MAT. FINITA e MAT. DISCRETA 2016/2017-

Prof. Ilda Perez

Parte II: Teoria elementar de números

.

1. Divisão com resto

Teorema 1(Divisão com resto nos inteiros)

Dados um número natural $a \in \mathbb{N}$ *e um número inteiro* $b \in \mathbb{Z}$, *b escreve-se de modo único:*

$b = aq + r$, *com* $q \in \mathbb{Z}$ *e* $r \in \mathbb{N}_0$, $0 \leq r < a$

q é o quociente da divisão de b por a e r é o resto da divisão de b por a.

Dem. Qualquer que seja o inteiro b ele está compreendido entre dois múltiplos inteiros de a, isto é, existe um único inteiro $q \in \mathbb{Z}$ tal que $aq \leq b < a(q+1)$, ou o que é equivalente $b = aq + r$, *com* $0 \leq r < a$.

Os próximos Teoremas 2 e 3 são duas consequências importantes do Teorema da divisão com resto:

Teorema 2 (Representação de um número numa base B)

Dado um número natural $B > 1$ *qualquer número natural* $n \in \mathbb{N}$ *escreve-se de maneira única na forma:*

$n = a_k B^k + a_{k-1} B^{k-1} + \ldots + a_1 B + a_0$ *com* $a_0, a_1, \ldots, a_k \in 0, 1, \ldots, B-1$ *e* $a_k \neq 0$.

A k-sequência $a_k a_{k-1} \ldots a_1 a_0$ *é a sequência de algarismos que representa o número n na base B e escreve-se* $n = (a_k a_{k-1} \ldots a_0)_B$.

Dem. Dado um número natural $B > 1$ a sucessão $B^0 = 1 < B^1 = B < B^2 < B^3 < \cdots < B^k < B^{k+1} < \ldots$ é estritamente crescente e qualquer que seja o número natural $n \in N$ existe um único $k \in \mathbb{N}_0$ tal que $B^k \leq n < B^{k+1} = B.B^k$. Pelo Teorema da divisão com resto temos então $n = a_k B^k + r$ com $a_k \neq 0, a_k \leq B-1$ e $0 \leq r \leq B^k - 1$.

A demonstração do Teorema 2 continua utilizando o mesmo argumento em relação a r etc... (ou por indição em $k \in \mathbb{N}_0$).

Nota Quando nos referimos a um número sem especificar a base estamos a usar notação decimal (base 10).

Exemplo 1. Escreva na base 10 o número $(551)_8$.

Resposta $(551)_8 = 5 \times 8^2 + 5 \times 8 + 1 = 320 + 40 + 1 = 361$.

Exemplo 2. Verifique que 352 se escreve 1012 na base 7 e que em notação binária (base 2) se escreve 101100000, isto é: $352 = (1012)_7 = (101100000)_2$.

O próximo Corolário do Teorema 2 relaciona o número de algarismos de um número escrito numa base B e o logaritmo do número na mesma base.

Corolário 1 (Logaritmo e número de algarismos numa base B):

Dados $n, B \in \mathbb{N}$, $B > 1$ verifica-se a igualdade:

n^o de algarismos de n na base $B = \lfloor log_B(n) \rfloor + 1$.

Dem. directa do Teorema 2 e da definição de logaritmo numa base (justifique).

Teorema 3 (Representação decimal de números racionais)

Qualquer número racional é representado por um dízima finita ou infinita periódica.

Dem. Feita nas aulas práticas (Exercícios II-7,8,9). O ponto essencial do argumento é reparar que quando reduzimos uma fração $\frac{p}{q}$ à dízima, ou aparece o resto zero, e a dízima neste caso é finita, ou os restos que aparecem pertencem ao conjunto finito $\{1, 2, \ldots, q-1\}$. Neste caso quando acrescentamos casas decimais, no máximo ao fim de $(q-1)$ passos, teremos uma repetição de restos e portanto uma dízima periódica (com período $\leq (q-1)$).

2. Divisibilidade. Algoritmo de Euclides

Definições 1. Dados dois números inteiros $a, b \in Z$ diz-se que a divide b ou a é um divisor de b se $b = aq$ para algum $q \in \mathbb{Z}$. Escreve-se neste caso $a|b$.

Notação: $a|b$ lê-se " a divide b" ou " a é um divisor de b ou "b é um múltiplo de a" ou "b é divisível por a".

$a \not| b$ lê-se "a não divide b.

$Div(a)$ - denota o conjunto de todos os divisores inteiros de a. Verifica-se sempre a inclusão: $\{-1, 1, a, -a\} \subseteq Div(a)$.

$Div^+(a)$ - o conjunto dos divisores naturais de a. Tem-se sempre $\{1, a\} \subseteq Div^+(a)$.

$a\mathbb{Z}$ - o conjunto dos múltiplos inteiros de a.

Definição 2. Um número primo é um número natural p, maior do que 1 e cujos únicos divisores naturais são 1 e p, i.e. $Div^+(p) = \{1, p\}$ e $Div(p) = \{\pm 1, \pm p\}$.

