TEORIA DE NÚMEROS

Filipe Oliveira, 2008

Conteúdo

1 Introdução: Divisibilidade no anel $(\mathbb{Z}, +, \times)$

1.1 Noção de divisibilidade

Definição 1.1.1 *Sejam $a, b \in \mathbb{Z}$, $a \neq 0$.*
Diz-se que a divide b $(a|b)$ se existir $q \in \mathbb{Z}$ tal que $b = aq$.

Se $a|b$, diz-se ainda que b é divisivel por a ou que b é múltiplo de a.

Propriedades 1.1.2 *Sejam $a, b \in \mathbb{Z}$, $a \neq 0$.*

i. Para todo $a \in \mathbb{Z}/\{0\}$, $a|a$. (Reflexividade)

ii. Se $a|b$ então para todo $c \in \mathbb{Z}$, $a|bc$.

iii. $a|b \Leftrightarrow ma|mb$ para todo $m \in \mathbb{Z}$, $m \neq 0$.

iv.Se $a|b$ e $b|c$, então $a|c$. (Transitividade)

v. Se $a|b$ e $a|c$, então para todo $x, y \in \mathbb{Z}$, $a|xb + yc$.

vi. Se $a|b$ e $b \neq 0$, então $|a| \leq |b|$.

vii. Se $a|b$ e $b|a$, então $|a| = |b|$.

Prova:

i. Basta observar que a=1.a

ii. Se $a|b$, então existe $q \in \mathbb{Z}$, tal que $b = aq$.
Então $bc = aqc = q'a$ com $q' = qc \in \mathbb{Z}$. Por definição, $a|bc$.

iii. Basta observar que se $b = qa$, $bm = q(am)$.

iv. Como $a|b$ e $b|c$, existem $q_1, q_2 \in \mathbb{Z}$ com $b = aq_1$ e $c = bq_2$.

Assim, $c = bq_2 = aq_1q_2 = aq$, com $q = q_1q_2 \in \mathbb{Z}$. Por definição, $a|c$.

v. Como $a|b$ e $a|c$, existem $q_1, q_2 \in \mathbb{Z}$ com $b = aq_1$ e $c = aq_2$.
Sejam $x, y \in \mathbb{Z}$. Tem-se $xb + yc = xaq_1 + yaq_2 = a(xq_1 + yq_2)$, pelo que $a|xb + yc$.

vi. Seja $q \in \mathbb{Z}$ tal que $b = aq$.
Visto que $b \neq 0$, necessariamente $q \neq 0$, pelo que $|q| \geq 1$. Assim, $|b| = |aq| = |a|.|q| \geq |a|$.

vii. Basta utilizar o resultado da alínea vi. duas vezes.

1.2 Divisão Euclidiana

Será de extrema importância para o que se segue a noção de divisão euclidiana, que se enuncia aqui sob forma de teorema:

Teorema 1.2.1 - Divisão Euclidiana

Sejam $a, b \in \mathbb{Z}$, com $a > 0$.
Então existem dois únicos inteiros relativos q e r com as seguintes propriedades:

i. $b = aq + r$

ii. $0 \leq r < a$.

q e r são ditos respectivamente quociente e resto da divisão euclidiana de b por a.

Prova:

a) Existência
Considere-se o conjunto

$$S = \{b - am \ ; \ m \in \mathbb{Z} \text{ e } b - am \geq 0\}.$$

Tem-se $S \subset \mathbb{N}_o$ e $S \neq \emptyset$, logo pelo princípio de boa ordenação dos números inteiros naturais, S possui um mais pequeno elemento $r \geq 0$.
Visto que $r \in S$, existe $q \in \mathbb{Z}$ tal que $r = b - aq$, pelo que $b = aq + r$.

Provamos agora que $r < a$: Supondo que $r \geq a$, tem-se que $r = b - aq \geq a$, e $b - a(q + 1) \geq 0$, pelo que $b - a(q + 1) \in S$.
Mas $b - a(q + 1) < b - aq = r$, o que contradiz a minimalidade de r.

b) Unicidade
Suponhamos a existência de dois pares (q_1, r_1) e (q_2, r_2) que satisfazem as alíneas i. e ii. do teorema.
Então $b = aq_1 + r_1 = aq_2 + r_2 : a(q_1 - q_2) = r_2 - r_1$.
Dado que $r_1, r_2 \in [0; a[$, tem-se que $|r_2 - r_1| < a$.
Assim, $a|q_2 - q_1| = |a(q_1 - q_2)| = |r_2 - r_1| < a$. Como $a > 0$ conclui-se desta desigualdade que $|q_2 - q_1| < 1$. Como $q_2 - q_1 \in \mathbb{Z}$, necessariamente $q_2 = q_1$, o que implica também que $r_2 = r_1$.

Observação 1.2.1 *Seja $a, b \in \mathbb{Z}$, $a > 0$.*
Seja r o resto da divisão euclidiana de b por a.
Então

$$a|b \Leftrightarrow r = 0.$$

De facto, se $r = 0$, tem-se $b = aq$ e, por definição, $a|b$.
Reciprocamente, se $a|b$, então existe $q \in \mathbb{Z}$ com $b = aq = aq + 0$, pelo que $r = 0$.

1.3 Máximo Divisor Comum

Definição 1.3.1 *Sejam $a, b \in \mathbb{Z}$, $ab \neq 0$.*
Seja

$$S = \{c \in \mathbb{N} \ ; \ c|a \ e \ c|b\}.$$

$S \subset \mathbb{N}$, $1 \in S \neq \emptyset$ e S é majorado (por exemplo por $|a|$) pelo que S possui um elemento máximo d. d é então dito máximo divisor comum de a e b, e denota-se $d = (a, b)$.

Desta definição decorre de maneira imediata a seguinte propriedade:

Propriedade 1.3.2 *Sejam $a, b \in \mathbb{Z}$, $ab \neq 0$.*

$$d = (a, b)$$

$$\Leftrightarrow$$

i. $d|a$ e $d|b$

ii. Para todo $c \in \mathbb{Z}$ tal que $c|a$ e $c|b$, tem-se $c \leq d$.

O próximo teorema exprime a possibilidade de se obter o máximo divisor comum de dois inteiros como combinação linear dos mesmos (com coeficientes em $\mathbb{Z}$!!).

Teorema 1.3.1 *Sejam $a, b \in \mathbb{Z}$, $ab \neq 0$.*
Então existem $x_o, y_o \in \mathbb{Z}$ tais que $(a, b) = ax_o + by_o$.

Prova:
Considere-se o conjunto

$$S = \{ax + by \ ; \ x, y \in \mathbb{Z} \text{ e } ax + by > 0\}.$$

Sempre pelo princípio de boa ordenação dos números inteiros, S possui um elemento mínimo $d = ax_o + by_o$.

Mostramos agora que $d = (a, b)$, com a ajuda da Propriedade 1.3.2:

i) $d|a$ e $d|b$:

De facto, se $d \not| a$: sejam q e r o quociente e o resto da divisão euclidiana de a por d. Pela Observação 1.2.1, $a = qd + r$, com $q \in \mathbb{Z}$ e $0 < r < d$.
Tem-se $r = a - qd = a - q(ax_o + by_o) = a(1 - qx_o) + b(-qy_o) \in S$, o que contraria a minimalidade de d.
Assim $d|a$, e, por uma prova análoga, $d|b$.

ii) Seja $c \in \mathbb{Z}$ com $c|a$ e $c|b$. Devemos provar que então $c \leq d$.
De facto, pela Propriedade 1.1.2-iii., $c|ax_o + by_o = d$, e, pela alínea v.,
$c \leq |c| \leq |d| = d$.

Deste resultado resultam os seguintes corolários:

Corolário 1.3.3 *Sejam $a, b \in \mathbb{Z}$, $ab \neq 0$.*
Seja $c \in \mathbb{Z}$ tal que $c|a$ e $c|b$. Então $c|(a, b)$.

À luz do Teorema 1.3.1, a prova é imediata, já que existem $x_o, y_o \in \mathbb{Z}$ tais que $(a, b) = x_o a + y_o b$.

Corolário 1.3.4 *Sejam $a, b \in \mathbb{Z}$, $ab \neq 0$.*
O conjunto

$$S = \{ax + by \ ; \ x, y \in \mathbb{Z}\}$$

constitui o conjunto dos múltiplos de $d = (a, b)$.

Prova: Seja $M = \{md \ ; \ m \in \mathbb{Z}\}$. Pretende-se provar que $M = S$.
Seja $\alpha \in M$: $\alpha = md = m(ax_o + by_o) = a(mx_o) + b(my_o) \in S$, pelo Teorema 1.3.1.
Seja $\alpha \in S$: $\alpha = ax + by$. $d|a$, $d|b$, logo $d|ax + by = \alpha$. Assim, existe $m \in \mathbb{Z}$ tal que $\alpha = md$ e $\alpha \in M$.

Seguem-se algumas propriedades elementares do máximo divisor comum:

Teorema 1.3.2 *Sejam $a, b \in \mathbb{Z}$, $ab \neq 0$, $d = (a, b)$ e $m \in \mathbb{Z}$.*
Então:

i. $(a, b + ma) = (a, b) = (a, -b)$.

ii. $(am, bm) = |m|(a, b)$ *se* $m \neq 0$.

iii. $(\frac{a}{d}, \frac{b}{d}) = 1$.

iv. Se $g \in \mathbb{Z}$, $g \neq 0$, é tal que $g|a$ e $g|b$, então $(\frac{a}{g}, \frac{b}{g}) = \frac{1}{|g|}(a, b)$.

Prova:

i. Seja $g = (a, b + ma)$. $g|a$ e $g|b + ma$. Logo $g|(b + ma).1 + (-m).a = b$. Assim, pelo Corolário 1.3.3 $g|a$ e $g|b$: $g|(a, b) = d$.
Por outro lado, $d|a$ e $d|b$, pelo que $d|b + ma$. De novo pelo Corolário 1.3.3, $d|(a, b + ma) = g$.
Pela Propriedade 1.1.2-vii., $|g| = |d|$.
Como por definição do máximo divisor comum se tem $d > 0$ e $g > 0$, $d = g$.
A outra igualdade decorre de uma prova análoga.

ii. Suponhamos que $m > 0$.
Seja $d = (a, b)$. $d|a$ e $d|b$, logo $dm|am$ e $dm|bm$. Pelo Corolário 1.3.3, $dm|(am, bm)$. Por definição, existe $k \in \mathbb{Z}$ tal que $(am, bm) = kdm$.
Desta igualdade se tira que $kdm|am$ e $kdm|bm$. Pela Propriedade 1.1.2-iii., $kd|a$ e $kd|b$. Logo

$kd|d$ pelo Corolário 1.3.3.
Pela Propriedade 1.1.2-vi., $|k|d = |kd| \leq d$: $k = 1$ e $md = (am, bm)$.

Se $m < 0$, $(am, bm) = (-am, -bm) = -m(a, b) = |m|(a, b)$.

iii. $d = (a, b) = (d\frac{a}{d}, d\frac{b}{d}) = d(\frac{a}{d}, \frac{b}{d})$, logo $(\frac{a}{d}, \frac{b}{d}) = 1$.

iv. Basta proceder como na alínea anterior.

A noção de máximo divisor comum pode facilmente ser generalizada para uma família de n inteiros:

Definição 1.3.5 *Sejam $a_1, \ldots a_n$ n inteiros não nulos.*
Define-se $d = (a_1, \ldots, a_n)$, o máximo divisor comum dos inteiros $a_1, \ldots, a_n$ como o maior natural que verifica as seguintes propriedades:

i. $\forall j \in \{1, \ldots, n\}$, $d|a_j$.

ii. Seja $c \in \mathbb{Z}$. Se $\forall j \in \{1, \ldots, n\}$, $c|a_j$, emtão $c \leq d$.

A prova do seguinte teorema fica ao cuidado do leitor:

Teorema 1.3.3 *Sejam $a_1, \ldots, a_n$ n inteiros não nulos e seja $d = (a_1, \ldots, a_n)$.*
Então

$$\{\sum_{j=1}^{n} x_j a_j \ ; \ (x_1, \ldots, x_n) \in \mathbb{Z}^n\} = \{md \ ; \ m \in \mathbb{Z}\}.$$

Nota: Em particular existem $x_{1_o}, \ldots, x_{n_o} \in \mathbb{Z}$ tais que $d = \sum_{j=1}^{n} x_{j_o} a_j$.

1.4 Algoritmo de Euclides

Neste capítulo apresentamos um método que permite, na prática, calcular o máximo divisor comum de dois inteiros não nulos a e b, bem como escrevê-lo como combinação linear de a e b,

o que, pelo Teorema 1.3.1, é sempre possivel.

Sejam a e b dois inteiros não nulos, com $a > 0$. Começa-se por executar a divisão euclidiana de b por a:

$$b = aq_1 + r_1 \ , \ 0 \leq r_1 < a.$$

De seguida faz-se a divisão euclidiana de a por r_1:

$$a = r_1 q_2 + r_2 \ , \ 0 \leq r_2 < r_1.$$

Sucessivamente, executa-se a divisão euclidiana de r_j por r_{j+1}:

$$r_j = q_{j+2} r_{j+1} + r_{j+2} \ , \ 0 \leq r_{j+2} < r_{j+1}.$$

A sucessão (r_j) é uma sucessão estritamente decrescente de inteiros positivos ou nulos, pelo que ao fim de um número finito de N etapas, $r_N = 0$:

$$r_{N-4} = q_{N-2} r_{N-3} + r_{N-2}$$

$$r_{N-3} = q_{N-1} r_{N-2} + r_{N-1}$$

$$r_{N-2} = q_N r_{N-1} + 0.$$

Tem-se então

$$(a, b) = (a, aq_1 + r_1) = (a, r_1) = (r_1 q_2 + r_2, r_1) = (r_2, r_1) = \cdots =$$

$$= (r_{j+1}, r_j) = \cdots = (r_{N-1}, r_{N-2}) = (r_{N-1}, q_n r_{N-1}) = r_{N-1}.$$

Por outro lado,

$$(a, b) = r_{N-1} = r_{N-3} - q_{N-1} r_{N-2} = r_{N-3} - q_{N-1}(r_{N-4} - q_{N-2} r_{N-3}) =$$

$$= r_{N-3}(1 + q_{N-1} q_{N-2}) + r_{N-4}(-q_{N-1}) = \ldots$$

Na segunda igualdade, (a, b) encontra-se expresso como combinação de r_{N-2} e r_{N-3}, de seguida aparece como combinação de r_{N-3} e r_{N-4},...,continuando o algoritmo acaba-se por obter (a, b) como combinação de a e b.

Exemplo: $a = 68$, $b = 126$.

$$116 = 1.68 + 48 : \ r_1 = 48$$

$$68 = 1.48 + 20 : \ r_2 = 20$$

$$48 = 2.20 + 8 : \ r_3 = 8$$

$$20 = 2.8 + 4 : \ r_4 = 4$$

$$8 = 2.4 + 0 : r_5 = 0$$

Assim, $(116, 68) = 4$, e

$$4 = 20 - 2.8 = 20 - 2.(48 - 2.20) = -2.48 + 5.20 = -2.48 + 5.(68 - 1.48) = 5.68 - 7.48 =$$

$$= 5.68 - 7(116 - 1.68) = 12.68 + (-7).116$$

1.5 Teorema de Bezout e Lema de Euclides

Apresentamos nesta secção duas propriedades elementares mas de importância capital: o teorema de Bezout e o lema de Euclides.

Começamos por definir o conceito de números primos entre si:

Definição 1.5.1 *Sejam $a_1, \ldots, a_n$ n inteiros não nulos.*
Diz-se que $a_1, \ldots, a_n$ são primos entre si se $(a_1, \ldots, a_n) = 1$.

Teorema 1.5.1 *Teorema de Bezout*
Sejam $a, b \in \mathbb{Z}$, $ab \neq 0$.
Então

$$(a, b) = 1 \Leftrightarrow \exists (x_o, y_o) \in \mathbb{Z}^2 \ , \ ax_o + by_o = 1.$$

Prova:

$\Rightarrow$ Trata-se de uma aplicação directa do Teorema 1.3.1.

$\Leftarrow$ Seja $d = (a, b)$: $d|a$ e $d|b$, logo $d|ax_o + by_o = 1$: $d = 1$.

Teorema 1.5.2 *Sejam $a, b, m \in \mathbb{Z}$, $abm \neq 0$.*
Então

$$(a, m) = (b, m) = 1 \Leftrightarrow (ab, m) = 1,$$

i.e., m é primo com a e b se e só se m for primo com ab.

Prova:

$\Leftarrow$ Sejam x_o, y_o com $abx_o + my_o = 1$. Então $a(bx_o) + m(y_o) = 1 : (a, m) = 1$, e, da mesma forma, $(b, m) = 1$.

$\Rightarrow$ Sejam x_o, y_o, x'_o, y'_o tais que $ax_o + my_o = 1$ e $bx'_o + my'_o = 1$.
Multiplicando estas duas igualdades vem $x_o x'_o ab + m(y'_o x_o a + y_o x'_o b + y_o y'_o m) = 1 : (ab, m) = 1$.

Por indução, facilmente se deduz o seguinte corolário:

Corolário 1.5.2 *Sejam $a, b \in \mathbb{Z}$, $ab \neq 0$.*

Se $(a, b) = 1$ então para todo $n, k \in \mathbb{N}$, $(a^n, b^k) = 1$.

Teorema 1.5.3 : Lema de Euclides
Sejam $a, b, c \in \mathbb{Z}$, $abc \neq 0$.
Se $a|bc$ e $(a, b) = 1$ então $a|c$.

