# Teoria dos Números

## 1 Noções Básicas

A Teoria dos Números é a área da matemática que lida com os números inteiros, isto é, com o conjunto $\mathbb{Z} = \{..., -4, -3, -2, -1, 0, 1, 2, 3, 4...\}$. Ela permite resolver de forma imediata problemas que seriam muito difíceis de outra forma, por exemplo:

**Problema 1**

1. *Seja $p$ um número primo tal que $p > 3$. Prova que $p^2 - 1$ é múltiplo de 24.*

2. *Encontra dois inteiros $x$ e $y$ tais que $x^2 + y^2 + 1$ seja múltiplo de 4.*

3. *Encontra um inteiro $n$ tal que $2^n - 1$ é múltiplo de $n$*

4. *Encontra um inteiro $n$ tal que $2^n + 1$ é primo e $n$ é múltiplo de 5.*

Se já conseguires resolver todos estes problemas, então este texto não é para ti. Se não, verás que no final te vão parecer meros exercícios! Comecemos com algumas definições:

**Definição 1 (Divide)** *Sejam $a$ e $b$ dois inteiros. Diz-se que $a$ divide $b$, ou que $b$ é múltiplo de $a$, ou ainda que $a$ é um divisor de $b$, se existe um inteiro $c$ tal que $ac = b$. Escreve-se: $a|b$.*

Lembra-te que trabalhamos com todos os inteiros e não apenas com os positivos, e temos, por exemplo, $-3|9$, $4|28$, $5|-15$ e $-73|-146$. Os números 1 e $-1$ são chamados as unidades, porque dividem todos os inteiros, ou seja $1|n$ e $-1|n$ qualquer que seja o inteiro $n$. Por outro lado o 0 não divide nenhum inteiro, excepto ele próprio. Na realidade qualquer inteiro divide-se a ele mesmo, ou seja, verifica-se $n|n$, para todo o inteiro $n$. Abaixo enunciamos mais algumas propriedades:

**Teorema 1** *Neste teorema e ao longo do resto do texto, letras representam números inteiros.*

1. *$a|b$ implica que $a|bc$ e que $ac|bc$*

2. *$a|b$ e $b|c$ implica que $a|c$*

3. *Se* $a|b$ *e* $a|c$, *então* $a|b+c$

4. *Se* $a|b$ *e* $b|a$, *então* $a = b$ *ou* $a = -b$

5. *Se* $a|b$ *e* $a \geq 0$ *e* $b \geq 0$ *então* $a \leq b$

6. $an|am$ *e* $a \neq 0$ *implica que* $n|m$

Convence-te de que o teorema é verdade, não achamos necessário dar aqui uma demonstração rigorosa.

Os divisores de um número $n$ são os números que o dividem, obviamente. A próxima definição é fundamental em Teoria dos Números e certamente já conheces:

**Definição 2 (primo)** *Um inteiro positivo* $a$ *diz primo se* $a$ *tem* 4 *divisores.*

Por exemplo, o 73 é primo, porque os seus únicos divisores são 73, $-73$, 1 e $-1$. Por outro lado o 6 não é primo porque, para além dos 4 divisores tem ainda o 2, o 3, o $-2$ e o $-3$. 1 não é primo porque só tem dois divisores.

Certamente conheces, da escola primária, o chamado algoritmo da divisão que passamos a enunciar numa forma um pouco mais geral:

**Teorema 2** *Sejam* $a$ *e* $b$ *inteiros (não necessariamente positivos) tais que* $b \neq 0$. *Então dividindo* $a$ *por* $b$ *obtemos um único quociente* $q \in \mathbb{Z}$ *e um único resto* $r$ *tal que* $0 \leq r < |b|$ *que verificam a igualdade* $a = qb + r$

O que o teorema diz é que existe um único $r < |b|$ positivo tal que $a - r$ é múltiplo de $b$. Nota que os múltiplos de $b$ são os mesmos que os de $-b$.