Proposição 1 *Qualquer número natural $n > 1$ tem um divisor primo.*

Dem. Seja n um número natural maior do que 1. Se n é primo está demonstrado. Se n não é primo tem um divisor próprio $1 < d_1 < n$. Se d_1 é primo está demonstrado. Se d_1 não é primo d_1, e portanto n (justifique), tem um divisor próprio d_2: $1 < d_2 < d_1 < n$. Ou d_2 é primo e encontrámos um divisor ou não e o processo continua. Como o conjunto dos números menores do que n é finito a sucessão de divisores próprios de n, no caso de n não primo: $d_1 > d_2 > d_3 > ... > d_p > 1$ tem certamente um termo mais pequeno (mínimo) d_p que tem de ser um número primo.

Observações 1. Como consequência directa da Proposição 1 qualquer número natural se escreve como produto de factores primos. Deduza-o aqui. (Provaremos mais tarde)

2) Dado um número natural (ou inteiro) $n \in \mathbb{N}$ se o "número for pequeno" é fácil determinar o conjunto, $Div^+(n)$, dos seus divisores naturais. Se n for um "número muito grande " não é fácil saber se o número dado tem algum divisor, isto é se o número é ou não primo, e portanto não é fácil determinar o conjunto $Div^+(n)$.

Apesar desta obervação existe, como veremos a seguir, um processo eficaz de determinar o elemento máximo de $Div^+(a) \cap Div^+(b)$, $a, b \in \mathbb{N}$ $(ou\ a, b \in \mathbb{Z})$, isto é de calcular o máximo divisor comum de dois inteiros dados. Recorde-

mos que:

Definição 3. O máximo divisor comum de dois números naturais(ou inteiros) a e b, $mdc(a,b)$, é o maior dos divisores comuns a a e a b (isto é, o elemento máximo de $Div^+(a) \cap Div^+(b)$.)

Teorema 3 (Euclides) *Sejam* $a, b \in \mathbb{N}$, $a \leq b$. *Se* $b = aq + r$, $q, r \in \mathbb{N}$ *e* $0 \leq r < a$ *então:*

(i) Se $r = 0$ $mdc(a,b) = a$

(ii) Se $r \neq 0$ $mdc(a,b) = mdc(r,a)$.

Dem. O caso $r = 0$ é imediato. Consideremos pois o caso $r \neq 0$, i.e. $b = aq + r,\ 1 \leq r < a$.

Mostramos que $c \in \mathbb{N}$ é divisor comum a a e b se e só se c é um divisor comum a a e r isto é: $Div(a) \cap Div(b) = Div(a) \cap Div(r)$.

Seja $c \in Div(a) \cap Div(b)$ então $a = ca'$ e $b = cb'$. Como $0 < r = b - aq$ vem $r = cb' - ca'q = c(b' - a'q)$ e $b' - a'q \in \mathbb{Z}$ pelo que $c \in Div(r)$ e portanto $c \in Div(a) \cap Div(r)$.

Seja $c \in Div(a) \cap Div(r)$ então $a = ca'$ e $r = cr'$. Como $b = aq + r$ vem $b = c(a'q + r')$ e $a'q + r \in \mathbb{Z}$ pelo que $c \in Div(b)$ e portanto $c \in Div(a) \cap Div(b)$.

Algoritmo de Euclides para o cálculo de $mdc(a,b)$

Consiste em utilizar o Teorema 3 para calcular $mdc(a,b)$.

Exemplo 1. Calcular $mdc(438, 189)$

Passo 1) $438 = 189 \times 2 + 60$ portanto, pelo Teorema 3:

$mdc(438, 189) = mdc(189, 60)$

Passo 2) $189 = 60 \times 3 + 9$ portanto, pelo Teorema 3:

$mdc(438, 189) = mdc(189, 60) = mdc(60, 9)$

Passo 3) $60 = 9 \times 6 + 6$

$mdc(438, 189) = mdc(189, 60) = mdc(60, 9) = mdc(9, 6)$

Passo 4) $9 = 6 \times 1 + 3$

$\mathbf{mdc(438, 189)} = mdc(189, 60) = mdc(60, 9) = mdc(9, 6) = mdc(6, 3) = \mathbf{3}$

Uma consequência importante do Algoritmo de Euclides:

Teorema 4 Combinações lineraes inteiras de dois naturais

Dados $a, b \in \mathbb{N}$ seja $d := mdc(a, b)$. Então:

(1) Existem números inteiros $m, n \in \mathbb{Z}$ tais que $d = ma + nb$ (i.e. d é uma combinação linear inteira de a e b).

(2) Se $c \in \mathbb{Z}$ e existem $x, y \in \mathbb{Z}$ tais que $c = xa + yb$ então $d|c$.

Dem. A demonstração de (1) é uma consequência do Algoritmo de Euclides. veremos com o exemplo acima.

A demonstração de (2): seja $d = mdc(a, b)$. Por definição de divisor comum $a = da'$ e $b = db'$, $a', b' \in \mathbb{N}$. Por (1) $d = ma + nb$ com $m, n \in \mathbb{Z}$. Seja $c = xa + yb$ temos $c = xa'd + yb'd = (xa' + yb')d$ com $xa' + yb' \in \mathbb{Z}$, i.e. $d|c$.