Prova:

Sejam x_o, y_o tais que $ax_o + by_o = 1$. Então $c = x_o ac + y_o bc$. Tem-se que $a|ac$, e, por hipótese, $a|bc$. Logo $a|x_o ac + y_o bc = c$.

1.6 Mínimo múltiplo comum

Definição 1.6.1 *Sejam $a_1, \ldots, an$ n inteiros não nulos.*
Diz-se que m é múltiplo comum de $a_1, \ldots, an$ se para todo $j \in \{1, \ldots, n\}$, $a_j|m$.
Define-se

$$[a_1, \ldots, a_n] = \min\{m \in \mathbb{N} \ , \ m \text{ é múltiplo comum dos } a_j \ , \ 1 \leq j \leq n.\}$$

o mínimo múltiplo comum de $a_1, \ldots, a_n$.

Note-se que o conjunto $S = \{m \in \mathbb{N} \ ; \ m$ é múltiplo comum dos $a_j \ , \ 1 \leq j \leq n\}$ é não vazio visto que $|a_1 a_2 \ldots a_n| \in E$. Como $S \subset \mathbb{N}$, o princípio de boa ordenação garante a existência de um elemento mínimo em S.

Propriedades 1.6.2

i.Se m é múltiplo comum de $a_1, \ldots, a_n$, $[a_1, \ldots, a_n] | m$.

ii. Se $k > 0$, $k[a_1, \ldots, a_n] = [ka_1, \ldots, ka_n]$.

iii. $[a, b](a, b) = |ab|$.

Prova:

i. Seja $M = [a_1, \ldots, a_n]$. Efectuando a divisão euclidiana de m por M obtem-se $m = qM + r$, $0 \leq r < M$.
Basta provar que $r = 0$. Supondo que $r > 0$, para todo $j \in \{1, \ldots, n\}$, $a_j | m$ e $a_j | M$, logo $a_j | m - qM = r$ e r é múltiplo comum de $a_1, \ldots, a_n$. Obtem-se a contradição observando que $r < M$.

ii. Seja $M = [a_1, \ldots, a_n]$ e $m = [ka_1, \ldots, ka_n]$. Para todo $j \in \{1; \ldots; n\}$, kM é múltiplo de ka_j, pelo que $kM \geq m$.
Por outro lado, m é múltiplo de cada ka_j, pelo que $\frac{m}{k}$ é um inteiro, múltiplo de cada a_j. Assim, $\frac{m}{k} \geq M : m \geq kM$ e $m = kM$.

iii. Basta provar o resultado para $a, b > 0$, visto que $(a, b) = (-a, b)$ e $[a, b] = [-a, b]$. Comecemos por considerar o caso em que a e b são primos entre si:
$[a; b]$ é múltiplo de a, logo existe $k \in \mathbb{N}$ com $ka = [a; b]$. Tambem, $b | [a, b]$ logo $b | ka$. Como $(a, b) = 1$, pelo lema de Euclides, $b | k$ e $b \leq k$. Assim, $[a, b] \geq ab$. Por outro lado, ab é múltiplo comum de a e b: por definição $[a, b] \leq ab$: $ab = [a, b] = [a, b](a, b)$.

No caso geral, seja $d = (a, b)$. Então, pelo Teorema 1.3.2, alínea iii., $(\frac{a}{d}, \frac{b}{d}) = 1$. Sabemos então que $[\frac{a}{d}, \frac{b}{d}] = \frac{ab}{d^2}$. Multiplicando por d^2 obtem-se o resultado.

1.7 Números primos e Teorema fundamental da aritmética

Definição 1.7.1 *Um inteiro $p \geq 2$ é dito número primo se os seus únicos divisores forem 1 e p. O conjunto de todos os números primos será notado $\mathbb{P}$.*

Propriedades 1.7.2 *Sejam $a, b \in \mathbb{Z}$ e $p \in \mathbb{P}$.*

i. Se $p \not| a$, $(p, a) = 1$.

ii. Se $p|ab$ então $p|a$ ou $p|b$.

Prova:

i. Basta observar que os únicos divisores de p são 1 e p. Assim $(a, p) = 1$ ou $(a, p) = p$. Como $p \not| a$, $(p, a) = 1$.

ii. Suponhamos que $p \not| a$. Pela alínea anterior, $(a, p) = 1$. Como $p|ab$, pelo lema de Euclides, obtem-se que $p|b$.

Da alínea ii. resulta facilmente por indução o seguinte corolário:

Corolário 1.7.3 *Sejam $a_1 \dots a_n$ n inteiros e $p \in \mathbb{P}$.*

Se $p|a_1 a_2 \dots a_n$ então existe $j \in \{1; \dots; n\}$ tal que $p|a_j$.

Teorema 1.7.1 : Teorema fundamental da aritmética
Todo número natural N pode ser representado de maneira única na forma

$$N = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n},$$

onde para todo $j \in \{1; \dots; n\}$, $p_j \in \mathbb{P}$, $p_1 < p_2 < \dots < p_n$ e $a_j \in \mathbb{N}$.

Prova:
a) Existência da decomposição:

Seja $N \in \mathbb{N}$. Se N primo, não há nada a provar. Se N não é primo, seja o conjunto

$$S = \{d \in \mathbb{N} \ ; \ d|N \text{ e } 1 < d < N\}.$$

Por hipótese, $S \neq \emptyset$, pelo que S possui um mais pequeno elemento q_1.
Tem-se $q_1 \in \mathbb{P}$: se não fosse o caso, existiria um elemento $P_1 \in]1; q_1[$ com $P_1|q_1$. Como $q_1|N$,

ter-se-ia $P_1|N$ e $P_1 \in S$, o que contradiz a minimalidade de q_1.
Assim, $N = q_1 n_1$, $n_1 \in \mathbb{N}$. Se $n_1 \in \mathbb{P}$, a prova está terminada. Senão, repete-se o algoritmo, e existe $q_2 \in \mathbb{P}$ tal que $q_2|n_1$, e $N = q_1 q_2 n_2$, $n_2 \in \mathbb{N}$.
De notar que a sucessão n_j assim formada é estritamente decrescente, pelo que ao fim de um número finito de r etapas, $n_r = 1$ e $N = q_1 q_2 \dots q_r$, com $q_j \in \mathbb{P}$.

b) Unicidade da decomposição:

Suponhamos que $N = q_1 q_2 \dots q_n = q'_1 q'_2 \dots q'_s$, onde as duas decomposições diferem.
Simplificamos esta equação por forma a obter

$$q_{i_1} q_{i_2} \dots q_{i_\alpha} = q'_{i_1} q'_{i_2} \dots q'_{i_\beta}$$

tal que $\forall j$, $\forall k$, $q_j \neq q'_k$.
Observe-se então que $q_{i_1}|q'_{i_1} q'_{i_2} \dots q'_{i_\beta}$. Pelo Corolário 1.7.3, existe k tal que $q_{i_1}|q'_k$. Como $q'_k \in \mathbb{P}$, $q_{i_1} = q'_k$, o que é uma contradição.

Deste teorema resulta o seguinte critério de divisibilidade:

Teorema 1.7.2 *Seja* $n \in \mathbb{N}$, $n = \prod_{i=1}^{r} q_i^{a_i}$, *com* $q_i \in \mathbb{P}$, $a_i > 0$ *e seja* $d > 0$.
Então

$$d|n \Leftrightarrow d = \prod_{i=1}^{r} q_i^{b_i} \text{ , para certos } b_i \in \{0; \dots a_i\}.$$

Prova:

Suponhamos que $d = \prod_{i=1}^{r} q_i^{b_i}$, $b_i \in \{0; \dots a_i\}$.
Então

$$n = \prod_{i=1}^{r} q_i^{a_i} = \prod_{i=1}^{r} q_i^{b_i} \prod_{i=1}^{r} q_i^{a_i - b_i} = d \prod_{i=1}^{r} q_i^{a_i - b_i}.$$

Visto que $r = \prod_{i=1}^{r} q_i^{a_i - b_i} \in \mathbb{Z}$, $d|n$.
Inversamente, suponhamos que $d|n$, isto é, existe $r \in \mathbb{Z}$ tal que $n = qd$.

Consideremos as decomposições canónicas em factores primos de r e d:

$$d = \prod_{i=1}^{r} q_i^{b_i} \text{ , } r = \prod_{i=1}^{r} q_i^{c_i},$$

com $c_i, b_i \in \mathbb{N}_o$.

Assim, $n = qd = \prod_{i=1}^{r} q_i^{b_i+c_i}$, pelo que $a_i = b_i + c_i \geq b_i$.

Este critério permite ainda calcular de maneira prática o máximo divisor comum e o mínimo múltiplo comum de entre dois inteiros a e b positivos:

Propriedade 1.7.4 *Sejam* $a = \prod_{i=1}^{r} q_i^{a_i}$ *e* $b = \prod_{i=1}^{r} q_i^{b_i}$ *dois inteiros positivos, com* $q_i \in \mathbb{P}$ *e* $a_i, b_i \in \mathbb{N}_o$.
Então

$$(a,b) = \prod_{i=1}^{r} q_i^{\min\{a_i,b_i\}} \text{ e } [a,b] = \prod_{i=1}^{r} q_i^{\max\{a_i,b_i\}}.$$

Na prática, para verificar se um certo inteiro n é primo, seria necessário testar se n é divisivel por algum elemento do conjunto $\{2; 3; \ldots; n-1\}$.

Na realidade, não é necessário testar todos estes números:

Propriedade 1.7.5 *Seja* $n \in \mathbb{N}$. *Se para todo inteiro* $m \in [2; \sqrt{n}]$, $m \nmid n$, $n \in \mathbb{P}$.

Prova:

Seja $n \in \mathbb{N}$ um tal inteiro. Supondo que $n \notin \mathbb{P}$, existem dois inteiros $n_1 \neq 1$ e $n_2 \neq 1$ tais que $n = n_1 n_2$.
Então, $n = n_1 n_2 > \sqrt{n}\sqrt{n} = n$, o que é uma contradição.

Terminamos com duas propriedades elementares do conjunto dos números primos $\mathbb{P}$:

Teorema 1.7.3 *O conjunto* $\mathbb{P}$ *é infinito.*

Prova:

De facto, suponhamos que $\mathbb{P} = \{p_1, p_2, \ldots, p_n\}$, com $n \in \mathbb{N}$.

Consideremos o inteiro $N = p_1 p_2 \dots p_n + 1$. Como $N > p_n$, $N \notin \mathbb{P}$. Seja então p_k um divisor primo de N: $p_k | N$, $p_k | p_1 p_2 \dots p_n$, logo $p_k | N - p_1 p_2 \dots p_n = 1$, o que é absurdo.

Teorema 1.7.4 *Seja $\{p_n\}_{n\in\mathbb{N}}$ a sucessão dos números primos, ordenados de maneira crescente.*

A série $\sum \frac{1}{p_n}$ diverge.

Note que um corolário deste teorema é a infinidade do conjunto $\mathbb{P}$. (!!)

Comecemos por provar o seguinte lema:

Teorema 1.7.1 *Seja $k \in \mathbb{N}$ e $p_1, p_2, \dots, p_k$ os k primeiros números primos.*
Consideremos os conjuntos

$$N_k = \{n \in \mathbb{N} \ ; \ n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \ , \ \alpha_j \in \mathbb{N}\}$$

e, para $x \geq 1$,

$$N_k(x) = \{n \leq x \ ; \ n \in N_k\}.$$

Então,

$$\forall x \geq 1 \ , \ card\,(N_k(x)) \leq 2^k \sqrt{x}.$$

Prova:

Seja $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \in N_k(x)$. O inteiro n pode ser escrito sob a forma

$$n = n_1^2 p_1^{r_1} p_2^{r_2} \dots p_k^{r_k},$$

onde $n_1 \in \mathbb{N}$ e $r_j \in \{0; 1\}$. Para observar este facto, basta fazer a divisão euclidiana de α_j por 2: $\alpha_j = 2\beta_j + r_j$, $\beta_j \in \mathbb{N}_o$ e $p = \left(p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}\right)^2 p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$.

Visto que $n \leq x$, $n_1^2 \leq x$: $n_1 \leq \sqrt{x}$. Assim, n_1 pode tomar no máximo $\sqrt{x}$ valores distintos.

O produto $p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ pode tomar exactamente 2^k valores distintos, pelo que
$card\,(N_k(x)) \leq 2^k \sqrt{x}$, o que conclui a prova.

Prova do teorema 1.7.4:

Suponhamos que a série $\sum \frac{1}{p_n}$ é convergente. Então a sua série resto tende para 0: seja k tal que $\sum_{n=k+1}^{\infty} \frac{1}{p_n} < \frac{1}{2}$.

Consideremos os conjuntos

$$M_k = \mathbb{N}/N_k = \{n \in \mathbb{N} \ ; \ \exists p \in \mathbb{P},\ p > p_k \text{ e } p|n\}$$

e, para $x \geq 1$,

$$M_k(x) = \{n \leq x \ ; \ n \in M_k\}.$$

Claramente, quando x é um inteiro positivo, $card\,(N_k(x)) + card\,(M_k(x)) = x$.

Por outro lado,

$$card\,(M_k(x)) \leq card\,(\{n \in \mathbb{N} \ ; \ p_{k+1}|x\}) + card\,(\{n \in \mathbb{N} \ ; \ p_{k+2}|x\}) + \cdots \leq \sum_{n=k+1}^{\infty} \frac{x}{p_n} < \frac{x}{2}.$$

Assim, $card\,(N_k(x)) = x - card\,(M_k(x)) > \frac{x}{2}$.
Pelo lema,

$$\frac{x}{2} < card\,(N_k(x)) < \sqrt{x}2^k,$$

de onde se conclui que para todo inteiro x, $\sqrt{x} < 2^{k+1}$, o que é obviamente absurdo.

2 Revisões: Grupos e Aneis Quociente

2.1 Estrutura quociente

Definição 2.1.1 *Seja G um conjunto.*
A relação binária $\mathcal{R}$ diz-se relação de equivalência se:

i. $\forall x \in G,\ x\mathcal{R}x$. *(Reflexividade)*

ii. $\forall x, y \in G,\ x\mathcal{R}y \Rightarrow y\mathcal{R}x$. *(Simetria)*

iii. $\forall x, y, z \in G$, $x\mathcal{R}y$ *e* $y\mathcal{R}z \Rightarrow x\mathcal{R}z$. *(Transitividade)*

Nestas condições define-se, para $x \in G$, a classe de equivalência de x por:

$$\overline{x} = \{y \in G; x\mathcal{R}y\},$$

ou seja, o conjunto dos elementos de G que estão em relação com x.

Define-se então o quociente

$$G/\mathcal{R} = \{\overline{x}; x \in G\},$$

o conjunto formado de todas as classes de equivalência de elementos de G.

Propriedade 2.1.2 *Seja G um conjunto e $\mathcal{R}$ uma relação de equivalência sobre G.*
Então o conjunto das suas classes de equivalência (isto é, os elementos de $G/\mathcal{R}$) formam uma partição de G, ou seja:

i. $\bigcup_{A \in G/\mathcal{R}} A = G$

ii. Para todo $A, B \in G/\mathcal{R}$, se $A \neq B$ então $A \cap B = \emptyset$.

Daqui resulta facilmente que todo elemento de G pertence a uma e a uma só classe de equivalência.

Prova:

i. Por definição, tem-se $\bigcup_{A\in G/\mathcal{R}} A \subset G$.

Por outro lado, seja $x_o \in G$.
Como $\mathcal{R}$ é reflexiva, $x_o\mathcal{R}x_o$, pelo que $x_o \in \overline{x_o} \subset \bigcup_{A\in G/\mathcal{R}} A$ de onde se conclui que

$G \subset \bigcup_{x\in G/\mathcal{R}} A$.

ii. Sejam A e B duas classes de equivalência, com $A \cap B \neq \emptyset$.
Vamos provar que então $A = B$.

Seja $z \in A \cap B$ e $x, y \in G$ com $A = \overline{x}$ e $B = \overline{y}$.
Por definição, $x\mathcal{R}z$ e $y\mathcal{R}z$. Como $\mathcal{R}$, é simétrica, tem-se $z\mathcal{R}y$.
Como $\mathcal{R}$ é transitiva, de $x\mathcal{R}z$ e $z\mathcal{R}y$ deduz-se que $x\mathcal{R}y$.

É agora fácil provar que $\overline{x} = \overline{y}$. De facto, seja $w \in \overline{y}$. Por definição, $y\mathcal{R}w$.
Uma vez mais por transitividade, $x\mathcal{R}w$:
$w \in \overline{x}$ de onde se conclui que $\overline{y} \subset \overline{x}$.
Prova-se a outra inclusão de fórmula análoga, pelo que $A = B$.

Exemplo: $G = \mathbb{Z}$ e $\mathcal{R}$ a relação binária definida por:

$$\forall x, y \in \mathbb{Z}\ ,\ x\mathcal{R}y \Leftrightarrow 2|x - y.$$

Verifica-se facilmente que $\mathcal{R}$ é uma relação de equivalência.
Vamos agora determinar $\overline{1}$:

$$x \in \overline{1} \Leftrightarrow 1\mathcal{R}x \Leftrightarrow 2|x-1 \Leftrightarrow \exists n \in \mathbb{Z}\ ,\ x - 1 = 2n \Leftrightarrow \exists n \in \mathbb{Z}\ ,\ x = 2n + 1 \Leftrightarrow x \text{ é impar:}$$

$$\overline{1} = \{\dots, -5, -3, -1, 1, 3, 5, \dots\}$$

Da mesma forma,

$$x \in \overline{0} \Leftrightarrow 0\mathcal{R}x \Leftrightarrow 2|x - 0 \Leftrightarrow \exists n \in \mathbb{Z}\ ,\ x = 2n \Leftrightarrow x \text{ é par:}$$

$$\overline{0} = \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\}.$$

Temos assim duas únicas classes de equivalência:

$$\mathbb{Z}/\mathcal{R} = \{\overline{0}, \overline{1}\} = \{\{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\}, \{\dots, -5, -3, -1, 1, 3, 5 \dots\}\}.$$

De notar que $\overline{0} \cup \overline{1} = \mathbb{Z}$ e $\overline{0} \cap \overline{1} = \emptyset$, ou seja, $\overline{0}$ e $\overline{1}$ formam uma partição de $\mathbb{Z}$.

