Como seria de esperar, o Teorema Fundamental da Aritmética tem imensas consequências importantes. Por exemplo, dadas factorizações em potências primas de dois inteiros, é imediato reconhecer se um deles divide o outro ou se os números são primos entre si.

Dados dois inteiros podemos sempre supor (usando para o efeito expoentes nulos, se necessário) que temos factorizações desses inteiros que usam exactamente os mesmos primos. É fácil verificar o seguinte:

Proposição

Sejam $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ *e* $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$, *com* $k \geq 1$, $p_1, p_2, \dots, p_k$ *números primos e* $\alpha_i, \beta_i \geq 0$ *inteiros, as factorizações de dois números inteiros* a, b *maiores do que* 1. *Então,*

$$\mathrm{mdc}(a,b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \dots p_k^{\min(\alpha_k,\beta_k)}$$

$$\mathrm{mmc}(a,b) = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \dots p_k^{\max(\alpha_k,\beta_k)}$$

Exemplo

Sejam $a = 2200$ e $b = 5250$. Factorizando estes inteiros em números primos temos $a = 2^3 \cdot 5^2 \cdot 11^1$ e $b = 2^1 \cdot 3^1 \cdot 5^3 \cdot 7^1$, ou seja:

$$a = 2^3 \cdot 3^0 \cdot 5^2 \cdot 7^0 \cdot 11^1 \text{ e } b = 2^1 \cdot 3^1 \cdot 5^3 \cdot 7^1 \cdot 11^0.$$

Então,

$$\begin{aligned} mdc(a,b) &= 2^{\min(3,1)} \cdot 3^{\min(0,1)} \cdot 5^{\min(2,3)} \cdot 7^{\min(0,1)} \cdot 11^{\min(1,0)} \\ &= 2^1 \cdot 3^0 \cdot 5^2 \cdot 7^0 \cdot 11^0 \\ &= 2 \cdot 5^2 \\ &= 50 \\ mmc(a,b) &= 2^{\max(3,1)} \cdot 3^{\max(0,1)} \cdot 5^{\max(2,3)} \cdot 7^{\max(0,1)} \cdot 11^{\max(1,0)} \\ &= 2^3 \cdot 3^1 \cdot 5^3 \cdot 7^1 \cdot 11^1 \\ &= 231000 \end{aligned}$$

A escrita formal usada na proposição e no exemplo anteriores, é usualmente substituída pelas regras práticas seguintes:

- O máximo divisor comum de dois inteiros é igual ao produto dos factores primos comuns, cada um elevado ao menor dos expoentes. Quando não existem factores primos comuns os números são primos entre si.
- O mínimo múltiplo comum de dois inteiros é igual ao produto dos factores primos não comuns e dos comuns, cada um elevado ao maior dos expoentes.

Exemplo

Vamos determinar $\mathrm{mdc}(36, 60)$ e $\mathrm{mmc}(36, 60)$. Utilizamos as factorizações em potências primas: $36 = 2^2 \cdot 3^2$ e $60 = 2^2 \cdot 3^1 \cdot 5^1$. Tem-se, $\mathrm{mdc}(36, 60) = 2^2 \cdot 3^1 = 12$ e $\mathrm{mmc}(36, 60) = 2^2 \cdot 3^2 \cdot 5^1 = 180$.

Aritmética modular

Muitos problemas do dia-a-dia podem ser simplificados pela *aritmética modular*. A ideia básica consiste na escolha de um inteiro n (que depende do problema e é chamado *módulo*), e na substituição dos inteiros envolvidos pelo resto da sua divisão por n.

Exemplo

Sendo hoje terça-feira, que dia da semana será daqui a 1000 dias? Utilizar o calendário para responder seria pouco prático... Mais prático seria agrupar os 1000 dias em conjuntos de 7 e ver quantos sobram. Ora, $1000 = 142 * 7 + 6$. Assim, daqui a 1000 dias teremos o mesmo dia da semana que daqui a 6 dias. "Segunda-feira" é a resposta.

Definição

Seja n um inteiro positivo. Dois números inteiros a e b dizem-se congruentes módulo *n se tiverem o mesmo resto na divisão por n. Se a é congruente com b módulo n escreve-se* $a \equiv b \pmod{n}$.