Exercício. Vimos no Exemplo 1 que $mdc(438, 189) = 3$. Utilizamos os passos do Algoritmo de Euclides do Exemplo 1 para determinar $m, n \in \mathbb{Z}$ tais que $3 = m \times 438 + n \times 189$. Começamos do Passo 4) para o Passo 1) do Exemplo 1.

Passo 4) $3 = 9 - 6$

Passo 3) $6 = 60 - 9 \times 6$, portanto $3 = 9 - (60 - 9 \times 6) = -60 + 9 \times 7$.

Passo 2) $9 = 189 - 60 \times 3$, portanto $3 = -60 + (189 - 60 \times 3) \times 7 = 189 \times 7 - 60 \times 22$

Passo 1) $60 = 438 - 189 \times 2$ e $3 = 189 \times 7 - (438 - 189 \times 2) \times 22 = 438 \times (-22) + 189 \times 51$.

Resposta: Valores possíveis satisfazendo a igualdade pedida: $m = -22$ e $n = 51$.

Proposição 2. *Sejam $a, b \in \mathbb{N}$ e $d := mdc(a, b)$. Se $(x_0, y_0) \in \mathbb{Z}^2$ satisfaz a igualdade*

$$(*) \quad ax_0 + by_0 = d$$

então (todos) os pares $(x, y) \in \mathbb{Z}^2$ que satisfazem a igualdade $(*)$ são os pares da forma $(x, y) = (x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t), \quad t \in \mathbb{Z}$.

Dem. Exercício da prática.

Definição 4. Dois números naturais $a, b \in \mathbb{N}$ dizem-se números primos entre si ou números relativamente primos se $mdc(a, b) = 1$.

3. Teorema Fudamental da Aritmética

Teorema 5 (Factorização em números primos - Teorema Fundamental da Aritmética)

Qualquer número natural $n \in \mathbb{N}$ escreve-se, de modo único, a menos de reordenação dos factores, como produto de números primos.

Dem. A demonstração deste Teorema é uma consequência da Proposição 1 , que garante que qualquer número natural se decompõe num produto de primos e do próximo Lema 1 que garante a unicidade da decomposição em factores primos.

Lema 1 *Sejam $a, b \in \mathbb{N}$ e p um número primo tal que $p|ab$. Então $p|a$ ou $p|b$.*

dem. do lema 1. Vamos supor que p não divide a e mostrar que então p divide b.

Se $p \not| a$ então $mdc(p, a) = 1$. Pelo Teorema 4 sabemos que existem $m, n \in \mathbb{Z}$ tais que $1 = ma + np$ e $b = mab + npb$. Por hipótese $p|ab$, portanto $p|mab \;\; e \;\; p|npb$ portanto $p|b$.

Exercício 1. Recordar o cálculo de $mdc(a, b)$ e o $mmc(a, b)$ a partir da decomposição de a e b em factores primos.

Exercício 2. Mostrar que $\forall a, b \in \mathbb{N} \;\; a \times b = mdc(a, b) \times mmc(a, b)$.

4. Resultados fundamentais e conjecturas sobre números primos

Proposição 3

(1) Se $p \in \mathbb{N}$ é um número primo então $\sqrt{p}$ é um número irracional.

(2) Se um número natural n não é um quadrado perfeito então $\sqrt{n}$ é um número irracional.

Dem. (1) Seja p primo e suponhamos que $\sqrt{p}$ é um número racional, isto é, $\sqrt{p} = \frac{m}{n}, \quad mdc(m,n) = 1$.

De $(\sqrt{p})^2 = \frac{m^2}{n^2} \iff pn^2 = m^2$ deduzimos que $p|m^2$. Como p é primo, pelo Lema 1, $p|m$ e $m = pm_1, \ m_1 \in \mathbb{N}$ e $m^2 = p^2 m_1^2$. Substituindo em $pn^2 = m^2$ vem $n^2 = pm_1^2$ e concluímos, com argumento análogo ao anterior, que p tambem divide n, o que contraria a hipótese de que $mdc(m,n) = 1$.

(2) deduz-se de (1) e fica como exercício.

Teorema 6

Há infinitos números primos.

Dem. Suponhamos que havia um número finito de número primos: $p_1, \ldots, p_n$. Considere-se o número $N = p_1 \times p_1 \times \ldots \times p_n + 1$. O resto da divisão de N por qualquer número primo $p_1, \ldots, p_n$ é 1 portanto N não teria nenhum divisor primo, contrariando a Proposição 1 (e tambem o Teorema Fundamental da Aritmética).

Os próximos resultados e conjecturas mostram aspectos de como se distribuem os númerso primos entre os naturais.

O **Teorema dos números primos**, conjecturado independentemente por Legendre e Gauss nos finais do século XVIII e provado por Hadamard e de la Vallée Poussin um século depois, permite estimar a probabilidade de encontrar um número primo em determinado intervalo $[m,n]$.

A **Conjectura dos primos gémeos** e o recente **Teorema das progressões**

aritméticas de primos de B. Green e T. Tao (2004) dizem respeito a sequências de primos regularmente espaçados.

A próxima proposição diz que há pares de primos consecutivos tão distantes quanto queiramos.