2.2 Grupo quociente

Comecemos por observar o seguinte:

Propriedade 2.2.1 *Seja $(G, *)$ um grupo e H um subgrupo de G.*
Então a relação binária definida por

$$\forall x, y \in G \ , \ x\mathcal{R}y \Leftrightarrow x * y^{-1} \in H$$

é uma relação de equivalência sobre G.

Prova:

i. Seja $x \in G$. Então, $x * x^{-1} = 1_G \in H$: $x\mathcal{R}x$.

ii. Sejam $x, y \in G$, com $x\mathcal{R}y$. Então, $x*y^{-1} \in H$. Como H é subgrupo, $(x*y^{-1})^{-1} = y*x^{-1} \in H$: $y\mathcal{R}x$.

iii. Sejam $x, y, z \in G$, com $x\mathcal{R}y$ e $y\mathcal{R}z$. Então, $x * y^{-1} \in H$ e $y * z^{-1} \in H$.
Assim, $(x * y^{-1}) * (y * z^{-1}) = x * z^{-1} \in H : x\mathcal{R}z$.

Assim, podemos considerar o quociente $G/\mathcal{R}$.

O passo seguinte será "transportar"a operação $*$ (definida em G) para $G/\mathcal{R}$. Como é possivel definir uma operação sobre este conjunto à custa da operação * ?

A ideia mais simples seria a seguinte: dadas duas classes de equivalencia A e B de $G/\mathcal{R}$, tomar um representante de cada uma destas classes, isto é, dois elementos $a, b \in G$ tais que

$$A = \overline{a} \text{ e } B = \overline{b},$$

e definir então a operação entre classes por

$$A * B = \overline{a * b}.$$

Obviamente, para se ter assim uma definição coerente, seria necessário que $\overline{a * b}$ não dependesse dos representantes a e b escolhidos ao acaso nas classes A e B.

Mais precisamente, a operação entre classes está correctamente definida se:

$$\forall a, b \in G \ , \ \forall \alpha \in \overline{a} \ , \ \forall \beta \in \overline{b} \ , \ \overline{ab} = \overline{\alpha\beta}$$

$$\Leftrightarrow$$

$$\forall a, b, \alpha, \beta \in G \ , \ \alpha \mathcal{R} a \text{ e } \beta \mathcal{R} b \Rightarrow \alpha * \beta \mathcal{R} a * b. \tag{2.1}$$

Podemos provar a seguinte propriedade:

Propriedade 2.2.2 *Seja $(G; *)$ um grupo e H um subgrupo de G.*
Seja $\mathcal{R}$ a relação binária definida por

$$\forall x, y \in G \ , \ x \mathcal{R} y \text{ sse } x * y^{-1} \in H.$$

Então, $\mathcal{R}$ goza da propriedade (2.1) se e só se

$$\forall x \in G \ , \ x * H * x^{-1} \subset H,$$

isto é, $\forall x \in G \ , \ \forall h \in H \ , \ x * h * x^{-1} \in H$.

Prova:

$\Rightarrow$ Sejam $a, \alpha, b, \beta \in G$, com $\alpha \mathcal{R} a$ e $\beta \mathcal{R} b$: $\alpha * a^{-1} \in H$ e $\beta * b^{-1} \in H$.
Então,

$$(\alpha * \beta) * (a * b)^{-1} = \alpha * \beta * b^{-1} * a^{-1} = [\alpha * a^{-1}] * a * [\beta * b^{-1}] * a^{-1}.$$

Como $[\beta * b^{-1}] \in H$, $a * [\beta * b^{-1}] * a^{-1} \in H$ e, finalmente, $(\alpha * \beta) * (a * b)^{-1} \in H$: $\alpha * \beta \mathcal{R} a * b$.

$\Leftarrow$ Seja $h \in H$ e $x \in G$.
Temos que $h \mathcal{R} 1$ e $x \mathcal{R} x$, pelo que $x * h \mathcal{R} x * 1$, o que significa que

$$(x * h) * (x * 1)^{-1} = x * h * x^{-1} \in H.$$

Os subgrupos H que verificam a condição da Propriedade 2.2.2 são ditos normais, ou distinguidos, ou ainda invariantes.

Se H é distinguido, podemos assim definir uma operação $*$ no quociente $G/\mathcal{R}$. Na realidade o resultado é ligeiramente mais forte:

Teorema 2.2.1 *Seja $(G, *)$ um grupo e H um subgrupo distinguido de G.*
Seja $\mathcal{R}$ a relação de equivalência dada por

$$\forall x, y \in G \ , \ x * y^{-1} \in H.$$

Então a operação definida nos elementos do quociente $G/\mathcal{R}$ por

$$\forall \overline{x}, \overline{y} \in G/\mathcal{R} \ , \ \overline{x} * \overline{y} = \overline{x * y}$$

confere a $G/\mathcal{R}$ uma estrutura de grupo. Este grupo é dito grupo quociente de G por H e denota-se por G/H.

Prova:

De facto, é fácil observar que a operação $*$ definida em $G/\mathcal{R}$ é interna e associativa, que a classe do neutro de G, $\overline{1}$, é elemento neutro e finalmente que $\overline{x^{-1}}$ é o inverso de $\overline{x}$: $\overline{x^{-1}} = \overline{x}^{-1}$.

Para terminar, eis alguns subgrupos normais famosos: (prove que de facto o são!)

- Os subgrupos de um grupo comutativo G.
- Os núcleos dos homomorfismos de grupo
- O centro do grupo , isto é, o subgrupo definido por:

$$\mathcal{Z}_G = \{y \in G \ ; \ \forall x \in G \ , \ x * y = y * x\}.$$

2.3 Aneis Quociente

Seja $(A, +, \times)$ um anel e I um subgrupo aditivo do grupo $(A, +)$.
Como por definição de anel, este grupo é abeliano, I é automaticamente um subgrupo normal, pelo que podemos considerar o grupo quociente A/I, com a operação "+", herdada da operação aditiva do anel A.

Note que esta operação, na secção anterior, era denotada "$_*$".
Temos pois $A/I = A/\mathcal{R}$, onde $\mathcal{R}$ é definida por

$$x \mathcal{R} y \text{ sse } x * y^{-1} = x + (-y) = x - y \in I.$$

Gostariamos agora de definir uma estrutura de anel em A/I, pelo que devemos definir uma operação multiplicativa neste quociente.

Seria obviamente interessante transportar a operação $\times$ de A para A/I. Como vimos no capítulo anterior, a condição para o poder fazer é

$$\forall a, b, \alpha, \beta \in A \ , \ a\mathcal{R}\alpha \text{ e } b\mathcal{R}\beta \Rightarrow a \times b\mathcal{R}\alpha \times \beta. \tag{2.2}$$

A condição necessária e suficiente para que tal se verifique é que I verifique as propriedades da seguinte definição:

Definição 2.3.1 *Seja $(A, +, \times)$ um anel e $(I, +)$ um subgrupo de (A,+).*

I é dito um ideal de A se

$$\forall x \in A \ , \ x \times I \subset I \ e \ I \times x \subset I,$$

isto é

$$\forall x \in A \ , \ \forall i \in I \ , \ x \times i \in I \ e \ i \times x \in I.$$

Como anunciado, temos a seguinte propriedade:

Propriedade 2.3.2
A relação de equivalência $\mathcal{R}$ goza da propriedade de compatibilidade (2.2) se e só se I for um ideal de A.

Prova:

$\Leftarrow$ Sejam $a, b, \alpha, \beta \in A$, com $a\mathcal{R}\alpha$ e $b\mathcal{R}\beta$.
Tem-se $a - \alpha \in I$ e $b - \beta \in I$ por definição de $\mathcal{R}$.

Como I é ideal, $(a - \alpha) \times b \in I$ e $\alpha \times (b - \beta) \in I$.
Finalmente, como I é um grupo,

$$a \times b - \alpha \times \beta = (a - \alpha) \times b + \alpha \times (b - \beta) \in I,$$

pelo que $a \times b\mathcal{R}\alpha \times \beta$.

$\Rightarrow$ Seja $x \in A$ e $i \in I$.

$i - 0 \in I$ e $x - x = 0 \in I$, pelo que $i\mathcal{R}0$ e $x\mathcal{R}x$.

Assim, por (2.2), $i \times x \mathcal{R} 0 \times x = 0$ e $x \times i \mathcal{R} x \times 0 = 0$, ou seja

$$i \times x - 0 = i \times x \in I \text{ e } x \times i - 0 = x \times i \in I.$$

Assim, quando I é um ideal de A, é possivel definir em A/I uma multiplicação herdada da multiplicação de A. Na realidade, o resultado é um pouco mais forte:

Teorema 2.3.1 *Seja $(A, +, \times)$ um anel e I um ideal de A.*
Seja $\mathcal{R}$ a relação de equivalência definida por

$$\forall x, y \in A \ , \ x \mathcal{R} y \text{ sse } x - y \in I.$$

Então as operações (bem) definidas no quociente $A/\mathcal{R}$ por

$$\forall x, y \in A \ , \ \overline{x} + \overline{y} = \overline{x + y} \text{ e } \overline{x} \times \overline{y} = \overline{x \times y}$$

conferem a $A/\mathcal{R}$ uma estrutura de anel. Este anel é dito "anel quociente de A por I"e denota-se A/I.

Já vimos que $(A/I, +)$ é um grupo, basta pois fazer apenas álgumas verificações muito fáceis (associatividade de $\times$, propriedades de distributividade,...etc).

Note que as noções de "subgrupo normal"e de "ideal"foram inicialmente inventadas para possibilitar esta construção.

2.4 Aplicação: os aneis quociente $\mathbb{Z}_n$

Consideremos o anel $(\mathbb{Z}, +, \times)$.
Para todo inteiro $n \geq 2$, é fácil verificar que $I = n\mathbb{Z}$ é um ideal de $\mathbb{Z}$.

Assim podemos considerar o anel $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

Lembramos que

- Enquanto conjunto, $\mathbb{Z}_n = \mathbb{Z}/\mathcal{R}$, onde a relação de equivalência $\mathcal{R}$ é dada por

$$\forall x, y \in \mathbb{Z} \ , \ x \mathcal{R} y \Leftrightarrow x - y \in n\mathbb{Z} \ (\ \Leftrightarrow n | x - y \ ).$$

- As operações em $\mathbb{Z}_n$ são definidas por

$$\forall x, y \in \mathbb{Z}\ ,\ \overline{x} + \overline{y} = \overline{x+y} \text{ e } \overline{x}.\overline{y} = \overline{xy}.$$

É ainda fácil observar que $\mathbb{Z}_n$ possui exactamente n elementos:

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

De facto, para $x \in \mathbb{Z}$, se $r \in \{0; 1; \ldots; n-1\}$ fôr o resto da divisão euclidiana de x por n:

$$x = qn + r, \text{ pelo que } x - r = qn \text{ e } n|x - r\ :\ x \in \overline{r}.$$

Notemos ainda que $\overline{1}$ é elemento neutro multiplicativo de $\mathbb{Z}_n$.

O próximo teorema fornece uma condição necessária e suficiente para que $\overline{x}$ seja invertível em $\mathbb{Z}_n$:

Teorema 2.4.1 *Seja $n \in \mathbb{N}$ um inteiro, $n \geq 2$, e $m \in \mathbb{Z}$.*

As seguintes afirmações são equivalentes:

(i) n e m são primos entre si.
(ii) $\overline{m}$ é regular em $\mathbb{Z}_n$.
(iii) $\overline{m}$ é invertível em $\mathbb{Z}_n$.
(iv) Existem $a, b \in \mathbb{Z}$, $an + bm = 1$.

Prova:

- Já vimos no capítulo anterior que (i) $\Leftrightarrow$ (iv).

- $(iv) \Rightarrow (iii)$:
  De facto, tem-se

  $$(iv) \Leftrightarrow \exists b \in \mathbb{Z}\ ,\ n|1 - bm \Leftrightarrow \exists b \in \mathbb{Z}\ ,\ bm\mathcal{R}1 \Leftrightarrow \exists b \in \mathbb{Z}\ ,\ \overline{b}.\overline{m} = \overline{bm} = \overline{1} \text{ em } \mathbb{Z}_n \Leftrightarrow (iii).$$

- $(iii) \Rightarrow (ii)$ é evidente.

- $(i) \Rightarrow (ii)$:
  Suponhamos que (ii) não se verifica. Então existe $a \in \mathbb{Z}$ tal que $\overline{a} \neq \overline{0}$ e $\overline{m}.\overline{a} = \overline{0}$.
  Logo, $n|am$ e n e m não são primos entre si: se o fossem, teriamos pelo lema de Euclides que $n|a$, ou seja $\overline{a} = \overline{0}$.

- $(ii) \Rightarrow (i)$: Suponhamos que n e m não são primos entre si. Seja $p \in \mathbb{P}$ um divisor comum de n e m: $n = pN$, $m = pM$.
  Então $\overline{m}.\overline{N} = \overline{M}.\overline{pN} = \overline{M0} = \overline{0}$, mas $n \not| N$: $\overline{N} \neq \overline{0}$.
  Logo $\overline{m}$ não é regular.

Nota: Provámos mais implicações do que seria necessáro!

Deste teorema resulta o seguinte corolário fundamental, de prova imediata:

Corolário 2.4.1 *Seja $n \in \mathbb{N}$, $n \geq 2$:*

As seguintes afirmações são equivalentes:

(i)$n \in \mathbb{P}$

(oii)$\mathbb{Z}_n$ não possui divisores de 0

(iii) $\mathbb{Z}_n$ é um corpo.

3 Congruências

3.1 Definição e primeiras propriedades

Definição 3.1.1 *Seja n um inteiro, $n \geq 2$ e $a, b \in \mathbb{Z}$.*
Diz-se que "a é congruente a b módulo n" se $n|a-b$. Denota-se

$$a \equiv b \mod n.$$

Assim, temos as seguintes equivalências:

$$a \equiv b \mod n \Leftrightarrow \overline{a} = \overline{b} \text{ em } \mathbb{Z}_n$$

$$\Leftrightarrow a \text{ e } b \text{ possuem o mesmo resto na divisão euclidiana por } n.$$

Traduzindo em termos de congruências as propriedades dos aneis $\mathbb{Z}_n$ estudadas no capítulo anterior, obtemos de maneira imediata o seguinte:

Propriedade 3.1.2 *Seja n um inteiro, $n \geq 2$ e $a, b, c, d \in \mathbb{Z}$.*

Então:

(i) $a \equiv a \mod n$

(ii) $a \equiv b \mod n \Rightarrow b \equiv a \mod n$

(iii) $a \equiv b \mod n$ *e* $b \equiv c \mod n \Rightarrow a \equiv c \mod n$

(iv) $a \equiv b \mod n$ *e* $c \equiv d \mod n \Rightarrow ac \equiv bd \mod n$

(v) $\forall k \in \mathbb{N}$, $a \equiv b \mod n \Rightarrow a^k \equiv b^k \mod n$

(vi) $\forall (x, y) \in \mathbb{Z}^2$, $a \equiv b \mod n$ *e* $c \equiv d \mod n \Rightarrow ax + cy \equiv bx + dy \mod n$

(vii) $a \equiv b \mod n$ *e* $d|n (d \geq 2\ ) \Rightarrow a \equiv b \mod d$.

(viii) $a \equiv b \mod n \Leftrightarrow \forall k \in \mathbb{N}$, $a + kn \equiv b \mod n$.

(ix) $a \equiv b \mod n \Leftrightarrow \forall k \in \mathbb{N}$, $ak \equiv kb \mod kn$.

(x) Se $a \equiv b \mod n$ *e para* $d \geq 2$, $d|a$, $d|b$ *e* $d|n$, *então* $\frac{a}{d} \equiv \frac{b}{d} \mod \frac{n}{d}$.

De facto,

- (i),(ii) e (iii) é uma tradução do facto da relação binária $\equiv$ ser uma relação de equivalência.

- (iv),(v) e (vi) são consequências imediatas da definição das operações no anel $\mathbb{Z}_n$ (compatíveis com a relação de equivalência acima mencionada).

- (vii),(viii),(ix) e (x) são de prova imediata.

Assim, a noção de congruência é apenas uma maneira prática de falar dos aneis $\mathbb{Z}_n$.

Por exemplo, se quisermos mostrar que $7|3.2^{101}+9$:
Esta questão limita-se a saber se $\overline{3.2^{101}+9} = \overline{0}$ no anel $\mathbb{Z}_7$.

Utilizando as propriedades das congruências, podemos observar que:

$$2^3 = 8 = 1 + 7 \equiv 1 \mod 7,$$

pelo que

$$2^{99} = (2^3)^{33} \equiv 1 \mod 7,$$

ou ainda

$$2^{101} = 4.2^{99} \equiv 4 \mod 7,$$

e finalmente,

$$3.2^{101} + 9 \equiv 4.3 + 9 \mod 7 : 3.2^{101} + 9 \equiv 21 \equiv 0 \mod 7.$$

Assim, $7|3.2^{101}+9$.

Utilizando agora o facto de $\overline{m}$ ser regular em $\mathbb{Z}_n$ se e só se m e n são primos entre si, obtemos os seguintes resultados:

Propriedade 3.1.3 *Seja $n \geq 2$ e $a, x, y \in \mathbb{Z}$, $a \notin n\mathbb{Z}$.*
Então:

(i) Se $ax \equiv ay \mod n$, então $x \equiv y \mod \frac{n}{(n,a)}$.