O resultado seguinte, de fácil demonstração, proporciona uma útil definição alternativa de congruência módulo n.

Lema

Seja n um inteiro positivo. Dois números inteiros a e b são congruentes módulo n se e só se $n \mid (a - b)$.

Lema (Propriedades)

Seja $n \in \mathbb{N}$, $a, b, c, d \in \mathbb{Z}$, tem-se:

(i) $a \equiv a \pmod{n}$;

(ii) *se* $a \equiv b \pmod{n}$, *então* $b \equiv a \pmod{n}$;

(iii) *se* $a \equiv b \pmod{n}$ *e* $b \equiv c \pmod{n}$, *então* $a \equiv c \pmod{n}$;

(iv) *se* $a \equiv b \pmod{n}$ *e* $c \equiv d \pmod{n}$, *então* $a + c \equiv b + d \pmod{n}$;

(v) *se* $a \equiv b \pmod{n}$ *e* $c \equiv d \pmod{n}$, *então* $ac \equiv bd \pmod{n}$;

(vi) *se* $a \equiv b \pmod{n}$ *e* $d \mid n$, *então* $a \equiv b \pmod{d}$;

(vii) *se* $a \equiv b \pmod{n}$, *então* $\mathrm{mdc}(a, n) = \mathrm{mdc}(b, n)$.

Como aplicação, podemos estabelecer critérios de divisibilidade de m em termos dos algarismos da sua representação decimal.

Exemplo

Ilustração do critério: "o natural m é divisível por 3 se e só se a soma dos algarismos da sua representação decimal é divisível por 3".
Observemos que

$$10 \equiv 1 \pmod 3, \text{ donde } 10^k \equiv 1 \pmod 3, \ \forall k \in \mathbb{N}.$$

Para $m = 84951$, fazemos

$$84951 = 8 \cdot 10^4 + 4 \cdot 10^3 + 9 \cdot 10^2 + 5 \cdot 10^1 + 1$$

logo

$$84951 \pmod 3 \equiv 8+4+9+5+1 \pmod 3 \equiv 27 \pmod 3 \equiv 0 \pmod 3.$$

Concluímos que 84951 é divisível por 3 sem usar o Algoritmo da Divisão!

Exercício

Estabeleça critérios de divisibilidade por 3 e por 9.

Proposição

Sejam n um número natural e a, x, y inteiros. Se $ax \equiv ay \pmod{n}$, então $x \equiv y \pmod{\frac{n}{\mathrm{mdc}(a,n)}}$.

Demonstração. Suponhamos que $ax \equiv ay \pmod{n}$. Sendo $d = \mathrm{mdc}(a, n)$, temos que $\mathrm{mdc}\left(\frac{a}{d}, \frac{n}{d}\right) = 1$. Da hipótese vem que n divide $ax - ay = a(x - y)$, donde se tira que $\frac{n}{d}$ divide $\frac{a}{d}(x - y)$. Como $\frac{n}{d}$ e $\frac{a}{d}$ são primos entre si, segue-se que $\frac{n}{d}$ divide $(x - y)$, ou seja, que $x \equiv y \pmod{\frac{n}{\mathrm{mdc}(a,n)}}$. □

Corolário

Sejam n um natural e a, x, y inteiros. Se $ax \equiv ay \pmod{n}$ e $\mathrm{mdc}(a, n) = 1$, então $x \equiv y \pmod{n}$.

Teorema de Euler

Definimos $\varphi(1) = 1$. Seja $n > 1$ um inteiro. Representamos por $\varphi(n)$ o número de naturais menores que n e que são primos com n. A função φ é conhecida por *função de Euler* e está implementada no GAP:

Exemplo

```
gap> Phi(3); Phi(6);Phi(9);Phi(10);Phi(11);Phi(10*11);
2
2
6
4
10
40
```

É imediato observar que se p é primo, então $\varphi(p) = p - 1$.

Prova-se o seguinte resultado. Devido a ele diremos por vezes que a função de Euler é multiplicativa.