Proposição 4

Qualquer que seja $n \in \mathbb{N}$ *existem dois númerso primos consecutivos* $p_1 < p_2$ *tais que* $p_2 - p_1 > n$.

Dem. Os números $N_1 = (n+1)! + 2, \ldots, N_n = (n+1)! + (n+1)$ são números compostos (não são primos). Sendo p_1 :=*maior primo menor do que* $(n+1)!+2$. Entre p_1 e o número primo seguinte, p_2, estão os n-números compostos $N_1, \ldots, N_n$, pelo que $p_2 - p_1 > n$.

Todos os números primos são impares, por isso, a menor "distância" entre dois números primos é 2. Um par de primos gémeos é um par de dois números primos consecutivos da forma $(p, p+2)$. Exemplos: $(3,5)$, $(5,7)$, $(11,13)$... A conjectura dos números primos diz que há infinitos pares de primos cnsecutivos à distância mínima:

Conjectura dos primos gémeos: *Existem infinitos pares de primos gémeos.*

Teorema das sequências de progressãoes aritmt́icas de números primos (resultado difcil B. Green, T.Tao - *Annals of Maths* 2008))

Os números primos contem infinitas progressões aritméticas de comprimento k *qualquer que seja o* k.

O próximo Teorema trata a probabilidade de encontrar um primo em determinado intervalo finito.

Teorema dos números primos(resultado difícil - Hadamard, de la Vallé-Poussin sec.XIX)

Para cada $n \in \mathbb{N}$ *define-se* $\pi(n) := n^o$ *de números primos* $\leq n$. *Tem-se* $\pi(n) \simeq \frac{n}{ln\ n}$

Exercício. Como aplicação do Teorema dos números primos estime quantos números primos há com 100 algarismos.

Terminamos esta breve introdução aos mistérios dos números primos enunciando uma segunda conjectura (ainda não demonstrada):

Conjectura de Goldbach *Qualquer número par escreve-se como soma de dois múmeros primos.*

Exemplos: $4 = 2 + 2,\ 6 = 3 + 3,\ 8 = 3 + 5,\ 10 = 3 + 7,\ 12 = 5 + 7$...

5. Congruências - Aritmética modular

Definição 5. Dois números $a, b \in \mathbb{Z}$ dizem-se *congruentes módulo* n, $n \in \mathbb{N}$, e escreve-se $a \equiv b \ (mod\ n)$ se (e só se) $n|(a-b)$.

Nota. Dizer que n divide $(a-b)$ é equivalente a dizer $(a-b)$ é múltiplo de n, i.e. $n|(a-b) \iff a-b \in n\mathbb{Z}$ ou ainda que a e b *têm o mesmo resto na divisão por* n (justifique).

Proposição 5. *Qualquer que seja* $n \in \mathbb{N}$ *a relação de congruência módulo* n *em* $\mathbb{Z}$ *tem as seguintes propriedades:*

1) É uma relação de equivalência em $\mathbb{Z}$, *i.e.,*

é reflexiva: $\forall a \in \mathbb{Z}, \quad a \equiv a(mod\ n)$,

'e simétrica: $\forall a, b \in \mathbb{Z} \quad a \equiv b(mod\ n) \Longrightarrow b \equiv a(mod\ n))$

é transitiva: $\forall a, b, c \in \mathbb{Z} \quad a \equiv b(mod\ n)\ e\ b \equiv c(mod\ n) \Longrightarrow a \equiv c(mod\ n))$

2) Dado um número inteiro $a \in \mathbb{Z}$ *a classe de equivalência de* a *(para a relação de congruência módulo* n*) denota-se* $\overline{a}$ *e é, por definição, o conjunto de todos os inteiros que são congruentes com* a *módulo* n. *Temos pois:*

$$\overline{a} := \{z \in \mathbb{Z} : \ z \equiv a(mod\ n)\} = \{z = a + nx : \ x \in \mathbb{Z}\} = a + n\mathbb{Z}$$

3) O conjunto das classes de congruência módulo n *(conjunto quociente de* $\mathbb{Z}$ *pela relação de equivalência* $\equiv (modn))$ *denota-se* $\mathbb{Z}/n\mathbb{Z}$ *ou* $\mathbb{Z}_n$ *e tem exactamente* n *elementos, as classes de equivalência dos restos das divisões por* n*:*

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

.

Dem. 1) e 2) Exercícios (feitos na aula).

3) Repare que $\overline{a} = \overline{b}$ se e só se $a \equiv b(mod\ n)$ (prove).

Como $a \equiv b(modn)$ se e só se a e b têm o mesmo resto $0 \leq r \leq n-1$, temos $\overline{a} = \overline{b} = \overline{r}$ e por isso podemos tomar como representantes das diferentes classes de congruência módulo n os restos da divisão por n escrevendo:

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

Proposição 6 (compatibilidade das operações em $\mathbb{Z}_n$ com a relação $\equiv (mod\ n)$)

Qualquer que seja $n \in N$, $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ *verificam-se as seguintes propriedades:*

1) Se $a_1 \equiv a_2 (mod\ n)$ *e* $b_1 \equiv b_2 (mod\ n)$ *então:*

$$a_1 + b_1 \equiv a_2 + b_2 (mod\ n) \quad e \quad portanto\ \overline{a_1 + b_1} = \overline{a_2 + b_2}$$

$$a_1.b_1 \equiv a_2.b_2 (mod\ n)\ e \quad portanto\ \overline{a_1.b_1} = \overline{a_2.b_2}$$

2) em particular, $\forall k \in \mathbb{N}$*:*

$$(a) \quad ka_1 \equiv ka_2 (mod\ n) \quad e \quad (b) \quad a_1^k \equiv a_2^k (mod\ n).$$

Definição 6. Soma e Multiplicação em $\mathbb{Z}_n$.