(ii) Se a e n são primos entre si, $ax \equiv ay \mod n \Rightarrow x \equiv y \mod n$.

Prova:
(ii) é uma consequência directa do facto de $\overline{a}$ ser regular em $\mathbb{Z}_n$ sse $(a,n)=1$.

(i) : Temos que $\left(\frac{a}{(a,n)}, \frac{n}{(a,n)}\right) = 1$.
Sejam $x, y \in \mathbb{Z}$, com $ax \equiv ay \mod m$.
Então $\frac{a}{(a,n)}x \equiv \frac{a}{(a,n)}y \mod \frac{n}{(a,n)}$.
Utilizando agora a alínea anterior, vem que $x \equiv y \mod \frac{n}{(a,n)}$.

Note ainda esta prova alternativa do ponto (ii):
Seja $d=(a,n)$. Como $ax \equiv ay \mod n$, por definição, $n|ax-ay$, pelo que existe $k \in \mathbb{Z}$ tal que $a(x-y)=nk$.
Assim, $\frac{a}{d}(x-y) = \frac{n}{d}k$. Logo, $\frac{n}{d}$ divide o produto $\frac{a}{d}(x-y)$. Pelo lema de Euclides, $\frac{n}{d}|(x-y)$, o que significa, por definição, que $x \equiv y \mod \frac{n}{d}$.

Terminamos esta secção com uma última propriedade:

Propriedade 3.1.4 *Sejam $x, y \in \mathbb{Z}$ e $\{m_i\}_{1\leq i\leq r}$ r inteiros, $m_i \geq 2$.*
Então,

$$\forall i \in \{1,2,\ldots,r\},\ x \equiv y \mod m_i \Leftrightarrow x \equiv y \mod m,$$

onde $m = [m_1, m_2, \ldots, m_r]$ é o mínimo múltiplo comum de $m_1, \ldots, m_r$.

Prova:
$\Leftarrow$ É evidente, já que para todo i, $m_i|m$.
$\Rightarrow$ Provamos a proposição para $r=2$, o caso geral podendo ser deduzido facilmente por indução.

Temos $m_1|(x-y)$ e $m_2|(x-y)$. Assim, $x-y$ é um múltiplo comum de m_1 e m_2, pelo que $[m_1,m_2]|(x-y)$. (Prove-o).

Obtemos então o seguinte corolário imediato:

Corolário 3.1.5 *Sejam $x, y \in \mathbb{Z}$ e $\{m_i\}_{1\leq i\leq r}$ r inteiros, $m_i \geq 2$, dois a dois primos entre si.*
Então,

$$\forall i \in \{1,2,\ldots,r\},\ x \equiv y \mod m_i \Leftrightarrow x \equiv y \mod m,$$

onde $m = m_1 m_2 \ldots m_r$.

De facto, como os m_i são dois a dois primos entre si, $[m_1, m_2, \ldots, m_r] = m_1 m_2 \ldots m_r$.

3.2 Sistemas de resíduos módulo n

Definição 3.2.1 *Seja $n \geq 2$.*

O conjunto $S \subset \mathbb{Z}$ diz-se um sistema completo de resíduos módulo n se

$$\forall C \in \mathbb{Z}/\mathbb{Z}_n \ , \ \exists! s \in S \ , \ s \in C.$$

Assim, um sistema completo de resíduos (s.c.r.) é formado por n inteiros, um em cada classe do anel quociente $\mathbb{Z}_n$.

Por exemplo, $\{0; 1; \ldots; n-1\}$ é um s.c.r. módulo n.
Tem-se a propriedade imediata:

Propriedade 3.2.2 *Seja $n \geq 2$ e $S \subset \mathbb{Z}$.*

$$S \text{ é um s.c.r. módulo } n \Leftrightarrow \forall x \in \mathbb{Z} \ , \ \exists! i \in \{1; \ldots; n\} \ , \ x \equiv s_i \mod n.$$

Definição 3.2.3 *Seja $n \geq 2$.*

O conjunto $S \subset \mathbb{Z}$ diz-se um sistema reduzido de resíduos módulo n se para toda classe invertível C de $\mathbb{Z}_n$,

$$\exists! s \in S \ , \ s \in C.$$

Para $x \in \mathbb{Z}$, sabemos que $\overline{x}$ é invertível em $\mathbb{Z}_n$ se e só se $(x, n) = 1$.

Assim, se $S = \{s_1, s_2, \ldots, s_n\}$ é um s.c.r., o conjunto

$$S' = \{s_i \in S \ ; \ (s_i, n) = 1\}$$

é um sistema reduzido de resíduos (s.r.r.).

Por exemplo, $\{0, 1, \ldots, 9\}$ é um s.c.r. módulo 10, e $\{1; 3; 7; 9\}$ é um s.r.r. módulo 10.

As seguintes propriedades são imediatas:

Propriedade 3.2.4 *Seja $n \geq 2$ e S um s.r.r. módulo n.*
Então:

a. $\forall s \in S$, $(s, n) = 1$.

b. $\forall x \in \mathbb{Z}$, $(x, n) = 1 \Rightarrow \exists! s \in S$, $x \equiv s \mod n$.

Observe que a propriedade **b**. é na realidade uma condição necessária e suficiente para que um subconjunto S de $\mathbb{Z}$ seja um s.r.r.

Obviamente, qualquer s.r.r. módulo n tem o mesmo cardinal, igual ao número de classes invertiveis de $\mathbb{Z}_n$. Esta observação leva à seguinte definição:

Definição 3.2.5 : Função ϕ de Euler.

Seja $n \geq 2$ e S um s.r.r. módulo n. Define-se então

$$\phi(n) = card(S) = card\{1 \leq k \leq n \ ; \ (k, n) = 1\}.$$

Esta função será largamente estudada no próximo capítulo. Notemos no entanto desde já que se $p \in \mathbb{P}$, $\phi(p) = p - 1$.

3.3 Teorema de Euler e pequeno Teorema de Fermat

Comecemos por provar o seguinte lema:

Teorema 3.3.1 *Seja $n \geq 2$ e $S = \{s_1, s_2, \ldots, s_{\phi(n)}\}$ um s.r.r. módulo n.*
Se $a \in \mathbb{Z}$ é primo com n, o conjunto

$$S' = \{as_1, as_2, \ldots, as_{\phi(n)}\}$$

é igualmente um s.r.r. módulo n.

Prova:
Seja $i \in \{1; \ldots; \phi(n)\}$: $(as_i, n) = 1$, visto que $(a, n) = (s_i, n) = 1$.
Assim, para todo $i \in \{1; \ldots; \phi(n)\}$, $\overline{as_i}$ é uma classe invertível de $\mathbb{Z}_n$.

Suponhamos agora que $as_i \equiv as_j \mod n$.
Como $(a, n) = 1$, a é um elemento regular, o que implica que $s_i \equiv s_j \mod n$, ou ainda $\overline{s_i} = \overline{s_j}$ em $\mathbb{Z}_n$. Como S é um s.c.r., $i = j$.

Acabámos pois de provar que as classes $\overline{as_1}$, $\overline{as_2}$, ..., $\overline{as_{\phi(n)}}$ são invertíveis de $\mathbb{Z}_n$, todas distintas. Como estão em número $\phi(n)$, são exactamente as classes invertíveis de $\mathbb{Z}_n$, pelo que por definição, S' é um s.r.r. módulo n.

Como consequência importante deste facto, temos o

Teorema 3.3.1 : Teorema de Euler
Seja $n \geq 2$ e $a \in \mathbb{Z}$ primo com n. Então

$$a^{\phi(n)} \equiv 1 \mod n.$$

Prova:
Seja $S = \{s_1, s_2, \ldots, s_{\phi(n)}\}$ um s.r.r. módulo n. Como vimos, o sistema $\{as_1, as_2, \ldots, as_{\phi(n)}\}$ é igualmente um s.r.r. módulo n. Assim,

$$\forall \in \{1, 2, \ldots, \phi(n)\}, \exists! j \in \{1, 2, \ldots, \phi(n)\}, as_i \equiv s_j \mod n.$$

Multiplicando as $\phi(n)$ congruências assim obtidas, obtem-se

$$\prod_{i=1}^{\phi(n)} as_i \equiv \prod_{j=1}^{\phi(n)} s_j \mod n.$$

Assim,

$$a^{\phi(n)} \prod_{i=1}^{\phi(n)} s_i \equiv \prod_{j=1}^{\phi(n)} s_j \mod n.$$

Como para todo i, $(s_i, n) = 1$, tem-se $(\prod_{i=1}^{\phi(n)} s_i, n) = 1$.
Logo, podemos simplificar na congruência $\prod_{i=1}^{\phi(n)} s_i$, o que termina a prova.

Observação 3.3.1

Se $(a,n) = 1$, sabemos que $\overline{a}$ é ivertivel em $\mathbb{Z}_n$. Graças ao teorema de Euler, podemos agora calcular explicitamente $\overline{a}^{-1}$:
De facto,

$$a.a^{\phi(n)-1} = a^{\phi(n)} \equiv 1 \mod n, \text{ pelo que } \overline{a}^{-1} = \overline{a^{\phi(n)-1}} = \overline{a}^{\phi(n)-1}.$$

Como corolário imediato do teorema de Euler, temos o

Corolário 3.3.2 : Pequeno teorema de Fermat

Seja $p \in \mathbb{P}$, e $a \in \mathbb{Z}$ tal que $p \nmid a$. Então

$$a^{p-1} \equiv 1 \mod p.$$

Basta observar, como p é primo, que $p \nmid a$ é equivalente a $(a,p) = 1$, e que $\phi(p) = p - 1$.

Observação 3.3.3 *Note que para todo $a \in \mathbb{Z}$ e todo $p \in \mathbb{P}$,*

$$a^p \equiv a \mod p.$$

De facto, se $p \nmid a$, esta congruência é uma consequência imediata do pequeno teorema de Fermat.
Se $p|a$, $a^p \equiv a \equiv 0 \mod p$.

3.4 Teorema de Wilson

O seguinte teorema fornece uma condição necessária e suficiente para que um inteiro $n \in \mathbb{N}$ seja primo:

Teorema 3.4.1 : Teorema de Wilson

Seja $n \geq 2$. Então

$$n \in \mathbb{P} \Leftrightarrow (n-1)! + 1 \equiv 0 \mod n.$$

Prova:
$\Leftarrow$ Supondo que $n \notin \mathbb{P}$, $n = ab$, com $1 < a < n$ (a é um divisor não trivial de n).
Então, $a|(n-1)!$, e, consequentemente, $a \not| (n-1)! + 1$.
Como $a|n$, necessariamente $n \not| (n-1)! + 1$.
(Se não, por transitividade, ter-se-ia $a|(n-1)! + 1$, o que é falso).
Finalmente, $(n-1)! + 1 \not\equiv 0 \mod n$.

$\Rightarrow$ Seja $p \in \mathbb{P}$. Então $\overline{1}$, $\overline{2}$, ..., $\overline{p-1}$ são invertíveis em $\mathbb{Z}_p$. Vamos determinar quais as classes que são o seu próprio inverso, isto é, os elementos de ordem 2 do grupo multiplicativo $\mathbb{Z}_p^*$. Para $C \in \mathbb{Z}_p^*$,

$$C^2 = \overline{1} \Leftrightarrow C^2 - \overline{1}^2 = 0 \Leftrightarrow (C - \overline{1})(C + \overline{1}) = \overline{0},$$

e, como $\mathbb{Z}_p$ é um corpo, não possui divisores de zero:

$$C^2 = \overline{1} \Leftrightarrow C = \overline{1} \text{ ou } C = -\overline{1} = \overline{p-1}.$$

Logo,

$$\forall j \in \{2, 3, \ldots, p-2\},\ \exists! k \in \{2, 3, \ldots, p-2\}/\{j\},\ \overline{k}.\overline{j} = \overline{1}.$$

Assim,

$$\prod_{j=1}^{p-2} \overline{j} = \overline{1},$$

isto é,

$$\prod_{j=1}^{p-2} j \equiv 1 \mod p.$$

Multiplicando por $(p-1)$,

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

3.5 Congruências lineares

Neste capítulo, vamos estudar as congruências lineares da forma

$$ax \equiv b \mod n, \tag{3.1}$$

em que $a, b \in \mathbb{Z}$, $n \geq 2$ e $x \in \mathbb{Z}$ é a incógnita.

Podemos desde já supor que $n \not| a$ (isto é $(a, n) \neq n$).
(De facto, se $n|a$, a resolução é trivial: (3.1) não possui soluções se $b \not\equiv 0 \mod n$ e qualquer $x \in \mathbb{Z}$ é solução de (3.1) se $b \equiv 0 \mod n$.)

Começamos por observar o seguinte:

$$x \in \mathbb{Z} \text{ solução de } (3.1) \Leftrightarrow \forall k \in \mathbb{Z},\ x + kn \text{ solução de } (3.1).$$

Assim, basta determinar as soluções de (3.1) num s.c.r. módulo n
(por exemplo $(0, 1, \ldots, n-1)$) e adicionar-lhes múltiplos de n para obter a solução geral.

Duas soluções distintas de (3.1) pertencentes a um mesmo s.c.r. são ditas soluções incongruentes módulo n.
Vamos agora estudar quatro métodos de resolução diferentes:

Método 1: À mão

Se n não for muito grande, por que não testar os n elementos de um s.c.r. ?

Por exemplo, para resolver a congruência linear

$$4x \equiv 4 \mod 6, \tag{3.2}$$

vamos calcular $4x$ para $x \in \{0, \ldots, 5\}$:

$$\begin{array}{lll} 4.0 = 0 \not\equiv 4 \mod 6 & 4.1 = 4 \equiv 4 \mod 6 & 4.2 = 8 \not\equiv 4 \mod 6 \\ 4.3 = 12 \not\equiv 4 \mod 6 & 4.4 = 16 \equiv 4 \mod 6 & 4.5 = 20 \not\equiv 4 \mod 6 \end{array}$$

Assim, as soluções de (3.2) no s.c.r. $(0, 1, 2, 3, 4, 5)$ são $x_o = 1$ e $x_1 = 4$.
A solução geral é então dada por:

$$x = 1 + 6k \text{ , ou } x = 4 + 6k \text{ , } k \in \mathbb{Z},$$

ou, se preferirmos,

$$x = 1 + 3k \text{ , } k \in \mathbb{Z}.$$

Método 2: Resolução de uma equação diofantina.

Notemos que $x \in \mathbb{Z}$ é solução de (3.1) sse existir $y \in \mathbb{Z}$ tal que

$$ax + ny = b. \tag{3.3}$$

Ora, já sabemos forncecer a solução geral de uma equação diofantina: se $d = (a, n) \not| b$, (3.3) não possui soluções. Caso contrário, a solução geral é dada por

$$x = x_o + t\frac{n}{d} \text{ , } y = y_o - t\frac{a}{d} \text{ , } t \in \mathbb{Z},$$

onde (x_o, y_o) é uma qualquer solução da congruência.

Assim, constatamos que (3.3) possui exactamente d soluções incongruentes módulo n:
$x_o + 0\frac{n}{d}$, $x_o + 1.\frac{n}{d}$, $x_o + 2\frac{n}{d}$, $\ldots$, $x_o + (d-1)\frac{n}{d}$.

Desta observação deduz-se a seguinte propriedade da congruência linear (3.1):

Propriedade 3.5.1 *Seja $n \geq 2$, $a, b \in \mathbb{Z}$.*
Então, a congruência linear

$$ax \equiv b \mod n$$

possui soluções se e só se $d = (a, n)|b$.
Nesse caso, existem exactamente d souções incongruentes módulo n.

Vamos agora resolver a congruência $4x \equiv 4 \mod 6$ com a ajuda de uma equação diofantina:

Temos pois que resolver a equação $4x + 6y = 4$.

$d = (4, 6) = 2|4$, logo existem soluções.

O algoritmo de Euclides forncece inteiros α, β tais que $4\alpha + 6\beta = d = 2$.
Por exemplo, $4.(-1) + 6.(1) = 2$.

Multiplicando por 2: $4.(-2) + 6(2) = 4$.
Uma solução particular será portanto $(x_o, y_o) = (-2, 2)$.
Assim, a solução geral é

$$\begin{cases} x = -2 + \frac{6}{2}t = -2 + 3t \\ y = 2 - t\frac{4}{2} = 2 - 2t \quad t \in \mathbb{Z}, \end{cases}$$

sendo a primeira linha a solução geral de (3.2).

Método 3: Inversão de um elemento no anel quociente.

Seja $d = (a, n)$. Como vimos, se $d \not| b$, (3.1) não possui soluções. Caso contrário, dividindo a equação por d obtem-se

$$\frac{a}{d}x \equiv \frac{b}{d} \mod \frac{n}{d}.$$

Já vimos que $\left(\frac{a}{d}, \frac{n}{d}\right) = 1$. Assim, $\overline{\frac{a}{d}}$ é invertivel em $\mathbb{Z}_{\frac{n}{d}}$. Pelo teorema de Gauss,

$$\frac{a}{d}x \equiv \frac{b}{d} \mod \frac{n}{d} \Leftrightarrow x \equiv \left(\frac{a}{d}\right)^{\phi(\frac{n}{d})-1} \frac{b}{d} \mod \frac{n}{d},$$

obtendo-se assim a solução geral de (3.1).