Proposição

Sejam n e m números naturais primos entre si. Então, $\varphi(nm) = \varphi(n)\varphi(m)$.

O resultado seguinte está na base do sistema RSA que abordaremos mais tarde.

Teorema (Teorema de Euler)

Seja n um número natural. Se a é um inteiro primo com n, então $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Corolário (Pequeno Teorema de Fermat)

Sejam a um inteiro e p um número primo. Se p não dividir a, então $a^{p-1} \equiv 1 \pmod{p}$.

Uma das aplicações do Teorema de Euler é a simplificação de congruências.

Exemplo

Vamos determinar os dois últimos algarismos da representação decimal do número 3^{1492}. Isto é equivalente a encontrar $3^{1492} \pmod{100}$, isto é, o resto da divisão de 3^{1492} por 100.
Como $\mathrm{mdc}(3, 100) = 1$ estamos nas condições do Teorema de Euler, que permite escrever $3^{\varphi(100)} \equiv 1 \pmod{100}$.
Tem-se $\varphi(100) = \varphi(4) \cdot \varphi(25) = 2 \cdot 20 = 40$, resultando assim que $3^{40} \equiv 1 \pmod{100}$. Além disso, $3^{40k} \equiv 1 \pmod{100}$, para qualquer $k \in \mathbb{N}$. Visto que $1492 \equiv 12 \pmod{40}$, então $3^{1492} \equiv 3^{12} \pmod{100}$.
Ora, $3^{12} = \left(\left(3^3\right)^2\right)^2 = \left(27^2\right)^2 = 729^2 \equiv 29^2 \pmod{100} \equiv 841 \pmod{100} \equiv 41 \pmod{100}$.
Portanto, os dois últimos algarismos da escrita decimal do número 3^{1492} são o 4 e o 1.

Exemplo

Vejamos que $18 \mid 5^{1000} + 5$.
Ora, $\varphi(18) = \varphi(2) \cdot \varphi(3^2) = 1 \cdot 6 = 6$. Pelo Teorema de Euler temos que $5^6 \equiv 1 \pmod{18}$, já que $\mathrm{mdc}(5, 18) = 1$. Como $1000 = 6 \cdot 166 + 4$, vem que $5^{1000} \equiv (5^6)^{166} \cdot 5^4 \equiv 1 \cdot 25^2 \equiv 7^2 \pmod{18}$. Tem-se $7^2 + 5 = 54 = 3 \cdot 18$, logo $5^{1000} + 5 \equiv 7^2 + 5 \equiv 0 \pmod{18}$.

Exercício

Verifique se $17 \mid 3^{233} + 1$.

Congruências Lineares

Uma congruência da forma $aX \equiv b \pmod{n}$ diz-se uma *congruência linear*. As congruências lineares podem ser manipuladas como equações as algébricas, excepto no que diz respeito à "lei do corte" para o produto.

Definição (Inverso (módulo n))

Seja a um número inteiro não nulo. Diz-se que a' é um inverso *de a módulo n se $a'a = aa' \equiv 1 \pmod{n}$.*

Teorema

Um inteiro não nulo a tem inverso módulo n se e só se $\mathrm{mdc}(a, n) = 1$.

Demonstração. Se a tem inverso módulo n, então $\exists a' \in \mathbb{Z} : a'a \equiv 1 \pmod{n}$, isto é, $n \mid a'a - 1$. Donde se obtém $a'a + (-k)n = 1$, para algum $k \in \mathbb{Z}$, e, portanto, 1 pode-se escrever como combinação linear de a e n. Logo, $\mathrm{mdc}(a, n) = 1$. Reciprocamente, se $\mathrm{mdc}(a, n) = 1$ então, existem $x, y \in \mathbb{Z}$ tais que $ax + ny = 1$. Daqui resulta que $n \mid ax - 1$, ou seja, $ax \equiv 1 \pmod{n}$. Consequentemente, x é um inverso de a módulo n. □

O GAP permite determinar um inverso módulo n (positivo e menor que n) de um inteiro inteiro a, no caso de este existir.

Exemplo

```
gap> 3^-1 mod 5;
2
gap> 2^-1 mod 23; 3^-1 mod 23;
12
8
```