Por exemplo se $a = 7$ e $b = 3$ temos $q = 2$ e $r = 1$. Se $a = -7$ e $b = 3$ temos $q = -3$ e $r = 2$. Se $a = -73$ e $b = -19$ temos $q = 4$ e $r = 3$, porque $-73 = 4 \times (-19) + 4$.

A próxima definição também já deve ser conhecida da escola:

**Definição 3 (Máximo divisor comum e mínimo múltiplo comum)** *Sejam* $a$ *e* $b$ *inteiros, não ambos* 0. *Definimos o seu máximo divisor comum como o maior inteiro positivo* $d$ *tal que* $d|a$ *e* $d|b$. *Escrevemos* $d = (a, b)$

*Analogamente definimos a mínimo múltiplo comum de* $a$ *e* $b$ *ao menor inteiro positivo* $m$ *tal que* $a|m$ *e* $b|m$. *Escrevemos* $m = [a, b]$.

Por exemplo $(12, 28) = 4$, $(-49, 21) = 7$, $(73, 58) = 1$, $[5, 3] = 15$, $[6, 10] = 30$. Se $(a, b) = 1$ dizemos que $a$ e $b$ são primos entre si.

**Exercício 1** *Prova que* $ab = (a, b)[a, b]$.

**Exercício 2** *Prova que dois inteiros consecutivos são primos entre si.*

É óbvio verificar que se $d|a$ e $d|b$ então $d|as + bt$ para quaisquer inteiros $s$ e $t$. No entanto $2|4$ e $2|8$, mas 2 não pode ser escrito como $2 = 4s + 8t$ porque o número da direita é sempre múltiplo de 4. O teorema seguinte garante-nos que no entanto $(a, b)$ pode ser escrito dessa forma.

**Teorema 3 (Bézout)** *Sejam* $a$ *e* $b$ *inteiros não ambos* 0. *Então existem inteiros* $s$ *e* $t$ *tais que:* $as + bt = (a, b)$

Se na demonstração te baralhares com a quantidade de letras, faz um exemplo com números concretos, por exemplo $a = 60$ e $b = -28$.

**Demonstração.**Consideremos o conjunto de todos os números positivos da forma $as + bt$ onde o $s$ e o $t$ podem variar ao longo dos inteiros.

É óbvio que esse conjunto contém alguns elementos, mesmo que $a$ e $b$ sejam negativos, porque se pusermos $s = a$ e $t = b$ temos que $a^2 + b^2$ é um número positivo e por isso pertence a esse conjunto.

Obviamente $(a, b)$ divide todos os elementos desse conjunto. Seja $d$ o menor desses números. Então dividindo $a$ por $d$ arranjamos $q$ e $r$ tais que $a = qd + r$. Mas $r \leq d$ e $r$ é da forma $as + bt$, por isso tem de ser zero (porque $d$ é o menor elemento do conjunto).

Assim $d|a$. Da mesma forma se prova que $d|b$.

Se houvesse algum número $c$ maior que $d$ e tal que $c|a$ e $c|b$, então $c|d$, o que entra em contradição com $c > d$.

Assim $d$ é mesmo $(a, b)$ e portanto $(a, b)$ pode ser escrito como $as + bt$. ∎

**Problema 2** *O Arquiduque De Boez tem duas ampulhetas, uma que se esvazia em* 105 *minutos e outra que demora* 165 *minutos. Será possível ao Arquiduque De Boez medir* 15 *minutos (possivelmente após preparar previamente as ampulhetas)*

**Exercício 3** *Se* $(a, b) = d$, *então* $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

**Exercício 4** *Prova que* $(a, b) = (a, b - a)$.

**Problema 3 (IMO 1959)** *Prova que a fracção* $\dfrac{21n + 4}{14n + 3}$ *é irredutível para todo o* $n$ *inteiro.*

**Teorema 4 (Lema de Euclides)** *Se* $a|bc$ *e* $(a, b) = 1$*, então* $a|c$.

**Demonstração.**Usando o Teorema anterior, sejam $s$ e $t$ tais que $1 = as + bt$. Multiplicando os dois lados da igualdade por $c$ obtemos $c = cas + bct$. Como $a|cas$ e $a|bc$, $a|c$.