Voltemos ao nosso exemplo:

$$4x \equiv 4 \mod 6 \Leftrightarrow 2x \equiv 2 \mod 3 \Leftrightarrow x \equiv 2.2^{\phi(3)-1} \equiv 2.2^{2-1} \equiv 1 \mod 3,$$

isto é,

$$x = 1 + 3t \ , \ t \in \mathbb{Z}.$$

Método 4: Recurso a um sistema

Consideremos a congruência linear

$$14x \equiv 16 \mod 180 \tag{3.4}$$

$d = (14, 180) = 2|16$, pelo que esta equação admite 2 soluções incongruentes módulo 180.

Dividindo desde já por d, obtem-se a congruência equivalente

$$7x \equiv 8 \mod 90 \tag{3.5}$$

Os métodos apresentados anteriormente poderão levar a longos cálculos, pelo que veremos aqui outra abordagem:
Notando que $90 = 2.3^2.5$, os inteiros $m_1 = 2$, $m_2 = 3^2$ e $m_3 = 5$ são dois a dois primos entre si.

Pelo Corolário 3.1.5,

$$(3.4)$$

$$\Leftrightarrow$$

$$\begin{cases} 7x \equiv 8 \mod 2 \\ 7x \equiv 8 \mod 5 \\ 7x \equiv 8 \mod 9 \end{cases}$$

Este sistema pode muito facimente, com qualquer um dos métodos anteriores, ser posto na forma

$$\begin{cases} x \equiv 0 \mod 2 \\ x \equiv 4 \mod 5 \\ x \equiv 5 \mod 9 \end{cases}$$

Temos ainda que resolver o sistema, o que poderá feito com o teorema dos restos chineses, que apresentamos na próxima secção.

3.6 Teorema dos restos chineses

Teorema 3.6.1 : Teorema dos restos chineses
Consideremos o sistema de congruências lineares

$$x \equiv a_i \mod m_i \ , \ 1 \leq i \leq r,$$

onde $a_i \in \mathbb{Z}$ *e os inteiros* $\{m_i\}$ *são dois a dois primos entre si.*

Então, a solução geral do sistema é

$$x = x_o + tm \ , \ t \in \mathbb{Z},$$

com $m = m_1 m_2 \dots m_r$*, e a solução particular* x_o *é dada por*

$$x_o = \sum_{i=1}^{r} \frac{m}{m_i} a_i b_i,$$

onde os inteiros b_i *verificam* $b_i . \dfrac{m}{m_i} \equiv 1 \mod m_i$.

Nota: Os inteiros b_i existem sempre, já que $\left(\dfrac{m}{m_i}, m_i\right) = 1$.

Prova do Teorema:

i. Sejam x_1 e x_2 duas soluções do sistema. Vamos provar que então x_1 e x_2 diferem de um múltiplo de m:
Temos para todo $i \in \{1, \dots, r\}$, $x_1 \equiv x_2 \mod m_i$. Pelo Corolário 3.1.5,

$$x_1 \equiv x_2 \mod m, \text{ pelo que } m|(x_1 - x_2).$$

Reciprocamente, se x é solução do sistema, para todo $k \in \mathbb{Z}$, $x + km$ é solução.

ii. x_o dado no teorema é uma solução da congruência:
Seja $j \in \{1, \dots, r\}$.
Para $i \neq j$, $\frac{m}{m_i} \equiv 0 \mod m_j$, já que $m_j | \frac{m}{m_i}$.

Assim,

$$x_o = \sum_{i=1}^{r} \frac{m}{m_i} a_i b_i \equiv \frac{m}{m_j} b_j a_j \equiv a_j \mod m_j,$$

o que conclui a prova do teorema.

Aplicação:
Resolução do sistema de congruências

$$\begin{cases} x \equiv 0 \mod 2 \\ x \equiv 4 \mod 5 \\ x \equiv 5 \mod 9 \end{cases}$$

Temos $(m_1, m_2, m_3) = (2, 5, 9)$, $m = 90$ e $(a_1, a_2, a_3) = (0, 4, 5)$.
Escolhemos inteiros b_1, b_2, b_3 que verifiquem

$$45b_1 \equiv 1 \mod 2 \text{ , } 18b_2 \equiv 1 \mod 5 \text{ e } 10b_3 \equiv 1 \mod 9 \text{ ,}$$

por exemplo, $b_1 = b_3 = 1$ e $b_2 = 2$.

Assim, $x_o = a_1 b_1 \frac{m}{m_1} + a_2 b_2 \frac{m}{m_2} + a_3 b_3 \frac{m}{m_3} = 194$.

A solução geral do sistema é

$$x = 194 + 90t \text{ , } t \in \mathbb{Z}.$$

Nota: As duas soluções incongruentes módulo 180 são 14 e 104.

4 Funções Aritméticas

4.1 Primeiras definições

Definição 4.1.1 *Uma função aritmética f é uma função*

$$f : \mathbb{N} \to \mathbb{C},$$

ou seja, uma sucessão de números complexos.

De entre as funções aritméticas, vamos estudar em particular álgumas funções ditas (totalmente) multiplicativas:

Definição 4.1.2 *Uma função aritmética diz-se multiplicativa se*

$$\begin{cases} f(1) = 1 \\ \forall n, m \in \mathbb{N} \ , \ (n, m) = 1 \Rightarrow f(nm) = f(n)f(m) \end{cases}$$

Diz-se ainda totalmente multiplicativa se esta última igualdade se verificar para todos os inteiros n e m.

Eis algumas funções totalmente multiplicativas que serão utilizadas ao longo deste capítulo:

- A função "injeção canónica"
$$i : n \to n.$$
- A função "um":
$$\mathbf{1} : n \to 1.$$
- A função de Dirac:
$$\delta : n \to \delta_{n,1}.$$

Definição 4.1.3 *Define-se a função μ de Moebius por*

$$\begin{array}{rccl} \mu: & \mathbb{N} & \to & \{-1;0;1\} \\ & n & \to & \begin{cases} 0 & \text{se } n \text{ não é livre de quadrados} \\ (-1)^{\omega(n)} & \text{no caso contrário,} \end{cases} \end{array}$$

onde $\omega(n)$ é o número de divisores primos de n.

Define-se ainda a função τ por

$$\tau : n \to card\{1 \leq d \leq n \ ; \ d|n\} = \sum_{d|n} 1.$$

Teorema 4.1.1 *As funções μ e τ são multiplicativas.*

Prova:

a. Função τ
Observemos o seguinte:

Teorema 4.1.1 *Seja $n \in \mathbb{N}$.*
Seja $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, $1 < p_1 < \cdots < p_r$, a decomposição em números primos de n.
Então

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1)\ldots(\alpha_r + 1).$$

A demonstração é imediata, pois, como vimos no primeiro capítulo,

$$d|n \text{ sse } d = \prod_{i=1}^{r} p_i^{\gamma_i},\ 0 \leq \gamma_i \leq \alpha_i,$$

existindo assim $(\alpha_i + 1)$ possibilidades para a potência γ_i.

Voltemos agora à prova do Teorema 4.1.1:
Tem-se $\tau(1) = 1$. Sejam $n, m \in \mathbb{N}$, com $(n, m) = 1$.
Sejam $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ e $n = \prod_{j=1}^{r} q_i^{\beta_i}$ as decomposições em números primos de n e m.

Como $(n, m) = 1$, tem-se, para todos os índices i, j, $p_i \neq q_j$.
Logo

$$\prod_{i,j} p_i^{\alpha_i} q_j^{\beta_j}$$

é a decomposição em factores primos de nm.
Pelo lema,

$$\tau(n)\tau(m) = \prod_{i=1}^{r}(\alpha_i + 1)\prod_{j=1}^{s}(\beta_j + 1) = \prod_{i,j}(\alpha_i + 1)(\beta_j + 1) = \tau(nm).$$

b. Função μ de Moebius.
Sejam $m, n \in \mathbb{N}$, com $(m, n) = 1$. Então, para todo $p \in \mathbb{P}$, $p^2|nm$ se e só se $p^2|n$ ou $p^2|m$.
Assim, se n ou m não for livre de quadrados, nm não é livre de quadrados.
Assim, neste caso,

$$\mu(nm) = \mu(n)\mu(m) = 0.$$

Suponhamos agora que n e m são livres de quadrados: $n = p_1 p_2 \dots p_r$ e $m = q_1 q_2 \dots q_s$, p_i, q_j primos, com $p_i \neq q_j$ para todos os índices i, j.

Assim,

$$\mu(n)\mu(m) = (-1)^r(-1)^s = (-1)^{r+s} = \mu(nm).$$

4.2 Produto de Convolução

Definição 4.2.1 *Sejam f e g duas funções aritméticas.*
Define-se a função aritmética F "produto de convolução de f por g":

$$\begin{array}{rccc} F: & \mathbb{N} & \to & \mathbb{C} \\ & n & \to & \displaystyle\sum_{d|n} f(d)g(\frac{n}{d}) \end{array}$$

Denota-se $F = f * g$.

Exemplos:

i. Para $n \in \mathbb{N}$,

$$\mathbf{1} * \mathbf{1}(n) = \sum_{d|n} \mathbf{1}(d)\mathbf{1}(\frac{n}{d}) = \sum_{d|n} 1 = \tau(n).$$

Assim,

$$\mathbf{1} * \mathbf{1} = \tau.$$

ii. Seja f uma função aritmética. Para $n \in \mathbb{N}$,

$$\delta * f(n) = \sum_{d|n} \delta(d) f(\frac{n}{d}) = f(n) \, : \, \delta * f = f.$$

Temos as seguintes propriedades imediatas do produto de convolução:

Propriedade 4.2.2 *Sejam f,g,h três funções aritméticas. Tem-se*
i. $f * g = g * f$
ii. $(f * g) * h = f * (g * h)$

Prova de i.
Seja $n \in \mathbb{N}$.
Seja, para $d \in \mathbb{N}$, $d' = \frac{n}{d}$.

$$d|n \Leftrightarrow d' \in \mathbb{N} \Leftrightarrow d'|n.$$

Vamos assim fazer a seguinte "mudança de variável":

$$f * g(n) = \sum_{d|n} f(d) g(\frac{n}{d}) = \sum_{d'|n} f(\frac{n}{d'}) g(d') = g * f(n).$$

Teorema 4.2.1 *Sejam f e g duas funções multiplicativas.*
Então $F = f * g$ é multiplicativa.

Prova:
Observemos primeiro o seguinte lema:

Teorema 4.2.1 *Sejam $m, n \in \mathbb{N}$, com $(m, n) = 1$.*
Então, para todo $d \in \mathbb{N}$,

$$d|mn \Leftrightarrow \exists! d_1, d_2 \in \mathbb{N} \ , \ d = d_1 d_2 \ e \ d_1|m_1, \ d_2|m_2.$$

Tem-se ainda $(d_1, d_2) = 1$.

Prova: Seja $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ e $m = \prod_{j=1}^{s} q_j^{\beta_j}$ a decomposição em números primos de n e m.
Como $(m, n) = 1$, $p_i \neq q_j$ para todos os índices i, j.

Sabemos que se $d|m_1m_2$, $d = \prod_{i,j} p_i^{\gamma_i} q_j^{\delta_j}$ com $\gamma_i \leq \alpha_i$ e $\delta_j \leq \beta_j$.
Basta pois escolher

$$d_1 = \prod_{i=1}^{r} p_i^{\gamma_i} \text{ e } d_2 = \prod_{j=1}^{r} q_j^{\delta_j}.$$

Quanto à unicidade, suponhamos que $d = d_1d_2 = d_1'd_2'$, onde os pares (d_1, d_2) e (d_1', d_2') verificam as condições do lema.
Como $d_1|n$ e $(d_2', n) = 1$, $(d_1, d_2') = 1$. (Verifique-o rapidamente).
Ora, $d_1|d_1'd_2'$: pelo lema de Euclides, $d_1|d_1'$.
Por um raciocínio análogo, $d_1'|d_1$, e $d_1 = d_1'$, o que implica também que $d_2 = d_2'$.

Prova do Teorema 4.2.1:

Sejam f, g duas funções multiplicativas, $F = f * g$ e n, m primos entre si. Então

$$F(nm) = \sum_{d|nm} f(nm)g(\frac{nm}{d}) = \sum_{d_1|n, d_2|m} f(nm)g(\frac{nm}{d_1d_2}) = \sum_{d_1|n, d_2|m} f(n)f(m)g(\frac{n}{d_1})g(\frac{m}{d_2}),$$

já que f e g são multiplicativas e $\left(\frac{n}{d_1}, \frac{m}{d_2}\right) = 1$.
Assim,

$$F(nm) = \sum_{d_1|n} \left(\sum_{d_2|m} f(n)f(m)g(\frac{n}{d_1})g(\frac{m}{d_2}) \right) = \sum_{d_1|n} f(n)g(\frac{n}{d_1}) \left(\sum_{d_2|m} f(m)g(\frac{m}{d_2}) \right) =$$

$$= \sum_{d_1|n} f(n)g(\frac{n}{d_1}) f * g(m) = (f * g(n))(f * g(m)).$$

Exemplo:

A função σ definida por $\sigma(n) = \sum_{d|n} d$ (soma dos divisores de d) é multiplicativa.

De facto, $\sigma = i * \mathbf{1}$.

Finalmente:

Teorema 4.2.2 *Seja $\mathcal{M}$ o conjunto das funções multiplicativas.*

$(\mathcal{M}, *)$ *é um grupo abeliano.*

Prova:
Já vimos que a operação $*$ é interna, associativa, comutativa, e tem por elemento neutro a função δ de Dirac.

Basta pois mostrar que toda função f possui um inverso, isto é uma função $g = f^{-1}$ tal que $f * g = \delta$.
Notemos que

$$\begin{aligned} f * g = \delta &\Leftrightarrow f * g(1) = 1 \text{ e } f * g(n) = 0 \text{ para } n > 1 \\ &\Leftrightarrow f(1)g(1) = 1 \text{ e } f(1)g(n) + \sum_{d|n, d\neq 1} f(d)g(\frac{n}{d}) = 0 \text{ se } n > 1 \\ &\Leftrightarrow g(1) = 1 \text{ para } \sum_{d|n, d\neq 1} f(d)g(\frac{n}{d}) = -g(n) \text{ para } n > 1 \end{aligned}$$

Vamos construir uma função g multiplicativa com esta propriedade. A construção faz-se por indução:

- Escolhemos $g(1) = 1$.
- Supondo a função construída para todo inteiro em $\{1; \ldots; n\}$ basta escolher

$$g(n+1) = -\sum_{d|(n+1), d\neq 1} f(d)g(\frac{n+1}{d}).$$

(Note que, como $d \neq 1$, $g(n+1)$ não aparece no termo de direita!)

É ainda necessário provar que a função g assim construída é multiplicativa, isto é,

$$(n, m) = 1 \Rightarrow g(nm) = g(n)g(m).$$

Isto pode ser verificado por indução sobre $N = m + n$, apesar de ser algo trabalhoso!

4.3 A função de Euler

Lembramos a definição da função ϕ de Euler:

$$\phi : n \to card\{1 \leq k \leq n \ ; \ (k, n) = 1\} = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} 1$$

Teorema 4.3.1 : Teorema de Euler
Para todo $n \in \mathbb{N}$,

$$\sum_{d|n} \phi(d) = n.$$

Prova:
Seja $n \in \mathbb{N}$ e d um divisor de n.
Consideremos o conjunto

$$N_d = \{1 \leq x \leq n \ ; \ (n,x) = d\}.$$

Claramente,

$$\forall x \in \{1; \ldots ; n\} \ , \ \exists! d \ , \ x \in N_d.$$

Assim,

$$n = \sum_{d|n} card\{N_d\}.$$

Vamos agora avaliar $card\{N_d\}$:

$$x \in N_d \Leftrightarrow \exists q \in \mathbb{N} \ , \ x = qd \leq n \text{ e } (q, \frac{n}{d}) = (\frac{x}{d}, \frac{n}{d}) = 1.$$

Existem portanto $\phi(\frac{n}{d})$ possibilidades para o inteiro q: $card\{N_d\} = \phi(\frac{n}{d})$.
Finalmente,

$$n = \sum_{d|n} \phi(\frac{n}{d}) = \mathbf{1} * \phi(n) = \phi * \mathbf{1}(n) = \sum_{n|d} \phi(d).$$

Corolário 4.3.1 *A função ϕ de Euler é multiplicativa.*

De facto, basta observar que

$$\mathbf{1} * \phi = i$$

de onde resulta que $\phi = \mathbf{1}^{-1} * i$ e ϕ é multiplicativa.

Já vimos que se $p \in \mathbb{P}$, $\phi(p) = p - 1$.
É também claro que, para $\alpha \in \mathbb{P}$, $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$. De facto, os inteiros do intervalo $[1; p^k]$ que não são primos com p, são os inteiros da forma pq, onde $1 \leq q \leq p^{\alpha-1}$, logo existem $p^{\alpha-1}$.