A soma e a multiplicação de números inteiros permitem definir (induzem) as operações de soma e multiplicação em $\mathbb{Z}_n$, definidas por:

Soma em Z_n: $\overline{a} + \overline{b} = \overline{a + b}$

Multiplicação em Z_n: $\overline{a}.\overline{b} = \overline{a.b}$

Nota. Como $\mathbb{Z}_n$ é finito podemos definir a soma e multiplicação de $\mathbb{Z}_n$ por tabelas. Exemplo feito na aula: Tabelas da soma e multiplicação de $\mathbb{Z}_2$ e $\mathbb{Z}_3$.

Exercćio para casa: Construa as tabelas de soma e multiplicação de $\mathbb{Z}_4$ e de $\mathbb{Z}_5$.

Nos próximos 2 parágrafos damos duas aplicações da Proposição 6: a primeira ao cálculo de potências de expoente natural em $\mathbb{Z}_n$, a segunda à obtenção de critérios de divisibilidade.

1) Como calcular potências de expoente natural em Z_n

Exemplo: Em Z_{20} determine $\overline{3}^{541}$:

Por definição $\overline{3}^{541} = \overline{r}$ onde $r :=$*resto da divisão de* 3^{541} *por* 20.

$3^3 = 27 \equiv 7(mod\ 20)$ e $541 = 3.180 + 1$ portanto, pela Proposição 6

$3^{541} = (3^3)^{180}.3 \equiv 7^{180}.3(mod\ 20)$.

$7^2 = 49 \equiv 9(mod\ 20)$ e $180 = 2.90$ portanto, pela Proposição 6:

$7^{180}.3 \equiv 9^{90}.3(mod\ 20)$

$9^2 = 81 \equiv 1(mod\ 20)$ e $90 = 2.45$ portanto, pela Proposição 6:

$9^{90}.3 \equiv 1^{45}.3 = 3(mod\ 20)$.

Como escrevemos normalmente estes cálculos:

$3^{541} = (3^3)^{180}.3 = 7^{180}.3 = (7^2)^{90}.3 = 9^{90}.3 = (9^2)^{45}.3 = 1^{45}.3 = 3(mod\ 20)$.

Resposta: Em Z_{20}, $\overline{3}^{541} = \overline{3}$

2) Critérios de divisibilidade

Pela Proposição 6 sabemos que se $a \equiv -1(mod\ b)$, resp. $a \equiv -1(mod\ b$ ou $a \equiv 0(mod\ b$, temos $a^k \equiv 1(mod\ b)$, resp. $a^k \equiv (-1)^k(mod\ b)$ ou $a^k \equiv 0(mod\ b$. Este facto permite estabelecer critérios de divisibilidade. Por exemplo (ver outros exemplos no Exercício 32)

Critério de divisibilidade por 3: *Um número natural (ou inteiro) é divisível por 3 se e só se a soma dos seus algarismos é divisível por 3.*

Seja $n = a_k \ldots a_0$ um número natural cujos algarismos são $a_k, \ldots, a_1, a_0,\ a_k \neq 0,\ a_i \in \{0, 1, \ldots, 9\}$. Por definição da notação decimal (base 10) temos:

$n = a_k 10^k + a_{k-1}10^{k-1} + \ldots + a_1 10 + a_0$. Pretendemos estudar quando é que n é múltiplo de 3 ou seja quando é que $n \equiv 0(mod 3)$ (equivalente a $\overline{n} = \overline{0}$ módulo 3.).

Pela Proposição 6, como $10 \equiv 1(mod 3)$ temos $10^i \equiv 1(mod\ 3), \forall i \in \mathbb{N}$ e portanto:

$(*)\ \ n = a_k 10^k + a_{k-1}10^{k-1} + \ldots + a_1 10 + a_0 \equiv a_k + a_{k-1} + \ldots a_1 + a_0(mod\ 3)$

Desta última igualdade concluímos que a classe de congruência módulo 3 de n á a mesma que a classe de congruência da soma dos seus algarismos. Em particular, $n \equiv 0(mod\ 3) \iff a_k + \ldots + a_1 + a_0 \equiv 0(mod\ 3)$ o que justifica

o critério de divisibilidade.

Notas: 1) De (*) concluímos nao só o critério de divisibilidade enunciado mas, mais geralmente que: o resto da divisão de um número natural (inteiro) por 3 é igual ao resto da divisão da soma dos seus algarismos por 3.

Exemplo: O resto da divisão de 3269 por 3 = resto da divisão de 3+2+6+9 = 20 por 3 = 2.

