 \end{array}$$

Note que ambas as colunas de congruências figuram apenas os números $1, 3, 4, 9, 10, 12$. Estes são todos os resíduos quadráticos módulo 13. O fato de haver repetição na segunda coluna, é que $(13-k)^2 \equiv k^2 \mod 13$, para $k \in \{1, 2, 3, 4, 5, 6\}$.

Teorema 4.54. *Seja p primo ímpar. Dentre os números $1, 2, ..., p-1$, temos $\frac{p-1}{2}$ resíduos quadráticos e $\frac{p-1}{2}$ que não são.*

Demonstração. Consideremos os quadrados dos números $1, 2, ..., \frac{p-1}{2}$, isto é,

$$1^2, 2^2, 3^2, ..., \left(\frac{p-1}{2}\right)^2.$$

Vamos mostrar que estes quadrados são incongruentes módulo p. Sejam $x, y \in \{1, 2, ..., \frac{p-1}{2}\}$ e suponha que $x^2 \equiv y^2 \mod p$. Logo $x^2 - y^2 = (x+y)(x-y) \equiv 0 \mod p$, e portanto, $p|(x+y)(x-y)$. Como $x + y < p$, segue que $p \nmid (x+y)$. Logo $p|(x-y)$, o que implica que $x \equiv y \mod p$, e portanto, $x = y$. Desta forma, concluímos que todos os quadrados acima são incongruentes módulo p. Agora, observe que se $k \in \{1, 2, ..., \frac{p-1}{2}\}$ então

$$p - k \in \{\frac{p+1}{2}, \frac{p+3}{2}, ..., p-1\}.$$

Logo, como $(p-k)^2 \equiv k^2 \mod p$, segue que os resíduos quadráticos pertencem as classes de congruência que contem os quadrados

$$1^2, 2^2, 3^2, ..., \left(\frac{p-1}{2}\right)^2.$$

Portanto, $\frac{p-1}{2}$ é o número de resíduos quadráticos dentre os números $1, 2, ..., p-1$. Os outros $\frac{p-1}{2}$ não são resíduo quadráticos. □

Exercício 4.55. Encontre todos os resíduos quadráticos módulo 17.

Proposição 4.56. *Seja $p > 2$ um número primo. Então a congruência $x^2 \equiv -1 \mod p$ possui solução se, e somente se, $p \equiv 1 \mod 4$.*

Demonstração. ($\Rightarrow$) Suponha que a congruência $x^2 \equiv -1 \mod p$ tenha solução. Então existe $b \in \mathbb{Z}$ tal que $b^2 \equiv -1 \mod p$. Disto segue que $\text{mdc}(p, b) = 1$ e logo, do PTF, obtemos

$$1 \equiv b^{p-1} = (b^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \mod p$$

e daí $(-1)^{\frac{p-1}{2}} = 1$, pois $-1 \not\equiv 1 \mod p$. Disto, segue que $\dfrac{p-1}{2}$ é par, isto é, $\dfrac{p-1}{2} = 2k$, ou ainda, $p - 1 = 4k$. Portanto $p \equiv 1 \mod 4$.

($\Leftarrow$) Suponha que $p \equiv 1 \mod 4$. Pelo Teorema de Wilson, $(p-1)! \equiv -1 \mod p$. Mas observe que

$$-1 \equiv (p-1)! = 1 \cdot 2 \cdot ... \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot ... \cdot (p-2) \cdot (p-1) = \prod_{j=1}^{\frac{p-1}{2}} j(p-j) \mod p.$$

Como $j(p-j) \equiv -j^2 \mod p$, temos

$$-1 \equiv \prod_{j=1}^{\frac{p-1}{2}} j(p-j) \equiv \prod_{j=1}^{\frac{p-1}{2}} (-j^2) = (-1)^{\frac{p-1}{2}} \left(\prod_{j=1}^{\frac{p-1}{2}} j \right)^2 = (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2} \right)! \right]^2 \mod p.$$

Mas $p \equiv 1 \mod 4$, logo $(-1)^{\frac{p-1}{2}} = 1$, e portanto

$$\left[\left(\frac{p-1}{2} \right)! \right]^2 \equiv -1 \mod p.$$

Portanto, $x = \left(\dfrac{p-1}{2} \right)!$ é uma solução da congruência $x^2 \equiv -1 \mod p$. □

Exercício 4.57. Encontre as soluções da congruência $x^2 \equiv -1 \mod p$, onde $p = 5, 13, 17$;

Exemplo 4.58. Existem infinitos primos da forma $4n + 1$, com $n \in \mathbb{N}$.

De fato, suponha que $P = \{p_1, p_2, ..., p_k\}$ são todos os primos da forma $4n + 1$. Considere o número

$$N = (2p_1 \cdot p_2 \cdot ... \cdot p_k)^2 + 1 \in \mathbb{N}.$$

Pelo TFA, N pode ser fatorado em fatores primos. Assim, seja q um fator primo de N. Logo $q|N$, e então $(2p_1 \cdot p_2 \cdot ... \cdot p_k)^2 + 1 \equiv 0 \mod q$. Isto significa que a congruência $x^2 \equiv -1$

mod q possui solução $x = 2p_1 \cdot p_2 \cdot ... \cdot p_k$. Logo, do teorema anterior, $q \equiv 1 \mod 4$, ou seja $q \in P$. Logo, $q|p_1 \cdot p_2 \cdot ... \cdot p_k$ e portanto $q|1$, absurdo! Portanto P não pode ser um conjunto finito.