Assim:

Propriedade 4.3.2 *Seja $n \in \mathbb{N}$.*

$$\Phi(n) = n \prod_{p|n, p \in \mathbb{P}} \left(1 - \frac{1}{p}\right).$$

Prova:

Seja $n = \prod_{i=1}^{s} p_i^{\alpha_i}$ a decomposição em números primos de n. Como Φ é multiplicativa,

$$\phi(n) = \Phi\left(\prod_{i=1}^{s} p_i^{\alpha_i}\right) = \prod_{i=1}^{s} \Phi(p_i^{\alpha_i}) = \prod_{i=1}^{s} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = \prod_{i=1}^{s} p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right) = n \prod_{p|n, p\in\mathbb{P}} \left(1 - \frac{1}{p}\right)$$

4.4 Alguns Resultados clássicos

Propriedade 4.4.1 *As funções* $\mathbf{1}$ *e* μ *são inversas uma da outra, i.e.*

$$\mu * \mathbf{1} = \delta.$$

Prova:

Para $n = 1$, $\mu * \mathbf{1} = \mu(1) = 1$.
Para $n > 1$, seja $n = \prod_{i=1^s} p_i^{\alpha_i}$ a decomposição em números primos de n. O inteiro d divide n se e só se

$$d = \prod_{i=1}^{s} p_i^{\gamma_i} \ , \ \gamma_i \leq \alpha_i.$$

Assim,

$$\mu * \mathbf{1}(n) = \sum_{d|n} \mu(d) = (\mu(p_1) + \cdots + \mu(p_s)) + (\mu(p_1p_2) + \mu(p_1p_3) + \cdots + \mu(p_{s-1}p_s)) +$$

$$+ \cdots + \mu(p_1p_2 \ldots p_s),$$

já que $\mu(d) = 0$ sempre que um certo p_i^2 aparece na decomposição em números primos de d. Logo,

$$\mu * \mathbf{1}(n) = (+1)C_s^1 + (-1)C_s^2 + (+1)C_s^3 + \cdots + (-1)^s C_s^s = (1-1)^s = 0.$$

Corolário 4.4.2 *Para todo* $n \in \mathbb{N}$,

$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d}.$$

Prova:

De facto, já vimos que $\phi = \mathbf{1}^{-1} * i = \mu * i$.
Temos ainda um outro corolário importante:

Corolário 4.4.3 : Fórmula de Inversão de Moebius
Seja f uma função multiplicativa.
Então

$$F(n) = \sum_{d|n} f(d) \Leftrightarrow f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

Teminamos o capítulo com a seguinte fórmula explícita da função σ:

Propriedade 4.4.4 *Seja $n \in \mathbb{N}$.*
Se $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ é a decomposição em números primos de n, tem-se:

$$\sigma(n) = \prod_{i=1}^{r} \frac{p^{\alpha_i+1} - 1}{p - 1}.$$

Prova: σ é multiplicativa, logo

$$\sigma(n) = \prod_{i=1}^{r} \sigma(p_i^{\alpha_i}).$$

Basta observar que os divisores de p^{α_i} são os números $p_i^{\beta_i}$, com $0 \leq \beta_i \leq \alpha_i$, pelo que

$$\sigma(p^{\alpha_i}) = 1 + p_i + p_i^2 + \cdots + p^{\alpha_i} = \frac{p^{\alpha_i+1} - 1}{p - 1}.$$

5 Reciprocidade quadrática

5.1 Símbolo de Legendre

Definição 5.1.1 *Seja $p \in \mathbb{P}$.*
Para todo inteiro $n \in \mathbb{Z}$ define-se o símbolo de Legendre $\left(\frac{n}{p}\right)$ por:

$$\left(\frac{n}{p}\right) = \begin{cases} 0 \text{ se } n \equiv 0 \mod p \\ 1 \text{ se } n \not\equiv 0 \mod p \text{ e } \exists \alpha \in \mathbb{Z}\ ,\ n \equiv \alpha^2 \mod p \\ -1 \text{ nos restantes casos.} \end{cases}$$

Por outras palavras, $\left(\frac{n}{p}\right) = 1$ sse $\overline{n}$ for um quadrado não nulo de $\mathbb{F}_p$. Neste caso, diz-se que n é um resíduo quadrático módulo p.

Temos a seguinte propriedade imediata:

Propriedade 5.1.2 *Seja $p \in \mathbb{P}$ e $n \in \mathbb{Z}$.*
Então, para todo $k \in \mathbb{Z}$,

$$\left(\frac{n}{p}\right) = \left(\frac{n+kp}{p}\right).$$

É sempre possivel calcular "à mão"o valor de um símbolo de Legendre.

Por exemplo, quais os valores de $\left(\frac{3}{5}\right)$ e $\left(\frac{4}{5}\right)$?

Começamos por calcular todos os quadrados de $\mathbb{F}_5$:
$\overline{0}^2 = \overline{0}$, $\overline{1}^2 = \overline{1}$, $\overline{2}^2 = \overline{4}$, $\overline{3}^2 = \overline{9} = \overline{4}$ e $\overline{4}^2 = \overline{16} = \overline{1}$. Assim, os quadrados de $\mathbb{F}_p$ são $\overline{0}$,$\overline{1}$ e $\overline{4}$, pelo que $\left(\frac{3}{5}\right) = -1$ e $\left(\frac{4}{5}\right) = 1$.

Notemos ainda que existem, em $\mathbb{F}_5$, dois quadrados não nulos: $\overline{1}$ e $\overline{4}$. Este resultado é na realidade mais geral:

Propriedade 5.1.3
Para todo número primo $p \geq 3$, existem exactamente $\frac{p-1}{2}$ quadrados não nulos no corpo $\mathbb{F}_p$.

Prova:
Começamos por notar que para $j, k \in \{1; 2; \ldots; \frac{p-1}{2}\}$ tem-se $\overline{k}^2 \neq \overline{j}^2$ sempre que $j \neq k$. Caso contrário ter-se-ia

$$j^2 \equiv k^2 \mod p \Leftrightarrow (j-k)(j+k) \equiv 0 \mod p \Leftrightarrow p|j-k \text{ ou } p|j+k,$$

o que é absurdo, visto que $j+k \in \{2; \ldots; p-1\}$ e $|j-k| \in \{1; \ldots; \frac{p-3}{2}\}$.

Assim, existem pelo menos $\frac{p-1}{2}$ quadrados não nulos em $\mathbb{F}_p$.

Por outro lado, consideremos o polinómio

$$P(X) = X^{\frac{p-1}{2}}.$$

Se $\overline{n} = \overline{y}^2$ fôr um quadrado não nulo de $\mathbb{F}_p$, $P(\overline{n}) = \overline{y}^{p-1} - 1 = \overline{0}$, em virtude do pequeno teorema de Fermat ($p \not| y$). Assim, $\overline{n}$ é uma raíz de P em $\mathbb{F}_p$.
Como P possui no máximo $\frac{p-1}{2}$ raízes distintas, fica provada a propriedade.

Deste resultado deduz-se o seguinte critério:

Propriedade 5.1.4 : Critério de Euler
Seja $p \in \mathbb{P}$, $p \geq 3$ e $n \in \mathbb{Z}$.

Então

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \mod p.$$

Prova:
Se $n \equiv 0 \mod p$, não há nada a provar.
Suponhamos pois que $n \not\equiv 0 \mod p$.
No corpo $\mathbb{F}_p$ tem-se

$$(\overline{n}^{\frac{p-1}{2}})^2 = \overline{n}^{p-1} = \overline{1} = \overline{1}^2,$$

em virtude do pequeno teorema de Fermat. Assim,

$$0 = (\overline{n}^{\frac{p-1}{2}})^2 - \overline{1}^2 = (\overline{n}^{\frac{p-1}{2}} - \overline{1})(\overline{n}^{\frac{p-1}{2}} + \overline{1}),$$

de onde se tira que

$$\overline{n}^{\frac{p-1}{2}} = \overline{1} \text{ ou } \overline{n}^{\frac{p-1}{2}} = \overline{-1}.$$

Já vimos, na prova da Propriedade 5.1.3, que a primeira condição se verifica se e só se n fôr um resíduo quadrático. Fica assim provado o critério de Euler.

Para "pequenos"valores de n e p, o critério de Euler é extremamente útil para calcular o valor de $\left(\frac{n}{p}\right)$. Por exemplo,

$$\left(\frac{5}{11}\right) \equiv 5^5 \mod 11.$$

Tem-se $5^3 = 125 \equiv 4 \mod 11$ e $5^2 \equiv 3 \mod 11$, pelo que

$$5^5 = 5^2.5^3 \equiv 4.3 \equiv 12 \equiv 1 \mod 11,$$

pelo que 5 é um quadrado de $\mathbb{F}_{11}$.

Do Critério de Euler, resulta directamente a seguinte propriedade:

Propriedade 5.1.5 *Seja $p \in \mathbb{P}$, $p \geq 3$ e $n, m \in \mathbb{Z}$.*
Então

$$\left(\frac{n}{p}\right)\left(\frac{m}{p}\right) = \left(\frac{nm}{p}\right).$$

Prova:
De facto,

$$\left(\frac{nm}{p}\right) \equiv (mn)^{\frac{p-1}{2}} \equiv m^{\frac{p-1}{2}} n^{\frac{p-1}{2}} \equiv \left(\frac{n}{p}\right)\left(\frac{m}{p}\right) \mod p$$

Obtem-se agora o resultado observando que os valores possiveis dos símbolos de Legendre são -1,0 e 1.

5.2 Lema de Gauss

Propriedade 5.2.1 *:* **Lema de Gauss**
Seja $p \in \mathbb{P}$, $p \geq 3$. Para $x \in \mathbb{Z}$, denotamos por $\tilde{x}$ o único inteiro que verifica

$$x \equiv \tilde{x} \mod p \text{ e } -\frac{p-1}{2} \leq \tilde{x} \leq \frac{p-1}{2}.$$

Então, para $q \in \mathbb{Z}$, se $q \not\equiv 0 \mod p$, tem-se

$$\left(\frac{q}{p}\right) = (-1)^{\alpha},$$

onde α representa o número de inteiros negativos do conjunto

$$E = \{\tilde{q}, \widetilde{2q}, \widetilde{3q} \ldots, \widetilde{\frac{p-1}{2}q}\}.$$

Antes de apresentarmos a prova, calculemos $\left(\frac{3}{7}\right)$ com a ajuda deste lema:
temos $\widetilde{3} = 3$ ($\in \{-2; \ldots; 2; 3\}$) , $\widetilde{2.3} = -1$ e $\widetilde{3.3} = 2$, pelo que $\alpha = 1$ e $\left(\frac{3}{7}\right) = -1$.

Prova do lema de Gauss:
Vamos provar que se $k, l \in \{1; \ldots \frac{p-1}{2}\}$ e $k \neq l$, tem-se necessariamente $|\widetilde{kq}| \neq |\widetilde{lq}|$.

De facto, no caso contrário, ter-se-ia $kq \equiv \epsilon lq \mod p$, onde $\epsilon \in \{-1; 1\}$, ou ainda
$k \equiv \epsilon l \mod p$, visto que $p \not| q$.
Em ambos os casos se obtem uma contradição, já que $k \neq l$ e $k + l \in \{3; 4; \ldots; p-2\}$. Assim, os elementos de E são exactamente os $\frac{p-1}{2}$ primeiros inteiros naturais, a menos de sinal. Logo, o produto de todos os elementos de E vale

$$(\tilde{q})(\widetilde{2q})(\widetilde{3q}) \ldots \left(\widetilde{\frac{p-1}{2}}\right) = (-1)^{\alpha} \left(\frac{p-1}{2}\right)!$$

Visto que

$$(\tilde{q})(\widetilde{2q})(\widetilde{3q}) \ldots \left(\widetilde{\frac{p-1}{2}}\right) \equiv q^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{q}{p}\right) \left(\frac{p-1}{2}\right)! \mod p,$$

a prova fica concluída, tendo em conta o facto de $\left(\frac{p-1}{2}\right)!$ ser invertivel em $\mathbb{F}_p$.

Como aplicação, damos o seguinte corolário:

Corolário 5.2.2 *Seja $p \in \mathbb{P}$.*
Então

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \text{ e } \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Prova:
A primeira igualdade é uma consequência directa do critério de Euler.

Quanto à segunda, com as notações anteriores, tem-se

$$E = \{2, 4, 6, \ldots, 2[\frac{p-1}{4}], 2([\frac{p-1}{4}] + 1) - p, 2([\frac{p-1}{4}] + 2) - p, \ldots, -3, -1.$$

Assim, $\alpha = \frac{p-1}{2} - [\frac{p-1}{4}]$.

Se $p \equiv \pm 1 \mod [8]$, α é par, e se $p \equiv \pm 3 \mod [8]$, α é impar.
Assim, α possui sempre a paridade de $\frac{p^2-1}{8}$, ficando assim provada o corolário.

5.3 Lei de reciprocidade quadrática

Seja $p \in \mathbb{P}$ e $n \in \mathbb{Z}$.
n decompõe-se na forma

$$n = \epsilon 2^{k_o} \prod_{j=1}^{s} q_j^{k_j} \text{ , onde } \epsilon \in \{-1; 1\} \text{ , } k_j \in \mathbb{N} \text{ e } q_j \in \mathbb{P} \text{ , } q_j \geq 3.$$

Assim,

$$\left(\frac{n}{p}\right) = \left(\frac{\epsilon}{p}\right) \left(\frac{2}{p}\right)^k \prod \left(\frac{q_j}{p}\right)^{k_j}.$$

Visto já termos visto fórmulas para $\left(\frac{\epsilon}{p}\right)$ e $\left(\frac{2}{p}\right)$, para conhecer $\left(\frac{n}{p}\right)$ basta saber calcular $\left(\frac{q}{p}\right)$ para todo número primo ímpar q.

O instrumento para o fazer é a lei de reciprocidade quadrática, que se enuncia da seguinte forma:

Teorema 5.3.1 Lei de reciprocidade quadrática
Sejam $p \geq 3$ e $q \geq 3$ dois números primos distintos. Então

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Este teorema foi conjecturado por Euler, e demonstrado pela primeira vez por Gauss, que, com apenas 18 anos, forneceu 8 demonstrações diferentes.
Antes de vermos uma delas, ilustramos como a lei de reciprocidade quadrática pode ser utilizada para calcular qualquer símbolo de Legendre:

Cálculo de $\left(\frac{42}{107}\right)$ $(107 \in \mathbb{P})$.

Decompondo 42 em factores primos, vem

$$\left(\frac{42}{107}\right) = \left(\frac{2}{107}\right)\left(\frac{3}{107}\right)\left(\frac{7}{107}\right).$$

Tem-se $\left(\frac{2}{107}\right) = (-1)^{\frac{107^2-1}{8}} = -1$, pelo Corolário 5.2.2.
Pela lei de reciprocidade quadrática,

$$\left(\frac{3}{107}\right) = \left(\frac{107}{3}\right)(-1)^{\frac{(107-1)(3-1)}{4}} = -\left(\frac{107}{3}\right).$$

Pela Propriedade 5.1.2, $\left(\frac{107}{3}\right) = \left(\frac{-1}{3}\right) = -1$, de onde se tira que $\left(\frac{3}{107}\right) = 1$.

Da mesma forma,

$$\left(\frac{7}{107}\right) = \left(\frac{107}{7}\right)(-1)^{\frac{(107-1)(7-1)}{4}} = -\left(\frac{107}{7}\right) = -\left(\frac{2}{7}\right) = -(-1)^{\frac{7^2-1}{8}} = -1.$$

Finalmente,

$$\left(\frac{42}{107}\right) = (-1).(1).(-1) = 1.$$

Prova da Lei de Reciprocidade quadrática:
Vamos apresentar uma prova baseada numa interpretação geométrica do lema de Gauss.
Tem-se $\left(\frac{q}{p}\right) = (-1)^{\alpha}$, onde α é o número de inteiros negativos do conjunto

$$E = \{\tilde{q}, \widetilde{2q}, \widetilde{3q} \ldots, \widetilde{\frac{p-1}{2}q}\},$$

com as notações do lema de Gauss.
São exactamente os elementos $\widetilde{xq} \in E$, tais que existe $y \in \mathbb{Z}$ com $-\frac{p}{2} < xq - yp < 0$. Assim α é o número de pontos (x, y) de coordenadas inteiras no domínio

$$\{0 < x < \frac{p}{2}; x\frac{p}{q} < y < x\frac{p}{q} + \frac{1}{2}\}.$$

Necessariamente, $0 < y < \frac{p}{2} + \frac{1}{2}$ ou ainda, como $\frac{p+1}{2} \in \mathbb{N}$, $y \in]0; \frac{p}{2}[$.

Assim, α é o número de pontos (x, y) de coordenadas positivas no rectângulo

$$R = \{(x, y); 0 < x < \frac{q}{2} \text{ e } 0 < y < \frac{p}{2}\}$$

que verificam $-\frac{p}{2} < xq - yp < 0$.

Da mesma forma, $\left(\frac{p}{q}\right) = (-1)^{\beta}$, onde β é o número de pontos de coordenadas inteiras de R que verificam $-\frac{q}{2} < yp - xq < 0$.

Como R possui $\frac{p-1}{2}\frac{q-1}{2}$ pontos de coordenadas inteiras,

$$\frac{p-1}{2}\frac{q-1}{2} - (\alpha + \beta)$$

é o número de pontos de coordenadas inteiras de R que verifica

$$xq - yp = 0 \text{ ou } xq - yp \leq -\frac{p}{2} \text{ ou } xq - yp \geq \frac{q}{2}.$$

É fácil ver que o conjunto definido pela primeira igualdade é vazio e os dois conjuntos definidos pelas outras duas desigualdades são dijuntos e possuem o mesmo número de elementos.

Assim, $\frac{p-1}{2}\frac{q-1}{2} - (\alpha + \beta)$ é um número par:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\alpha+\beta} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

5.4 Congruências quadráticas

Neste capítulo pretendemos desenvolver um método para resolver congruências quadráticas, da forma

$$ax^2 + bx + c \equiv 0 \mod p \tag{5.1}$$

onde $p \in \mathbb{P}$, $p \geq 3$ e $a, b, c \in \mathbb{Z}$.

Para $a \not\equiv 0 \mod p$, (isto é, $a \neq 0$ em $\mathbb{F}_p$), temos $(4a, p) = 1$ e

$$(5.1) \Leftrightarrow 4a^2x^2 + 4abx + 4ac \equiv 0 \mod p \Leftrightarrow (2ax + b)^2 \equiv b^2 - 4ac \mod p.$$

Assim, com $\Delta := b^2 - 4ac$, $\left(\frac{\Delta}{p}\right) \neq -1$ é condição necessária de existência de soluções para a congruência (5.1).