■

Se $(a, b) \neq 1$ o teorema pode não ser verdade. Por exemplo $4|6 \times 14 = 84$, mas $4 \not| 6$ e $4 \not| 14$.

Uma consequência importante deste lema é o conhecido Teorema fundamental da Aritmética que passamos a enunciar:

**Teorema 5 (Fundamental da Aritmética)** *Seja* $n > 1$ *um inteiro. Então existem números primos positivos* $p_1 < p_2 < ... < p_k$ *e números inteiros positivos* $a_1, a_2, ..., a_k$ *tais que*

$$n = p_1^{a_1} \times p_2^{a_2} \times ... \times p_k^{a_k}$$

*Para além disso essa decomposição em primos é única.*

**Demonstração.**A prova que apresentamos não é rigorosa, mas deve dar a ideia geral da demonstração: A primeira parte é bastante natural. Provemos por indução em $n$: para $n = 2$ é imediato (porque 2 é primo). Se $n > 2$ é primo também já está, se não, podemos escrever $n = ab$ com $a$ e $b$ menores que $n$. Então usando a hipótese de indução em $a$ e $b$, conseguimos escrever $n$ da forma desejada.

Para a segunda parte, se $n = p_1^{a_1} \times p_2^{a_2} \times ... \times p_k^{a_k} = q_1^{a_1} \times q_2^{a_2} \times ... \times q_j^{a_j}$, $p_1$ divide a expressão da direita, por isso um dos $q_i$ tem de ser igual a $p_1$. A mesma coisa para os outros $p_l$ e assim os primos do lado esquerdo estão todos no lado direito e trocando os seus papéis vemos que os primos têm de ser os mesmos.

Para obtermos a igualdade dos expoentes apenas precisamos de dividir pela menor potência de cada primo e ver que esse primo não pode dividir nenhum dos membros da expressão. ■

O teorema diz que podemos escrever todo o inteiro positivo como o produto de primos, e que esses primos são sempre os mesmos. Por exemplo $6 = 2 \times 3$ e $100 = 2^2 \times 5^2$, mas se factorizarmos 100 como o produto de primos, eles são sempre o 2 e o 5, cada um "duas vezes".

## 2 Congruências

A ferramenta mais poderosa em Teoria dos números é a aritmética modular, que provém da noção de congruência.

**Definição 4** *Sejam $a$, $b$ e $n$ inteiros, $n > 1$. Então diz-se que $a$ é congruente com $b$ módulo $n$ e escreve-se $a \equiv b \pmod{n}$ se $n|b-a$.*

Por exemplo, $a \equiv b \pmod 2$ se são ambos pares ou ambos ímpares e $a \equiv b \pmod 3$ se são ambos da forma $3k$, ambos da forma $3k+1$ ou ambos da forma $3k+2$. Números negativos também são comtemplados na definição, por isso $73 \equiv -45 \pmod{59}$. Se dividirmos $a$ por $n$ e obtemos resto $r$, então $a \equiv r \pmod n$, porque $a = qn + r$ e assim $n|a - r = qn$. Então $a \equiv 0 \pmod n$ se e só se $n|a$.

**Teorema 6**

1. $a \equiv a \pmod n$
2. *Se* $a \equiv b \pmod n$, *então* $b \equiv a \pmod n$
3. *Se* $a \equiv b \pmod n$ *e* $c \equiv d \pmod n$, *então* $a + c \equiv b + d \pmod n$
4. *Se* $a \equiv b \pmod n$ *e* $c \equiv d \pmod n$, *então* $ac \equiv bd \pmod n$
5. *Se* $a \equiv b \pmod n$, *então* $ac \equiv bc \pmod{nc}$
6. *Se* $a \equiv b \pmod n$, *então* $a^c \equiv b^c \pmod n$
7. *Se* $a \equiv b \pmod n$, *e* $c|n$, *então* $a \equiv b \pmod c$

Demonstra estes resultados. Não deves ter dificuldades se usares a definição. Apresentamos de seguida vários exemplos que ilustram bem as potencialidades desta ferramenta:

**Exemplo 1** *Encontra o resto de* $6^{2009}$ *a dividir por* 37.

**Demonstração.** $6^2 = 36 \equiv -1 \pmod{37}$, e assim $6^{2009} = 6 \times (6^2)^{1004} \equiv 6 \times (-1)^{1004} = 6 \pmod{37}$. Assim o resto da divisão é 6, porque $6^{2009} - 6$ é múltiplo de 37. ∎

**Exercício 5** *Calcula o resto da divisão de* $4^{2009}$ *por* 63.

**Exercício 6** *Calcula o último dígito de* $19^{2009}$.

**Exemplo 2** *Encontra* $n$ *inteiro tal que* $n^2 - 5$ *é múltiplo de* 13.

**Demonstração.**Seja $n$ esse inteiro. Então dividindo $n$ por 13 obtemos um resto $r$ tal que $0 \leq r < 13$ e $n \equiv r \pmod{13}$.

Então $n^2 \equiv r^2 \pmod{13}$. Por outro lado, $13|n^2 - 5$, ou seja $r^2 \equiv n^2 \equiv 5 \pmod{13}$. Mas calculando explicitamente verifica-se que não existe nenhum $r$ entre 0 e 12 tal que $r^2 \equiv 5 \pmod{13}$ e portanto não existe nenhum $n$ que verifiue o enunciado. ■

**Problema 4** *Seja* $n$ *um inteiro positivo. Prova que* $7|4^{2^n} + 2^{2^n} + 1$

Muitos problemas postos na forma "Encontra todos os $n$ tais que..." tem soluções deste tipo, ou seja: "Não existem soluções." Tenta agora voltar outra vez aos problemas do início. Apresentamos agora outra técnica importante na resolução de problemas de teoria de números:

**Lema 1**

$$a - b|a^n - b^n$$

**Demonstração.**

$$(a-b)\left(a^{n-1}b^0 + a^{n-2}b^1 + a^{n-3}b^2 + ... + a^2b^{n-3} + a^1b^{n-2} + a^0b^{n-1}\right) =$$

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

$$= a^n - b^n$$

Assim $(a-b)|(a^n - b^n)$.

■

**Exemplo 3** *Seja* $n$ *tal que* $2^n - 1$ *é primo. Prova que* $n$ *é primo.*

**Demonstração.**Suponhamos que é falso. Então existe $a > 1$ tal que $a|n$ e $a \neq n$. Mas então $2^a - 1|2^n - 1$ e $2^n - 1 > 2^a - 1 > 1$, o que impede $2^n - 1$ de ser primo. ■

**Lema 2** *Seja* $n$ *um inteiro e* $f(n)$ *a soma dos dígitos de* $n$. *Então* $n \equiv f(n)$ *(mod* 9*).*

**Demonstração.**Escrevemos a expansão decimal de $n$: $n = a_k a_{k-1}...a_1 a_0$, onde cada $a_i$ representa um dígito.

Então $n = 10^k a_k + 10^{k-1} a_{k-1} + ..., 10a_1 + a_0$. Mas $10 \equiv 1 \pmod 9$, logo $10^s \equiv 1^s \equiv 1 \pmod 9$ para qualquer $s \geq 1$ e assim $n \equiv a_k + ... + a_0 = f(n) \pmod 9$ ■

**Problema 5** *Prova que a soma dos dígitos de um quadrado pefeito nunca pode ser* 2009

**Problema 6** *Quantos $n$ existem entre* 1 *e* 2009 *tais que* $5|n^2 - 3n + 4$*?*

Se já resolveste todos os problemas até aqui, incluindo os do início, deixamos-te agora dois problemas que talvez não consigas resolver já mas que será um mero exercício no final da próxima sessão:

**Problema 7** *Seja $u_n = 2^n + 3^n + 6^n - 1$ para $n \geq 1$. Encontra todos os inteiros $a$ tais que $a$ é primo com todos os elementos da sequência.*

**Problema 8** *Encontra todos os inteiros $n$ para os quais existe um inteiro $a$ tal que* $2^n - 1|a^2 + 9$.