Embora saibamos a lista completa de resíduos quadráticos, na prática pode ser difícil reconhecer se um número é ou não um resíduo quadrático. Por exemplo, 2 é um resíduo quadrático módulo 1019? Veremos em breve uma ferramente prática na resolução destes problemas.

Definição 4.59. Seja p um primo ímpar e $a \in \mathbb{Z}$ tal que $\text{mdc}(a, p) = 1$. O **símbolo de Legendre** é o símbolo $\left(\frac{a}{p}\right)$ definino por

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & , \text{ se } a \text{ é resíduo quadrático módulo } p \\ -1 & , \text{ se } a \text{ não é resíduo quadrático módulo } p \end{cases}$$

Exemplo 4.60. Do exemplo 4.53, segue que

$$\left(\frac{1}{13}\right) = \left(\frac{3}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{9}{13}\right) = \left(\frac{10}{13}\right) = \left(\frac{12}{13}\right) = 1,$$

enquanto

$$\left(\frac{2}{13}\right) = \left(\frac{5}{13}\right) = \left(\frac{6}{13}\right) = \left(\frac{7}{13}\right) = \left(\frac{8}{13}\right) = \left(\frac{11}{13}\right) = -1.$$

Teorema 4.61 (Critério de Euler)**.** *Seja p um primo ímpar e $a \in \mathbb{Z}$ tal que $mdc(a, p) = 1$. Então*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p.$$

Demonstração. Primeiro, observe que como $\text{mdc}(a, p) = 1$, então do PTF, $a^{p-1} \equiv 1 \mod p$. Como p é ímpar, então $p - 1$ é par, e logo

$$a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \mod p.$$

Assim, $p|\left(a^{\frac{p-1}{2}} - 1\right)$ ou $p|\left(a^{\frac{p-1}{2}} + 1\right)$, isto é, $a^{\frac{p-1}{2}} \equiv \pm 1 \mod p$.

- Suponha que a é um resíduo quadrático módulo p. Assim, existe $b \in \mathbb{Z}$ tal que $b^2 \equiv a \mod p$ e $\text{mdc}(b, p) = 1$, pois $\text{mdc}(a, p) = 1$. Então, segue do P.T.Fermat, que

$$a^{\frac{p-1}{2}} \equiv \left(b^2\right)^{\frac{p-1}{2}} = b^{p-1} \equiv 1 \mod p \Rightarrow \left(\frac{a}{p}\right) = 1 \equiv a^{\frac{p-1}{2}} \mod p.$$

- Suponha agora que a não seja um resíduo quadrático módulo p. Para todo $r \in \{1, 2, ..., p-1\}$, a congruência linear $rx \equiv a \mod p$ possui exatamente uma solução $s \in \{1, 2, ..., p-1\}$, pois $\{1, 2, ..., p-1\}$ é um sistema completo de resíduos módulo p. Mais ainda, temos que $r \not\equiv s \mod p$, pois se $r \equiv s \mod p$, teríamos que $a \equiv rs \equiv s^2 \mod p$, ou seja, a seria uma resíduo quadrado, contradição! Logo, podemos rescrever o conjunto $\{1, 2, ..., p-1\}$ como

$$\{1, 2, ..., p-1\} = \{r_1, s_1, r_2, s_2, ..., r_{\frac{p-1}{2}}, s_{\frac{p-1}{2}}\}$$

tal que $r_i s_i \equiv a \mod p$ para $1 \leq i \leq \dfrac{p-1}{2}$. Assim, do Teorema de Wilson,

$$-1 \equiv (p-1)! = \prod_{i=1}^{\frac{p-1}{2}} r_i s_i \equiv \prod_{i=1}^{\frac{p-1}{2}} a = a^{\frac{p-1}{2}} \mod p \Rightarrow \left(\frac{a}{p}\right) = -1 \equiv a^{\frac{p-1}{2}} \mod p.$$

□

Exemplo 4.62. Seja $p = 29$ e $a = 3$. Então

$$\left(\frac{3}{29}\right) \equiv 3^{\frac{29-1}{2}} = 3^{14} \mod 29$$

Como $3^3 \equiv -2 \mod 29$ e $3^{14} = (3^3)^4 \cdot 3^2$, então

$$\left(\frac{3}{29}\right) \equiv 3^{14} = \left(3^3\right)^4 \cdot 3^2 \equiv (-2)^4 \cdot 9 = 16 \cdot 9 = 144 \equiv 28 \equiv -1 \mod 29$$

Portanto 3 não é um resíduo quadrático módulo 29.