Por outro lado, esta condição é suficiente:

Se existir $y \in \mathbb{Z}$ tal que $y^2 \equiv b^2 - 4ac \mod p$, basta resolver (em x) a congruência

$$2ax + b \equiv y \mod p \tag{5.2}$$

para se obter uma solução de (5.1). Ora, (5.2) possui sempre soluções, já que $(2a, p) = 1$, isto é, $2a$ é invertível em $\mathbb{F}_p$.

Fica assim provada a seguinte propriedade:

Propriedade 5.4.1 *Seja $p \in P$ e $a, b, c \in \mathbb{Z}$, com $(a, p) = 1$.*
Então, a congruência

$$ax^2 + bx + c \equiv 0 \mod p$$

possui solução sse

$$\left(\frac{\Delta}{p}\right) \neq 1 \text{ , onde } \Delta = b^2 - 4ac.$$

Torna-se agora importante determinar, no caso em que $\left(\frac{\Delta}{p}\right) = 1$, os valores de $y \in \mathbb{Z}$ para os quais $y^2 \equiv \Delta \mod p$, ou, por outras palavras as raízes $\mathbb{F}_p$-quadradas de Δ.

Para $\Delta = -1$ existe uma fórmula explícita:

Propriedade 5.4.2 *Seja $p \in \mathbb{P}$, com $p \equiv 1 \mod 4$ (isto é $\left(\frac{-1}{p}\right) = 1$).*
Então,

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \mod p.$$

Assim,

$$x^2 \equiv -1 \mod p \Leftrightarrow x \equiv \pm\left(\frac{p-1}{2}\right)! \mod p.$$

Prova:
Trata-se de uma consequência imediata do teorema de Wilson.

No caso geral, não existe uma fórmula geral, podendo-se no entanto recorrer a uma tabela de raízes primitivas.
Relembramos este conceito: para $p \in \mathbb{P}$, o grupo multiplicativo $\mathbb{F}_p^*$ é cíclico, ou seja, é gerado por um só elemento. Tal gerador tem então ordem $p - 1$ e é dito "raíz primitiva módulo p".

Exemplo em $\mathbb{F}_7^*$
$\overline{2}^1 = \overline{2}$, $\overline{2}^2 = \overline{4}$, $\overline{2}^3 = \overline{8} = \overline{1}$, logo $\overline{2}$ tem ordem 3.

$\overline{3}^1 = \overline{3}$, $\overline{3}^2 = \overline{9} = \overline{2}$, $\overline{3}^3 = \overline{6}$, $\overline{3}^4 = \overline{18} = \overline{4}$,$\overline{3}^5 = \overline{12} = \overline{5}$, $\overline{3}^6 = \overline{15} = \overline{1}$, logo $\overline{3}$ tem ordem 6: é uma raíz primitiva módulo 7.

Os índices de $\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}$ são respectivamente $6, 2, 1, 4, 5, 3$.

Definição 5.4.3 *Seja $p \in \mathbb{P}$ e g uma raíz primitiva módulo p.*
Para todo elemento $x \in \mathbb{F}_p^*$. Todo inteiro $i \in \mathbb{Z}$ tal que

$$g^i = x$$

é dito índice de x relativamente a g.

Nota: O índice de um elemento de $\mathbb{F}_p^*$ relativamente a uma raíz primitiva está determinado módulo $p-1$.

Assim, como vimos, Os índices de $\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}$ em $\mathbb{F}_7^*$ relativamente à raíz primitiva $\overline{3}$ são respectivamente $6, 2, 1, 4, 5, 3$.

Não existem regras gerais para determinar as raízes primitivas módulo p, podendo-se recorrer a tabelas de raízes primitivas. Como utilizar uma tal tabela para calcular raízes $\mathbb{F}_p$-quadradas?

Seja $p \in \mathbb{P}$, $p \geq 3$ e $n \in \mathbb{Z}$ tal que $\left(\frac{n}{p}\right) = 1$. Seja g uma raíz primitiva módulo p e i o índice de $\overline{n} \in \mathbb{F}_p^*$, isto é, $\overline{n} = g^i$. Pretendemos determinar $\overline{x} \in \mathbb{F}_p^*$ tal que $\overline{x}^2 = \overline{n}$. Seja j o índice de x relativo a g:

$$\overline{x}^2 = g^{2j} = g^i.$$

Assim, necessariamente, $g^{2j-i} = \overline{1}$: $i \equiv 2j \mod p-1$. Logo, i é par e podemos obter simplesmente $j = \frac{i}{2}$.

Exemplo: Tem-se $\left(\frac{5}{31}\right) = 1$.
Pretendemos determinar as raízes $\mathbb{F}_p$ quadradas de $\overline{5}$.
A tabela indica-nos que relativamente à raíz primitiva $g = 3$, o índice de $\overline{5}$ é $i = 20$, isto é,

$$\overline{5} = \overline{3}^{20} = (\overline{3^{10}})^2 = \overline{25}^2,$$

já que, pela tabela, $\overline{25}$ tem índice 10.
Assim,

$$x^2 = \overline{5} \Leftrightarrow x^2 = \overline{25}^2 \Leftrightarrow (x - \overline{25})(x + \overline{25}) = 0 \Leftrightarrow x = \pm\overline{25} \Leftrightarrow x = \overline{25} \text{ ou } x = \overline{6}.$$

A tabela pode ainda der útil para multiplicar elementos de $\mathbb{F}_p^*$, sendo então usada como uma autêntica tabela de logaritmos:
Suponhamos que pretendemos conhecer o produto $\overline{27}.\overline{34}$ em $\mathbb{F}_{37}^*$. A tabela diz-nos que $g = \overline{2}$ é raíz primitiva e $\overline{27} = g^6$, $\overline{34} = g^8$.
Assim,

$$\overline{27}.\overline{34} = g^{6+8} = \overline{30}.$$

5.5 Trinómios em $\mathbb{Z}_n$

Teorema 5.5.1 *Seja $p \in \mathbb{P}$ ($p \geq 3$ e $a, b, c \in \mathbb{Z}$, $p \nmid a$. A congruência*

$$ax^2 + bx + c \equiv 0 \mod p \tag{5.3}$$

possui duas soluções incongruentes módulo p se $\left(\frac{\Delta}{p}\right) = 1$, uma se $\left(\frac{\Delta}{p}\right) = 0$ e não possui soluções se $\left(\frac{\Delta}{p}\right) = -1$. Aqui, $\Delta := b^2 - 4ac$.

Observemos que, no corpo $\mathbb{Z}_p$,

$$\overline{a}x^2 + \overline{b}x + \overline{c} = 0 \Leftrightarrow \overline{4a^2}x^2 + \overline{4ab}x + \overline{4ac} = 0 \text{ (porque } (4a, p) = 1 : \ \overline{4a} \text{ invertível em } \mathbb{Z}_p)$$

$$\Leftrightarrow (\overline{2a}x + \overline{b})^2 = \overline{b^2 + 4ac} = \overline{\Delta}.$$

Assim,

- Se $\left(\frac{\Delta}{p}\right) = -1$, $\overline{\Delta}$ não é um quadrado em $\mathbb{Z}_p$, e (5.3) não tem solução.
- Se $\left(\frac{\Delta}{p}\right) = 0$, $\overline{\Delta} = 0$, e
$$(\overline{2a}x + \overline{b}) = \overline{0} \Leftrightarrow x = -\overline{b}.\overline{2a}^{p-2}.$$
- Se $\left(\frac{\Delta}{p}\right) = 0$, existe $\overline{\alpha} \neq \overline{0}$ tal que $\overline{\Delta} = \overline{\alpha}^2$. Assim,
$$(\overline{2a}x + \overline{b})^2 = \overline{\alpha}^2 \Leftrightarrow (\overline{2a}x + \overline{b} - \overline{\alpha})(\overline{2a}x + \overline{b} - \overline{\alpha}) = 0.$$
$$\Leftrightarrow (\overline{2a}x + \overline{b} - \overline{\alpha}) = \overline{0} \text{ ou } (\overline{2a}x + \overline{b} + \overline{\alpha}) = \overline{0},$$
isto é,
$$x = \overline{2a}^{p-2}(-\overline{b} \pm \overline{\alpha}).$$
Note que este cálculo apenas é válido porque $\mathbb{Z}_p$ é um corpo: não possui divisores de 0.

Exemplo: Soluções de $x^2 + 2x - 1 = 0$ no corpo $\mathbb{Z}_1 7$?

Calculando neste corpo, tem-se:

$$x^2 + 2x - 1 = 0 \Leftrightarrow 4x^2 + 8x - 4 = 0 \Leftrightarrow (2x + 2)^2 - 4 - 4 = 0 \Leftrightarrow (2x + 2)^2 = 8 \Leftrightarrow (x + 1)^2 = 2.$$

Nota: Havia um processo mais rápido de chegar a este resultado! Utilizámos no entanto o"método"de multiplicar pelo invertivel "$4a$", visto este processo "resultar"sempre.

Assim, devemos avaliar $\left(\frac{2}{17}\right)$:

$$\left(\frac{2}{17}\right) = (-1)^{\frac{17^2-1}{8}} = 1.$$

Logo, existe $\alpha \in \mathbb{Z}_{17}$ $(\alpha \neq 0)$, com $\alpha^2 = 17$.

Recorrendo a uma tabela de raízes primitivas:

$$2 = 3^1 4 = (3^7)^2 = 11^2.$$

Nota: o facto de 2 ter índice par (14) relativamente à raíz primitiva $g = 3$ móldulo 17 teria sido suficiente para afirmar que $\left(\frac{2}{17}\right) = 1$!

Finalmente, obtem-se

$$(x+1)^2 = 11^2 : x = 10 \text{ ou } x = -12 = 5.$$

Para resolver um trinómio no anel $\mathbb{Z}_n$, com $\mu(n) \neq 0$, deverá proceder-se da seguinte forma: $n = p_1 p_2 \dots p_r$, onde os p_i são números primos. Assim,

$$ax^2 + bx + c \equiv 0 \mod n \Leftrightarrow \forall i \in \{1; \dots; r\},\ ax^2 + bx + c \equiv 0 \mod p_i.$$

Bastará pois resolver cada equação do sistema com o método apresentado, e concluir com o teorema dos restos chineses.

E como resolver $ax^2 + bx + c = 0$ em $\mathbb{Z}_{p^n}$, onde $p \in \mathbb{P}$ e $n \in \mathbb{N}$? Observemos o seguinte:

Teorema 5.5.1 *Seja $n \geq 2$ e $p \in \mathbb{P}$.*

Se x_n é solução da congruência $ax^2 + bx + c \equiv 0 \mod p^n$, então

$$x_n = x_{n-1} + k_{n-1} p^{n-1},$$

onde x_{n-1} é solução de $ax^2 + bx + c \equiv 0 \mod p^{n-1}$.
Além disso, k_{n-1} é raíz de uma congruência linear módulo p facilmente determinável em função de a, b, c e x_{n-1}.

Prova:
Seja um tal x_n: $ax_n^2 + bx_n + c \equiv 0 \mod p^n$.
Em particular $ax_n^2 + bx_n + c \equiv 0 \mod p^{n-1}$. Assim, para todo k_{n-1},

$$x_{n-1} := x_n - k_{n-1} p^{n-1}$$

é solução de $ax^2 + bx + c \equiv 0 \mod p^{n-1}$.

Finalmente, usando o facto de x_n ser solução de $ax^2 + bx + c \equiv 0 \mod p^n$:

$$a(x_{n-1} + k_{n-1}p^{n-1})^2 + b(x_{n-1} + k_{n-1}p^{n-1}) + c \equiv 0 \mod p^n.$$

$$\Leftrightarrow$$

$$[ax_{n-1}^2 + bx_{n-1} + c] + 2ax_{n-1}k_{n-1}p^{n-1} + p^{2(n-1)} + bx_{n-1}p^{n-1} \equiv 0 \mod p^n.$$

$$\Leftrightarrow$$

$$[ax_{n-1}^2 + bx_{n-1} + c] + 2ax_{n-1}k_{n-1}p^{n-1} + bx_{n-1}p^{n-1} \equiv 0 \mod p^n.$$

Visto que $ax_{n-1}^2 + bx_{n-1} + c$ é divisivel por p^{n-1}, dividindo toda a congruência por p^{n-1} obtem-se a congruência linear em k_{n-1}:

$$\frac{1}{p^{n-1}}[ax_{n-1}^2 + bx_{n-1} + c] + 2ax_{n-1}k_{n-1} + bx_{n-1} \equiv 0 \mod p.$$

Iterando este resultado obtêm-se que as solução de

$$ax^2 + bx + c \equiv 0 \mod p^n$$

são da forma

$$x_n = k_1 + k_2p + k_3p^2 + \ldots k_np^{n-1},$$

onde os k_j podem ser calculados iterativamente.

Exemplo: Soluções de $x^2 \equiv 2 \mod 7^3$.

Começamos por resolver

$${k_1}^2 \equiv 2 \mod 7 :$$

$${k_1}^2 \equiv 2 \mod 7 \Leftrightarrow {k_1}^2 \equiv 3^2 \mod 7 \Leftrightarrow k_1 \equiv 3 \mod 7 \text{ ou } k_1 \equiv 4 \mod 7.$$

Procuramos agora soluções da forma $x_2 = k_1 + 7k_2$ para a congruência

$$x_2^2 \equiv 2 \mod 7^2 :$$

$$x_2^2 \equiv 2 \mod 7^2 \Leftrightarrow (k_1 + 7k_2)^2 \equiv 2 \mod 7^2 \Leftrightarrow k_1^2 + 14k_1k_2 \equiv 2 \mod 7^2.$$

- Para $k_1 = 4$, obtem-se

  $$14 + 14.4k_2 \equiv 0 \mod 7^2,$$

  e, divindo toda a congruência por 7:

  $$8k_2 + 2 \equiv 0 \mod 7 \Leftrightarrow k_2 = -4^{7-2} \mod 7 \Leftrightarrow k_2 \equiv 5 \mod 7.$$

- Para $k_1 = 3$:

$$7 + 14.3k_2 \equiv 0 \mod 7^2,$$

e, divindo toda a congruência por 7:

$$6k_2 + 1 \equiv 0 \mod 7 \Leftrightarrow k_2 = -6^{7-2} \mod 7 \Leftrightarrow k_2 \equiv 1 \mod 7.$$

Assim, as soluções incongruentes módulo 7^2 de

$$x^2 \equiv 2 \mod 7^2$$

são $x_2 = 4 + 7.5 = 39$ e $x_2 = 3 + 7.1 = 10$.

Se desejamos agora as soluções de

$$x^2 \equiv 2 \mod 7^3$$

iteramos o processo mais uma vez: procuramos agora soluções da forma $x_3 = x_2 + 7^2 k_3$:

$$x^2 \equiv 2 \mod 7^3 \Leftrightarrow (x_2 + 7^2 k_3)^2 \equiv 2 \mod 7^3 \Leftrightarrow x_2^2 + 2.7^2 k_3 x_2 \equiv 2 \mod 7^3.$$

- Para $x_2 = 39$, obtem-se

$$39^2 + 2.7^2.39k_3 \equiv 2 \mod 7^3 \Leftrightarrow 31 + 78.k_3 \equiv 0 \mod 7.$$

Nota: o facto de $1519 = 39^2 - 2$ ser divisivel por 49 não é um "milagre"mas antes uma consequência do Lema 5.5.1 !

Obtem-se assim $k_3 \equiv 4 \mod 7$.

- Para $x_2 = 10$,

$$10^2 + 2.7^2.10k_3 \equiv 2 \mod 7^3 \Leftrightarrow 2 + 20k_3 \equiv 0 \mod 7 : \ k_3 = 2.$$

Finalmente, as soluções incongruentes de

$$x^2 \equiv 2 \mod 7^3$$

são $x = 39 + 4.7^2 = 235$ e $x = 10 + 2.7^2 = 108$.

Aplicação: Raízes de $x^2 + 2x - 1 \equiv 0 \mod 833$?

Alguns cálculos elementares já feitos mostram que esta equação é equivalente a

$$(x + 1)^2 \equiv 2 \mod 833.$$

$833 = 19.7^2$. Como $(19, 7) = 1$, a equação é equivalente ao sistema

$$\begin{cases} (x+1)^2 \equiv 2 \mod 17 \\ (x+1)^2 \equiv 2 \mod 49 \end{cases}$$

Já resolvemos cada uma destas equações, tendo obtido

$$\begin{cases} x \equiv 10 \mod 17 \text{ ou } x \equiv 5 \mod 17 \\ x \equiv 38 \mod 49 \text{ ou } x \equiv 9 \mod 49 \end{cases}$$

Temos pois de resolver quatro sistemas: os sistemas

$$\begin{cases} x \equiv a_1 \mod 17 x \equiv a_2 \mod 49 \end{cases}$$

para $(a_1, a_2) \in \{(10, 38), (10, 9), (5, 38), (5, 9)$.
Com $m = 833$, $m_1 = 17$, $m_2 = 49$, As soluções deste sistema são da forma

$$x = a_1.b_1\frac{m}{m_1} + a_2.b_2\frac{m}{m_2} + km \ , \ k \in \mathbb{Z},$$

onde os b_i são tais que $b_i\frac{m}{m_i} \equiv 1 \mod m_i$.

Assim, $49b_1 \equiv 1 \mod 17$: podemos escolher $b_1 = 26$, e
$17b_2 \equiv 1 \mod 49$: podemos escolher $b_2 = 8$.
Assim, as soluções são dadas por

$$x = 442a_1 + 392a_2 + k833 \ , \ k \in \mathbb{Z}.$$

Obtem-se, fazendo o cálculo,

$$x \equiv 107 \mod 833 \text{ ou } x \equiv 401 \mod 833 \text{ ou } x \equiv 430 \mod 833 \text{ ou } x \equiv 724 \mod 833.$$

Note que encontrámos quatro raízes distintas em $\mathbb{Z}_{833}$ para um polinómio de grau 2.
Não há qualquer contradição, visto este anel possuir divisores de 0: tudo é possivel!

