Introdução à Teoria dos Números
Ficha 3: primeiras noções de Aritmética Modular

Exercício 0.1 *Existe algum inteiro n tal que n^2+n+1 é divisível por 5? Encontrar um n tal que n^2+n+1 é divisível por 7; encontrar uma sucessão infinita de inteiros com essa propriedade.*

Exercício 0.2 *Qual o resto na divisão de* $201314000465129457693496749 27$ *por 4? Notar que*

$$201314000465129457693496749 27 = 201314000465129457693496749 \times 10^2 + 27.$$

Seja $n = 4m + r$ com $0 \leq r < 4$; quais os possíveis restos na divisão de n^2 por 4?
Existe algum n inteiro tal que $n^2 = 201314000465129457693496749 27$?

Relações de congruência

Seja $m > 1$. Dois inteiros a e b dizem-se **congruentes** módulo m

$$a \equiv b \mod m$$

se m divide $a - b$.
Portanto, qualquer inteiro é congruente módulo m a um único $0 \leq a < m$.
O conjunto de todos os inteiros congruentes, módulo m, a um certo $0 \leq a < m$ chama-se uma classe de congruência módulo m.
Um conjunto de m inteiros representando todas as classes de congruência módulo m, diz-se um **sistema completo de resíduos** módulo m.

Exercício 0.3 *Verificar que se $a \equiv b \mod m$ e $c \equiv d \mod m$ então*

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

As tabuadas de soma e multiplicação módulo 4 são

$+$	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

Exercício 0.4 *Escrever as tabuadas da soma e multiplicação módulo* 7.

A equação linear

Dados inteiros a, b e m, a equação

$$ax \equiv b \mod m$$

tem solução se existem inteiros x_0 e y_0 tais que

$$ax_0 - b = my_0;$$

isso acontece se e só se $mdc(a, m)$ divide b.
Em caso afirmativo, dado x_0 (e y_0) que satisfaz a igualdade, as soluções da segunda equação são os inteiros da forma

$$x = x_0 + \frac{m}{d}k, \quad k \in \mathbb{Z},$$

e portanto há exactamente d classes de congruência módulo m que são solução da primeira equação.

Exercícios

1. Provar que $n^3 - n$ é divisível por 6, para todo o $n \geq 0$,

   a) por indução;

   b) usando as classes de congruência módulo 6.

2. Quais as classes de congruência módulo 12 que estão contidas na classe de congruência de 1 módulo 4?

3. Em que classes de congruência módulo 8 estão os quadrados perfeitos? 4926834923 poderá ser a soma de dois quadrados perfeitos?

4. Mostrar que se

$$n = a_0 + a_1 10 + a_2 10^2 + \cdots + a_k 10^k$$

então

$$n \equiv a_0 + a_1 + a_2 + \cdots + a_k \mod 3$$

e

$$n \equiv a_0 - a_1 + a_2 - \cdots + (-1)^k a_k \mod 11.$$

5. Para que módulos m é que existe um sistema completo de resídulos consistindo apenas de inteiros ímpares?

6. Resolver as seguintes congruências (encontrar todas as soluções ou justificar que não existem):

   a) $5x \equiv 3 \mod 11$;

   b) $12x \equiv 2 \mod 33$;

   c) $9x \equiv 21 \mod 12$;

   d) $110x \equiv 40 \mod 575$;

   e) $1011x \equiv 1101 \mod 1110$;

   f) $501x \equiv 345 \mod 72$;

   g) $55x \equiv 5 \mod 555$;

7. Notando que $2^3 = 8$ e $2^4 = 16$, calcular o resto na divisão de 2^{431}

   a) por 7;

   b) por 17.

8. Mostrar que todo o inteiro da forma $4k + 3$ tem algum factor da mesma forma. Deduzir que existem infinitos primos congruentes com 3 módulo 4.
   Podemos aplicar o mesmo raciocínio para inteiros da forma $4k+1$? E da forma $6k + 5$?

9. Seja p primo. Notando que para cada $1 < a < p - 1$ existe um (único) $1 < a' < p-1$ tal que $aa' \equiv 1 \mod p$, demonstrar o Teorema de Wilson:

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

   se e só se p é primo.