2) O critério de divisibilidade depende da base em que está escrito o número (não explicitando considera-se a base usual, base 10).

Exemplo: Qual o critério de divisibilidade por 3 de um número natural escrito na base 3? (Resposta: o último algarismo ser 0. Justifique!)

6. Estruturas algébricas importantes: Grupo Comutativo, Corpo

Grupo comutativo ou abeliano é um par $G = (G, *)$ constituido por um conjunto G munido de uma operação binária $\begin{array}{rccc} * : & G \times G & \longrightarrow & G \\ & (a, b) & \longrightarrow & a * b \end{array}$ que satisfaz as seguintes propriedades:

(* é comutativa) $a * b = b * a$

(* é associativa) $(a * b) * c = a * (b * c)$

(* possui elemento neutro) Existe um (único) $e \in G$ tal que $\forall a \in G,\ a * e = e * a = a$

(Todos os elementos têm um inverso) $\forall a \in G$ existe (um único) $a^{-1} \in G$ tal que $a * a^{-1} = a^{-1}a = e$.

Exemplos de grupos comutativos: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q} \setminus \{0\}, \times)$, $(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \times)$, $(\mathbb{C}, +)$, $(\mathbb{C} \setminus \{0\}, \times)$, $(\mathcal{M}_{m\times n}(\mathbb{R}), +)$ onde $\mathcal{M}_{m\times n}(\mathbb{R})$ é o conjunto da matrizes reais $m \times n$.

Notação aditiva: Se a operação $*$ se chamar soma (adição) o elemento neutro designa-se por 0 e o inverso de um elemento a designa-se por simétrico de a e escreve-se, $-a$ em vez de a^{-1}.

Há grupos não comutativos (Ex: grupo das matrizes invertíveis $n \times n$ com a multiplicação, grupo das isometrias do plano (ou de $\mathbb{R}^n$), grupo das simetrias de uma figura.)

Corpo é um triplo $K = (K, +, \times)$ em que K é um conjunto munido de duas operações binárias: $+$ (soma) e $\times$ (multiplicação e que satisfaz as seguintes propriedades:

1) $(K, +)$ é um grupo comutativo.

2) $(K \setminus \{0\}, \times)$ é um grupo comutativo (0 é o elemento neutro da soma).

3) Distributividade da multiplicação em relação à soma:

$$\forall a, b, c \in K \quad a \times (b + c) = (a \times b) + (a \times c)$$

Exemplos: $(\mathbb{Q}, +, \times)$ - corpo dos racionais, $(\mathbb{R}, +, \times)$- corpo dos reais, $(\mathbb{C}, +\times)$ corpo dos complexos.

Nota: Se K é um corpo K^n é um **espaço vectorial** de dimensão n (Álgebra linear!).

Questão 1: *$\mathbb{Z}_n$ é sempre um corpo? Existem $n \in \mathbb{N}$ para os quais $\mathbb{Z}_n$ seja um corpo? Se sim quais?*

7. Propriedades da soma e da multiplicação em Z_n

Proposição 7 (Propriedades da soma de $\mathbb{Z}_n$) *$\forall n \in \mathbb{N}$, $(\mathbb{Z}_n, +)$ é um grupo comutativo.*

Proposição 8 (Propriedades da multiplicação de $\mathbb{Z}_n$)

$\forall n \in \mathbb{N}$ a multiplicação $. : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ goza das seguintes propriedades: é comutativa, é associativa e existe elemento neutro $\overline{1}$.

Mais, a multiplicação é distributiva em relação à soma.

Exercício. Demonstrar as Proposições 7 e 8.

Nota: Com base nas proposições anteriores, $\forall n \in \mathbb{N}$, $\mathbb{Z}_n$ é um bom candidato a corpo, contudo, a existência de inversos para a multiplicação pode falhar! e ... falha!

Exemplo 1. *Em* $\mathbb{Z}_6$*,* $\overline{4}$ *não tem inverso!*, portanto $\mathbb{Z}_6$ não é um corpo.

Com efeito, suponhamos que $\overline{4}$ tem inverso $\overline{x} \in \mathbb{Z}_n$. Teríamos então $\overline{4x} = \overline{1}$, i.e. $4x \equiv 1(mod\ 6)$. O que é equivalente a dizer existe $y \in \mathbb{Z}$ tal que $4x + 6y = 1$. Pelo Teorema de Euclides sabemos que, como $mdc(4, 6) = 2$ e $2 \not| 1$, é impossível escrever 1 como combinaç ao linear inteira de 4 e 6 e portanto 4 não tem inverso em $\mathbf{Z_6}$.