Proposição 4.63. *Seja p um primo ímpar e $a, b \in \mathbb{Z}$ tais que $mdc(a, p) = mdc(p, b) = 1$. Então valem*

a) Se $a \equiv b \mod p$ então $\left(\dfrac{a}{p}\right) = \left(\dfrac{b}{p}\right)$.

b) $\left(\dfrac{a^2}{p}\right) = 1$

c) $\left(\dfrac{ab}{p}\right) = \left(\dfrac{a}{p}\right) \cdot \left(\dfrac{b}{p}\right)$

Demonstração. a) Exercício.

b) Exercício.

c) Pelo Critério de Euler,

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot ^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \mod p.$$

Logo $p \left| \left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \right.$, mas $p > 2$ e $\left| \left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \right| \leq 2$, então

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

□

Exemplo 4.64. $\left(\frac{12}{29}\right) = \left(\frac{2^2 \cdot 3}{29}\right) = \left(\frac{2^2}{29}\right) \cdot \left(\frac{3}{29}\right) = \left(\frac{3}{29}\right) = -1$

Exercício 4.65. Verifique se 1987 é um resíduo quadrático módulo 17.

O critério de Euler já nos fornece uma maneira de identificar resíduos quadráticos. Veremos agora dois resultados muito fortes aos quais facilitarão a identificação de resíduos quadráticos.

Teorema 4.66. *Para p um primo ímpar, temos*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & , \text{ se } p \equiv \pm 1 \mod 8 \\ -1 & , \text{ se } p \equiv \pm 3 \mod 8 \end{cases}$$

Teorema 4.67 (Reciprocidade Quadrática de Gauss)**.** *Sejam p e q dois primos ímpares distintos. Então*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}.$$

Exemplo 4.68. 1) Verifiquemos se 2 é um resíduo quadrático módulo 1019.

Como $1019 \equiv 3 \mod 8$, segue que $\left(\frac{2}{1019}\right) = -1$. Portanto, 2 não é um resíduo quadrático módulo 1019.

2) Verifiquemos se 31 é um resíduo quadrático módulo 1997.

Pela Reciprocidade quadrática de Gauss, temos

$$\left(\frac{31}{1997}\right) = (-1)^{\left(\frac{31-1}{2}\right)\left(\frac{1997-1}{2}\right)} \left(\frac{1997}{31}\right) = \left(\frac{1997}{31}\right).$$

Mas $1997 \equiv 13 \mod 31$, logo

$$\left(\frac{1997}{31}\right) = \left(\frac{13}{31}\right) = (-1)^{\left(\frac{31-1}{2}\right)\left(\frac{13-1}{2}\right)} \left(\frac{31}{13}\right) = \left(\frac{31}{13}\right).$$

Como $31 \equiv 5 \mod 13$, segue que

$$\left(\frac{31}{13}\right) = \left(\frac{5}{13}\right) = (-1)^{\left(\frac{5-1}{2}\right)\left(\frac{13-1}{2}\right)} \left(\frac{13}{5}\right) = \left(\frac{13}{5}\right).$$

Mas $13 \equiv 3 \mod 5$, e então, pelo critério de Euler,

$$\left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) \equiv 3^{\frac{5-1}{2}} = 3^2 \equiv -1 \mod 5.$$

Portanto,

$$\left(\frac{31}{1997}\right) = -1.$$

3) Calculemos $\left(\frac{3}{p}\right)$, onde p é um número primo maior que 3.

Pela reciprocidade quadrática, temos que

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}.$$

Mas como $p \equiv r \mod 3$ então

$$\left(\frac{p}{3}\right) = \left(\frac{r}{3}\right) = \begin{cases} \left(\frac{1}{3}\right) = 1 & , \text{ se } p \equiv 1 \mod 3 \\ \left(\frac{2}{3}\right) = -1 & , \text{ se } p \equiv 2 \mod 3 \end{cases}$$

Por outro lado,

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & , \text{ se } p \equiv 1 \mod 4 \\ -1 & , \text{ se } p \equiv 3 \mod 4 \end{cases}$$

Assim, analisando as informações acima, temos

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & , \text{ se } p \equiv 1 \text{ ou } p \equiv 11 \mod 12 \\ -1 & , \text{ se } p \equiv 5 \text{ ou } p \equiv 7 \mod 12 \end{cases}$$

Referências

[1] HEFEZ, Abramo; *Aritmética*, 1 ed., Coleção PROFMAT, Rio de Janeiro, SBM, 2013.

[2] HEFEZ, Abramo; *Elementos de Aritmética*, 2 ed., Textos Universitários, Rio de Janeiro, SBM, 2006.

[3] MILIES, César Polcino; COELHO, Sônia Pitta, *Números: Uma Introdução à Matemática*, 3 ed., São Paulo, EDUSP, 2003.

[4] SANTOS, José Plínio de Oliveira; *Introdução à Teoria dos Números*, 3 ed., Coleção Matemática Universitária, Rio de Janeiro, IMPA, 2005.

[5] SHOKRANIAN, Salahoddin; *Uma Introdução à Teoria dos Números*, 1ª ed.,Ciência Moderna, 2008.