# Introdução à Teoria dos Números

**Ficha de preparação** (semana de 06/10)

## Testes de primalidade

**Exercício 0.1** *Usar o Teorema de Fermat (e uma calculadora...) para verificar que* 1763 *não é primo.*

**Exercício 0.2** *Sabendo que* $561 = 3\times11\times17$, *mostrar que* $a^{561} \equiv a \mod 561$, *para todo o* $a$.

**Exercício 0.3** *Dizemos que* $n$ *é um pseudo-primo para a base* 2 *se* $2^{n-1} \equiv 1 \mod n$ *mas* $n$ *não for primo. Mostrar que* $n$ *é um pseudo-primo para a base* 2, *então* $2^n - 1$ *também o é.*
***Sugestão**: Mostrar que* $2^n - 1$ *divide* $2^{2^n-2} - 1$.

## Polinómios sobre $\mathbb{Z}_{/p}$

As operações de soma, produto e divisão com resto de polinómios são válidas para polinómios com coeficientes em $\mathbb{Z}_{/p}$ ($p$ primo).

**Exercício 0.4** *Dados os polinómios* $f(x) = 2x^7+3x^4+x^3+4x^2+1$ *e* $g(x) = 3x^4 + x + 1$, *com coeficientes em* $\mathbb{Z}_{/5}$, *fazer a divisão de* $f(x)$ *por* $g(x)$.

## Ordem módulo $p$

Dado $p$ primo e $a$ primo com $p$, a ordem de $a$ módulo $p$ é o menor inteiro positivo $k$ (que designamos $\mathrm{ord}_p(a)$ ou só $\mathrm{ord}(p)$, se estiver claro qual o primo $p$) que satisfaz $a^k \equiv 1 \mod p$.
A ordem só depende da classe de congruência de $a$ módulo $p$.

**Exercício 0.5** *Calcular os valores de* $\mathrm{ord}_7(a)$*, para cada* $a \in \mathbb{Z}_{/7}^{\times}$.

**Exercício 0.6** *Fixando um primo* $p$*, verificar as propriedades seguintes:*

*1) Se* $ord(a) = k$ *e* $a^h \equiv 1 \mod p$ *então* $k \mid h$*. Em particular* $ord(a) \mid p-1$.

*2) Se* $ord(a) = k$ *e* $ab \equiv 1 \mod p$ *então* $ord(b) = k$.

*3) Se* $ord(a) = k$ *então* $ord(a^j) = \frac{k}{d}$ *em que* $d = mdc(k, j)$.

*4) Se* $ord(a) = k$, $ord(b) = h$ *e* $mdc(k, h) = 1$ *então* $ord(ab) = kh$.

Se $\mathrm{ord}_p(a) = p - 1$, $a$ é uma **raiz primitiva** módulo $p$.

**Problemas** (Aula 08/10 e seguinte...)

1. Notando que $7^2 \equiv 5 \mod 11$, determinar, sem ser por tentativa e erro, quais as soluções de
$$x^{12} + 3x^{11} + 5 \equiv 0 \mod 11$$

2. Determinar (sem esforço...) a única solução da equação
$$47x^{120} + 7x^{100} + 54x^{20} + 25x + 2 \equiv 0 \mod 101$$

3. Se $g$ é raiz primitiva de $p$, para que valores de $k$ é que $g^k$ também é raiz primitiva?

4. Mostrar que se $a = b^2$ então $a$ não pode ser raiz primitiva de um primo $p$ ímpar.
**Sugestão**: se $a$ é raiz primitiva, então existe $s < p - 1$ tal que $a^s \equiv b \mod p$.

5. Se $p$ é um primo ímpar, para quantos $a \in \mathbb{Z}_{/p}$ é que
$$x^2 \equiv a \mod p$$
tem solução?
**Sugestão**: Seja $g$ uma raiz primitiva de $p$ e $g^k \equiv a$. Estudar a existência de solução em função da paridade de $k$.

6. Mostrar que se $p$ é primo ímpar então

$$x^2 \equiv -1 \mod p$$

tem solução se e só se $p \equiv 1 \mod 4$.

7. Mostrar que existem infinitos primos congruentes com 1 módulo 4.

**Sugestão**: Dados primos $p_1, p_2, \cdots, p_k$ congruentes com 1 módulo 4, considerar os factores primos de

$$(p_1 p_2 \cdots p_k)^2 + 1$$

8. Mostrar que se $p$ e $q$ são primos ímpares diferentes e $a$ é primo com $pq$,

$$a^{\phi(pq)/2} \equiv 1 \mod pq.$$

Concluir que $pq$ não tem raizes primitivas.

9. Usar o critério de Euler para determinar quais das seguintes equações têm solução e qual o seu número

a) $x^{12} \equiv 16 \mod 17$;

b) $x^{20} \equiv 13 \mod 17$;

c) $x^{48} \equiv 9 \mod 17$;

d) $x^{11} \equiv 9 \mod 17$;

10. Mostrar que $3^8 \equiv -1 \mod 17$. Justificar porque é que podemos concluir que 3 é raiz primitiva de 17.
Usar uma lista das classes de congruência de $3^i \mod 17$ para encontrar as soluções do problema anterior.

11. 3 é raiz primitiva módulo 31 e $3^{12} \equiv 8 \mod 31$. Determinar as soluções de

$$x^4 \equiv 8 \mod 31.$$