Como acabamos de ver no exemplo anterior, verificar se um elemento $\overline{a} \in \mathbf{Z_n}$ tem ou não inverso en $\mathbf{Z_n}$ consiste em resolver a equação linear na variável $\overline{x}$:

$$\overline{ax} = \overline{1} \tag{1}$$

Esta equação é equivalente, por definição de classe de congruência módulo n, à seguinte equação:

$$ax \equiv 1\ (mod\ n) \tag{1'}$$

Esta última equação, por definição de congruência módulo n, tem solução se e só se:

$$existem\ \ x, \in \mathbb{Z}\ tais\ que\ \ ax + ny = 1. \tag{1''}$$

Pelo Teorema de Euclides $(1'')$ tem solução se e só se $mdc(a, n) = 1$, isto é *os elementos* $\overline{a}$ *de* $\mathbb{Z}_n$ *que têm inverso são aqueles que são relativamente primos com* n*.*

Podemos pois enunciar a seguinte proposição:

Proposição 9 (existência de inversos em $\mathbb{Z}_n$) *Um elemento $\overline{a} \in \mathbb{Z}_n$ tem inverso em $\mathbb{Z}_n$ (ou é invertível em $\mathbb{Z}_n$ se e só se $mdc(a,n) = 1$ (a e n são primos entre si ou relativamente primos). Alem disso,*

Se $mdc(a,n) = 1$ sendo $x, y \in Z$ tais que $ax + ny = 1$ o inverso $\overline{a}^{-1}$ de a em $\mathbb{Z}_n$ é definido por $\overline{a}^{-1} = \overline{x}$.

Nota: A última afirmação da proposição anterior diz, em particular, que calcular o inverso de um elemento em $\mathbb{Z}_n$ se resume a utilizar o ALGORITMO DE EUCLIDES ! (Veremos no capítulo 8 um outro processo).

Exemplo 2. *Quais os elementos invertíveis de* $\mathbf{Z_6}$*?*

Temos $\mathbf{Z_6} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. Pela Proposição 9 os elementos invertíveis são os elementos $\overline{a}$ tais que $mdc(a,n) = 1$ e portanto apenas $\overline{1}$ e $\overline{5}$ têm inverso.

Repare que em ambos os casos o inverso é o próprio elemento: $\overline{1}.\overline{1} = \overline{1}$ e $\overline{5}.\overline{5} = \overline{1}$.

Dos resultados anteriores sai como Corolário o seguinte Teorema, que responde completamente à **Questão 1**:

Teorema 7. $\mathbf{Z_n}$ *é um corpo se e só se n é um número primo.*

Dem. Sabemos já que a única propriedade das operações de $\mathbf{Z_n}$ que pode falhar para garantir que $\mathbf{Z_n}$ seja um corpo é a existência de inversos para a multiplicação.

Se n for um número primo então qualquer elemento não nulo $\overline{a} \in \mathbf{Z_n}$ satisfaz a condição $mdc(a,n) = 1$ e, pela Proposição 9, é invertível, portanto $\mathbb{Z}_n$ é um corpo. *Se n não for um número primo* então $n = n_1.n_2$, com $n_1, n_2 > 1$. Neste caso $\overline{n_1} \in \mathbf{Z_n}$ não tem inverso pois $mdc(n_1, n) = n_1 > 1$. □

O estudo da existência de inverso de um elemento de $\mathbf{Z_n}$ é um caso particular do estudo de equações lineares numa variável em $\mathbf{Z_n}$, isto é de equações do tipo : $\overline{a}\overline{x} = \overline{b}$. Tendo-se o seguinte resultado geral:

Teorema *Sejam* $a, b \in \mathbf{Z_n}$ *e a equação:*

(E) $\qquad\qquad\qquad\qquad\qquad\qquad \overline{a}.\overline{x} = \overline{b}$

1) Se $mdc(a,n) \not| b$ *a equação* (E) *não tem solução.*

2) Se $mdc(a,n)|b$ *a equação* (E) *tem exactamente* d *soluções* $(mod\ n)$

Em particular, qualquer elemento invertível de $\mathbf{Z_n}$ *tem umúnico inverso.*

Dem. Exercicios 36 e 37.

Nota. Tudo o que deram em álgebra linear relativo a matrizes, sistemas de equações lineares aplica-se a matrizes com entradas em $\mathbb{Z}_p$, *p primo* sistemas, com variáveis em $\mathbb{Z}_p$, aplicações lineares etc... aos espaços vectoriais FINITOS $\mathbb{Z}_p^n$. Veja os exercícios 44 e 45.

8. Função de Euler e Teorema de Euler

Definição 7. (Função de Euler -$\Phi(n)$)

A função de Euler é a função $\Phi : \mathbb{N} \longrightarrow \mathbb{N}$ que a cada número natural $\mathbb{N}$ faz corresponder $\Phi(n) :=$ *o número de números relativamente primos com* n *e menores do que* n:

$$\Phi(n) := \mid \{a \in \mathbb{N} :\ a \leq n \text{ e } mdc(a,n) = 1\} \mid$$

Nota. Pela Proposição 9, $\Phi(n)$ é precisamente o n^o de elementos invertíveis de $\mathbb{Z}_n$. A Póxima proposição diz-nos como calcular $\Phi(n)$ a partir da factorização em números primos de n.

Proposição 10 (Cálculo de $\Phi(n)$)

Se n é um número natural, cuja decomposição em factores primos é da forma: $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, $\alpha_i \in \mathbb{N}$ então:

$$\Phi(n) = n\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right).$$

Dem. Ver exercício 49.