6 O Problema de Waring

6.1 A equação $a^2 + b^2 = n$

Neste capítulo vamos determinar quais os inteiros que se podem respresentar como soma de dois quadrados.

Teorema 6.1.1 *Seja $p \in \mathbb{P}$.*
A equação $a^2 + b^2 = p$ possui uma solução $(a, b) \in \mathbb{Z}^2$ se e só se

$$p = 2 \text{ ou } p \equiv 1 \mod 4.$$

Prova:

$\Rightarrow$ Suponhamos que $p = a^2 + b^2$.
O quadrado de um número inteiro é congruente com 0 (se for par) ou com 1 (se for impar) módulo 4.

Assim, $p \equiv a^2 + b^2 \equiv \epsilon \mod 4$, onde $\epsilon \in \{0; 1; 2\}$. Daqui se conclui que $p = 2$ ou $p \equiv 1 \mod 4$.

$\Leftarrow$ Se $p = 2$, $p = 1^2 + 1^2$.
Seja $p \in \mathbb{P}$, com $p \equiv 1 \mod 4$.

Tem-se que $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$, logo existe $x \in \mathbb{Z}$ com $x^2 \equiv -1 \mod p$.

Seja m a parte inteira de $\sqrt{p}$. Como $\sqrt{p} \notin \mathbb{N}$, $m < \sqrt{p} < m + 1$.

Finalmente, consideramos a função

$$f : (u, v) \in \{0; 1; \ldots; m\}^2 \to \overline{u + xv} \in \mathbb{Z}_p.$$

O domínio e f possui $(m + 1)^2$ elementos e o contradomínio $p < (m + 1)^2$.
Logo f não é injectiva:
existem dois pares (u_1, v_1) e (u_2, v_2) distintos com $f(u_1, v_1) = f(u_2, v_2)$, isto é

$$u_1 + xv_1 \equiv u_2 + xv_2 \mod p.$$

Assim,

$$u_1 - u_2 \equiv x(v_2 - v_1) \mod p.$$

Elevando ao quadrado:

$$(u_1 - u_2)^2 + (v_1 - v_2)^2 \equiv 0 \mod p.$$

Sejam $a = u_1 - u_2$ e $b = v_1 - v_2$.

- $p|a^2 + b^2$.
- $a^2 + b^2 > 0$ (porque os pares (u_1, v_1) e (u_2, v_2) são distintos).
- $a^2 + b^2 \leq m^2 + m^2 < 2p$.

Como $p \in \mathbb{P}$, necessariamente,

$$p = a^2 + b^2.$$

O seguinte lema mostra que se dois números inteiros n e m se escrevem como soma de dois quadrados, mn também:

Teorema 6.1.2 *Sejam $a, b, c, d \in \mathbb{Z}$. Tem-se*

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2.$$

Prova: É só fazer o cálculo!

Podemos agora enunciar o teorema principal:

Teorema 6.1.1 *Seja $n \in \mathbb{N}$.*
n é a soma de dois quadrados se e só se a decomposição de n em números primos é da forma

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}, \text{ com } \alpha_i \text{ par sempre que } p_i \equiv 3 \mod 4.$$

Prova:
$\Leftarrow$ Seja um tal n:

$$n = 2^{\alpha} \prod p_i^{\alpha_i} \prod q_j^{\beta_j},$$

onde $p_i, q_i \in \mathbb{P}$, $p_i \equiv 1 \mod 4$, $q_i \equiv 3 \mod 4$ e β_j pares.
Assim,

$$n = 2^{\alpha} \prod p_i^{\alpha_i} \prod (q_j^2 + 0^2)^{\frac{\beta_j}{2}}.$$

Pelo Lema 6.1.1, todos os factores se escrevem como soma de dois quadrados. Assim, utiizando iteradamente o Lema 6.1.2, n é a soma de dois quadrados.

$\Rightarrow$ Suponhamos que $n = a^2 + b^2$ e, por exemplo, β_1, a potência de q_1 é impar.
Seja $d = (a, b)$. Seja

$$k = \frac{n}{d^2} = \left(\frac{a}{d}\right)^2 + \left(\frac{b}{d}\right)^2.$$

q_1 aparece com potência impar na decomposição de k. Em particular, $q_1|k$.
Por outro lado, $k_1 = \frac{a}{d}$ e $k_2 = \frac{b}{d}$ são primos entre si.
Logo q_1 não pode dividir simultaneamente k_1 e k_2.
Como q_1 divide $k_1^2 + k_2^2$, $q_1 \nmid k_1$ e $q_1 \nmid k_2$.

Assim, existe $x \in \mathbb{Z}$, com $xk_1 \equiv k_2 \mod q_1$.
Finalmente,

$$0 \equiv k \equiv k_1^2 + k_2^2 \equiv k_1^2(1 + x^2) \mod q_1.$$

Como $q_1 \nmid k_1^2$, $x^2 \equiv -1 \mod q_1$, o que é absurdo visto $q_1 \equiv 3 \mod 4$.

Exemplo: $n = 765$**:**

$n = 3^2.5.17$: 5 e 17 são congruentes com 1 módulo 4. 3 é congruente com 3 módulo 4 mas está ao quadrado. Logo 765 pode ser representado como soma de quadrados. Fazemos a representação para cada factor:

$$3^2 = 3^2 + 0^2 \text{ , } 5 = 2^2 + 1^2 \text{ e } 17 = 4^2 + 1^2.$$

Utilizando a fórmula do Lema 6.1.2,

$$765 = (3^2 + 0^2)(2^2 + 1^2)(4^2 + 1^2) = (6^2 + 3^2)(4^2 + 1^2) = (24 + 3)^2 + (6 - 12)^2 = 27^2 + 6^2.$$

6.2 A equação $x^2 + y^2 = z^2$

Definição 6.2.1

O trio $(x, y, z) \in \mathbb{N}^3$ *diz-se um triângulo pitagórico se*

$$x^2 + y^2 = z^2.$$

z diz-se então a hipotenusa do triângulo. Se x,y e z são primos entre si, (x, y, z) *diz-se triângulo pitagórico primitivo.*

Afim de determinar todos os triângulos pitagóricos, vamos explicitar no que se segue todos os que são primitivos. Eis algumas propriedades destes triângulos:

Propriedade 6.2.2 *Seja (x, y, z) um triângulo pitagórico primitivo. Então:*
i. $(x, y) = (x, z) = (y, z) = 1$.
ii. *z é impar e x e y possuem paridade oposta.*
iii. *Se x é o elemento impar,*

$$(z - x, z + x) = 2.$$

i. Seja $d = (x, y)$. Como $z^2 = x^2 + y^2$, $d^2 | z^2 : d | z$. Logo d é divisor comum de x, y, z: $d = 1$. Da mesma forma se prova que $(y, z) = (x, z) = 1$.

ii. Apenas um dos números x, y e z pode ser par, pela alínea anterior. Se z é par: $z^2 \equiv 0 \mod 4$. Como x e y são impares, $x^2 + y^2 \equiv 2 \mod 4$, o que é absurdo.
Assim z é impar e x ou y é par. Por convenção, y será sempre o elemento par.

iii. É um pequeno exercício clássico:
Seja $d = (z - x, z + x)$: $d | 2x$, $d | 2y$, logo $d | (2x, 2y) = 2(x, y) = 1$.

Fica como exercício a prova do seguinte lema:

Teorema 6.2.1 *Sejam $a, b \in \mathbb{N}$, $(a, b) = 1$.*
Se $ab = c^2$, então existem r e s com $a = r^2$ e $b = s^2$ e $(r, s) = 1$.

Finalmente:

Propriedade 6.2.3 *As soluções primitivas de*

$$x^2 + y^2 = z^2,$$

com y par são:

$$x = r^2 - s^2 \ , \ y = 2rs \ , \ z = r^2 + s^2 \ \text{onde } r > s > 0 \ \text{e } (r, s) = 1.$$

Para mais, r e s são de paridade oposta.

Por um lado, um simples cálculo prova que $(x = r^2 - s^2, y = 2rs, z = r^2 + s^2)$ é um trio pitagórico, e que x, y, z são primos entre si.

Seja agora (x, y, z) um trio pitagórico primitivo.

Como $(z - x, z + x) = 2$, $z - x = 2u$ e $z + x = 2v$, com $(u, v) = 1$.
Assim,

$$y^2 = z^2 - x^2 = (z - x)(z + x) = 4uv,$$

pelo que $2|y$ e

$$(\frac{y}{2})^2 = uv.$$

Pelo Lema 6.2.1, existem r e s primos entre si tais que $u = r^2$ e $v = s^2$. Daqui resulta facilmente que $x = r^2 - s^2$, $y = 2rs$ e $z = r^2 + s^2$.
Finalmente, r e s são de paridade oposta já que z é impar.

Corolário 6.2.4 *Seja* $(x, y, z) \in \mathbb{N}$.
Então

$$(x, y, z) \text{ pitagórico } \Leftrightarrow \exists (r, s, d) \ , \ \ , \ x = d(r^2 - s^2) \ , \ y = 2drs \ , \ z = d(r^2 + s^2,)$$

onde $r > s$, $(r, s) = 1$ *e* r *e* s *são de paridade oposta.*

Prova:

$\Leftarrow$ É evidente.
$\Rightarrow$ Seja $d = (x, y, z)$. Basta observar que $(\frac{x}{d}, \frac{y}{d}, \frac{z}{d})$ é um trio pitagórico primitivo.

6.3 A equação $x^4 + y^4 = z^2$

Na realidade, esta equação não possui soluções não triviais, isto é, tais que $xyz \neq 0$.

Suponhamos que existe uma solução não trivial.
Seja x_o, y_o, z_o uma solução tal que $z_o > 0$ é minimal. Necessariamente, x_o, y_o, z_o são primos entre si. Senão, existiria $p \in \mathbb{P}$ divisor comum de x, y e z. Então, $(\frac{x_o}{p}, \frac{y_o}{p}, \frac{z_o}{p^2})$ é solução, o que contradiz a minimalidade de z_o.

Assim, (x_o^2, y_o^2, z_o) é um triângulo pitagórico primitivo.

Logo, existem (a, b) primos entre si com

$$x_o^2 = a^2 - b^2 \ , \ y_o^2 = 2ab \ , \ z_o = a^2 + b^2.$$

a é impar: de facto, se a é par, b é impar, e

$$x_o^2 \equiv -1 \mod 4,$$

o que é absurdo.

Assim, $x_o^2 + b^2 = a^2$ é outro triângulo pitagórico primitivo, b par.

Logo, existem r, s com $r > s$, $(r, s) = 1$ tais que

$$b = 2rs,\ x_o = r^2 - s^2 \text{ e } a = r^2 + s^2.$$

Logo,

$$y_o^2 = 2ab = 4rs(r^2 + s^2).$$

Como $(r, s) = 1$, r,s e $r^2 - s^2$ são quadrados:

$$r = u^2,\ s = v^2,\ s^2 + r^2 = t^2,$$

de onde resulta que

$$u^4 + v^4 = t^2.$$

Temos pois uma outra solução da equação inicial. A contradição resulta do facto de $t < z_o$:

$$t^2 = s^2 + r^2 = a < a^2 + b^2 = z.$$

Este processo de prova chama-se "descida infinita de Fermat.

Corolário 6.3.1
A equação

$$x^4 + y^4 = z^4$$

não possui soluções não triviais.

Nota: Trata-se de um caso particular do famoso teorema de Fermat-Wiles.

6.4 O teorema de Waring

Propriedade 6.4.1 : Identidade de Lagrange

Sejam $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4 \in \mathbb{Z}$. *Então*

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 + (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2.$$

Prova: É só fazer o cálculo!

Esta surpreendente igualdade diz em particular que se dois números inteiros se excrevem como soma de quatro quadrados, o seu produto também.
Neste capítulo, vamos provar o seguinte resultado, conhecido como problema de Waring de ordem 2:

Teorema 6.4.1 *Todo número inteiro natural n pode ser escrito como soma de quatro quadrados.*

Pela observação, basta provar o resultado para $n \in \mathbb{P}$, já que todo inteiro natural se escreve como produto de números primos.

Teorema 6.4.1 *Seja* $p \in \mathbb{P}$.
Existem $x, y \in \mathbb{Z}$ *e* $m \in \{1; \ldots; p-1\}$ *tais que*

$$1 + x^2 + y^2 = mp.$$

Prova:
Suponhamos que $p \geq 3$.
Comecemos por observar que os $\frac{p+1}{2}$ números x^2, com $0 \leq x \leq \frac{p-1}{2}$, são todos distintos módulo p (cf. prova da Propriedade 5.1.3).
Da mesma forma os $\frac{p+1}{2}$ números da forma $-1 - y^2$, onde $0 \leq y \leq \frac{p-1}{2}$, são distintos módulo p.
O conjunto

$$E = \{x^2; 0 \leq x \leq \frac{p-1}{2}\} \cup \{-1 - y^2; 0 \leq y \leq \frac{p-1}{2}\},$$

possuindo $p+1$ elementos e existindo apenas p classes de resíduos módulo p, podemos afirmar a existência de $x, y \in \{0; \ldots; \frac{p-1}{2}\}$ tais que

$$1 + x^2 + y^2 \equiv 0 \mod p,$$

pelo "princípio das gavetas".

Logo, existe $m \in \mathbb{Z}$ tal que $1 + x^2 + y^2 = mp$.
Como $1 + x^2 + y^2 < 1 + 2\frac{p^2}{4} < p^2$, $m < p$.

A propriedade sendo evidente para $p = 2$, fica provado o lema.
Prova do Teorema 6.4.1:
Como $1 = 0^2 + 1^2$, fica provada, pelo lema anterior, a existência de x_1, x_2, x_3 e x_4 inteiros tais que

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp \ , \ 0 < m < p,$$

para todo $p \in \mathbb{P}$, $p \geq 3$.

Seja m_o um mais pequeno inteiro tal que $m_o p$ se escreve como soma de quatro quadrados. Provamos agora que $m_o = 1$.
Suponhamos que $m_o > 1$.
Se m_o é par, então $m_o p$ é par. Existem então três possibilidades:
i. Todos os x_i^2 são pares (então todos os x_i são pares).
ii)Todos os x_i^2 são impares (então todos os x_i são impares).
iii) Dois dos x_i^2 são pares e dois são impares, por exemplo x_3^2 e x_4^2 (então x_1 e x_2 são pares, e x_3,x_4 impares).

Em todos os casos, $x_1 + x_2$, $x_1 - x_2$, $x_3 + x_4$, $x_3 - x_4$ são números pares.
Assim,

$$(\frac{x_1 + x_2}{2})^2 + (\frac{x_1 - x_2}{2})^2 + (\frac{x_3 + x_4}{2})^2 + (\frac{x_3 - x_4}{2})^2 = \frac{1}{2}(x_1^2 + x_2^2 + x_3^2 + x_4^2) = \frac{1}{2} m_o p,$$

o que contradiz a minimalidade de m_o.

Logo, m_o é impar, mais precisamente $3 \leq m_o < p$.
Definimos agora y_i por: $y_i \equiv x_i \mod m_o$ e $-\frac{m_o - 1}{2} \leq y_i \leq \frac{m_o - 1}{2}$.

Tem-se $y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \mod m_o$ e $y_1^2 + y_2^2 + y_3^2 + y_4^2 \leq (m_o - 1)^2$ pelo que

$$\exists n \in \{0; \ldots; m_o - 1\} \ , \ y_1^2 + y_2^2 + y_3^2 + y_4^2 = m_o n.$$

n é não nulo, se não ter-se-ia todos os y_i nulos e consequentemente todos os x_i diviseis por p. Então, $m_o p$ seria divisivel por p^2, o que é absurdo.

Finalmente,

$$m_o^2 pn = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = Z_1^2 + Z_2^2 + Z_3^2 + Z_4^2$$

para certos Z_i, pela identidade de Lagrange. Verifica-se facilmente que para todo i, $m_o | Z_i$, pelo que

$$np = \left(\frac{Z_1}{m_o}\right)^2 + \left(\frac{Z_2}{m_o}\right)^2 + \left(\frac{Z_3}{m_o}\right)^2 + \left(\frac{Z_4}{m_o}\right)^2,$$

com $n < m_o$ o que contraria a minimalidade de m_o.
Assim $m_o = 1$ e a prova está concluida.

Por exemplo, se quisermos escrever $143 = 11 \times 13$ como soma de quatro quadrados, basta descobrir a decomposição de 11 e 13:
Por exemplo, $13 = 3^2 + 2^2 + 0^2 + 0^2$ e $11 = 3^2 + 1^2 + 1^2 + 0^2$.
Assim, pela identidade de Lagrange,

$$\begin{aligned} 143 = 13 \times 11 = (3^2 + 2^2 + 0^2 + 0^2)(3^2 + 1^2 + 1^2 + 0^2) = (3.3 + 2.1 + 0.1 + 0.0)^2 + \\ + (3.1 - 2.3 + 1.0 - 0.0)^2 + (3.1 - 0.3 + 0.1 - 2.0)^2 + (3.0 + 0.3 + 2.1 - 0.1)^2, \end{aligned}$$

ou seja,

$$146 = 11^2 + 3^2 + 3^2 + 2^2.$$

Referências

1. Théorie des Nombres, D. Duverney, Dunod, 1998.
2. Introduction à la théorie des nombres, JM De Koninck & A Mercier, Collection Universitaire de Mathématiques, 1994.