Problemas aritméticos

Que valores toma a função

$$f : \mathbb{Z} \to \mathbb{Z}, \qquad f(x) = x^2 + x + 1?$$

$f(x)$ só toma valores ímpares;

Problemas aritméticos

Que valores toma a função

$$f : \mathbb{Z} \to \mathbb{Z}, \qquad f(x) = x^2 + x + 1?$$

$f(x)$ só toma valores ímpares;

$$f(x + 3k) = (x + 3k)^2 + x + 3k + 1 = f(x) + 6kx + 9k^2 + 3k;$$

O resto na divisão de $f(x)$ por 3 é 0 ou 1, para qualquer $x \in \mathbb{Z}$.

Problemas aritméticos

Será que 20131400046549674927 é um quadrado perfeito?

O resto na divisão de m^2 por 4 é 0 ou 1, para qualquer $m \in \mathbb{Z}$,

$$20131400046549674927 = (\cdots) \times 4 + 3$$

Problemas aritméticos

Será que 20131400046549674927 é um quadrado perfeito?

O resto na divisão de m^2 por 4 é 0 ou 1, para qualquer $m \in \mathbb{Z}$,

$$20131400046549674927 = (\cdots) \times 4 + 3$$

Será que

$$32070004559 \mid (2^{16035002279} - 1)\,?$$

Relação de congruência e classes de congruência

Seja $m \in \mathbb{N}$. Dois inteiros a e b dizem-se **congruentes** módulo m

$$a \equiv b \mod m$$

se m divide $a - b$.

A congruência é uma relação de equivalência em $\mathbb{Z}$, para qualquer escolha do módulo m. A classe de congruência de a é

$$\cdots, a - 3m, a - 2m, a - m, a, a + m, a + 2m, a + 3m, \cdots$$

Relação de congruência e classes de congruência

Cada classe de congruência tem um e um só representante no conjunto

$$[m] = \{0, 1, \cdots, m-1\}$$

Um **sistema completo de resíduos módulo** m é um conjunto

$$\{n_0, n_1, \cdots, n_{m-1}\} \subset \mathbb{Z}$$

tal que se $i \neq j$ então n_i e n_j não são congruentes $\mod m$.
Ou, ordenando os n_i,

$$n_i \equiv i \mod m \ \forall 0 \leq i < m$$

$\mathbb{Z}_{/m}$ designa o conjunto das classes de congruência módulo m.

Operações entre classes de congruência

Se $a \equiv b \mod m$ e $c \equiv d \mod m$ então

$$a + c \equiv b + d \mod m \qquad ac \equiv bd \mod m$$

Estão bem definidas em $\mathbb{Z}_{/m}$ as operações de soma e produto.
Tabuadas módulo 4:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

A equação linear numa variável

$$ax \equiv b \mod m$$

Se $mdc(a, m) = d$, a equação tem d soluções distintas se $d|b$ e não tem soluções caso contrário.

Se x_0 e y_0 são inteiros satisfazendo

$$ax_0 + my_0 = d,$$

as soluções do primeiro caso são

$$x_0\frac{b}{d} + k\frac{m}{d}, \qquad 0 \leq k < d$$

A equação linear numa variável (cont.)

$$ax \equiv b \mod m$$

Se $mdc(a, m) = d$ e $d \mid b$, a equação

$$\frac{a}{d}x \equiv \frac{b}{d} \mod \frac{m}{d}$$

tem uma solução única $x_0 \mod \frac{m}{d}$.

As d soluções da equação original são as classes de congruência mod m

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

A união destas classes é a classe de $x_0 \mod \frac{m}{d}$.

A equação linear numa variável (cont.)

$$ax \equiv b \mod m$$

Se $mdc(a, m) = 1$, a solução única $x_0 \mod m$ é

$$x_0 \equiv \bar{a}b \mod m$$

onde $\bar{a}$ é o inverso de a em $\mathbb{Z}_{/m}$, ou seja a classe de congruência que satisfaz $a\bar{a} \equiv 1 \mod m$.

Usamos também a notação a^{-1} para $\bar{a}$, com o cuidado de não confundir com o número racional $\frac{1}{a}$!