O próximo teorema, essencial para o sistema de criptografia RSA, dá um método alternativo ao algoritmo de Euclides para determinar o inverso de um elemento em $\mathbb{Z}_n$:

Teorema 8 (Teorema de Euler) *Se $a \in \mathbb{Z}$ é um número relativamente primo com n, i.e. $mdc(a, n) = 1$, então:*

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

Passos principais da demonstração:

Consideremos $S = \{s_1, \dots, s_m\}$ o conjunto de todos os números menores do que n e relativamente primos com n. Claro que $m = \Phi(n)$.

Seja $a \in S$ e multipliquemos a por todos os números de S obtendo:

$s_1 a,\ s_2 a,\ s_3 a, \dots,\ s_m a.$

1) Reparemos que: $\forall i = 1, \dots, m \quad mdc(s_i a, n) = 1$ e $s_i a = s_j a (mod\ n)$ se e só se $s_i = s_j (mod\ n)$ visto que como $mdc(a, n) = 1$, $n | (s_i - s_j)a$ se e só se $n | (s_i - s_j)$.

2) Consideremos o produto $P = (s_1 a)(s_2 a) \dots (s_m a)$

Por um lado: $P = (s_1 s_2 \dots s_m) a^m$,

por outro lado, 1) implica que $P \equiv s_1 s_2 \dots s_m (mod\ n)$.

Portanto,

$(s_1 s_2 \dots s_m) a^m \equiv s_1 s_2 \dots s_m (mod\ n) \iff n \mid (s_1 s_2 \dots s_m)(a^m - 1)$

Como $mdc(s_i, n) = 1$, teremos de ter $n|(a^m - 1) \iff a^m \equiv 1(mod\ n)$. Como $m := \Phi(n)$ o resultado está demonstrado.

O Corolário A que se segue, é obtido do Teorema de Euler aplicado ao caso particular em que n é um número primo $n = p$ (e $\Phi(p) = p-1$). É conhecido por Pequeno Teorema de Fermat:

Corolário A (Pequeno Teorema de Fermat) *Seja $p \in \mathbb{N}$ um número primo. Então $\forall a \in \mathbb{Z},\ a \not\equiv 0(mod\ p)$:*

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

Os exercícios 42) e 43) propõe uma demonstração alternativa para o Pequeno teorema de Fermat.

O próximo Corolário B estende o Teorema de Euler no caso em que n é o produto de dois números primos e será usado no próximo parágrafo.

Corolário B *Se $n \in \mathbb{N}$ é o produto de dois números primos $n = p_1p_2$ e $x \equiv 1(mod\ \Phi(n))$ então qualquer que seja $m \in \mathbb{N}_0,\ m < n$:*

$$(*) \qquad m^x \equiv m(modn).$$

Dem. Seja $m \in \mathbb{N},\ 0 \leq m < n$ e $x \equiv 1(mod\ \Phi(n) \iff x = \Phi(n)j + 1,\ com\ j \in \mathbb{Z}$

Se $m \equiv 0(mod\ n)$ claro que $m^x \equiv 0(mod\ n)$

Se $mdc(m, n) = 1$ $(*)$ pelo Teorema de Euler: $m^x = (m^{\Phi(n)})^j.m \equiv m(mod\, n)$.

Demonstramos agora o caso $mdc(m, n) = p_1\ ou\ p_2$, isto é: $m = p_1k$ com $k \in \{1, \ldots, p_2 - 1\}$, ou $m = p_2k$ com $k \in \{1, \ldots, p_1 - 1\}$. Consideramos apenas o primeiro caso, $m = p_1k$, o outro é análogo. Temos então:

$m^x = (p_1.k)^{\Phi(n).j}.p_1k = (p_2q + 1).p_1k \equiv p_1k(mod\ p_1p_2)$ o que prova $(*)$.

A segunda igualdade vem do facto de $mdc(p_1k, p_2) = 1$ e $\Phi(n) = (p_1 - 1)(p_2 - 1) = \Phi(p_1)\Phi(p_2)$, portanto, pelo Teorema de Euler $(p_1.k)^{\Phi(n).j} \equiv 1(mod\ p_2) \iff (p_1.k)^{\Phi(n).j} = p_2q + 1,\ com\ q \in \mathbb{Z}$.

9. Criptografia - o sistema RSA

Objectivo da Criptografia: Estabelecer um código que permita enviar mensagens entre duas partes de tal modo que se a mensagem for interceptada por terceiros estes não a consigam descodificar.

Sistemas de códigos bem conhecidos - **Cifra de César** e variações.

O **Sistema RSA** (Rivest-Shamir-Adleman 78) baseia-se na ideia de função armadilha - operação que é fácil de fazer mas difícil de desfazer.

Como funciona o sistema RSA:

1. O código: parte secreta e pública

Utilizadores (só eles): conhecem dois números primos p_1, p_2 (e.g. da ordem dos 100 dígitos cada um), calculam fácilmente:

$$n = p_1 p_2,\ \Phi(n) = (p_1 - 1)(p_2 - 1)$$

Escolhem um *expoente de encriptação* e : um número primo com $\Phi(n)$ i.e. tal que $mdc(e, \Phi(n)) = 1$ (p.exemplo e um número primo)

Podem tornar público: n e e.

Porque (até ao momento!...) não há nenhum processo eficaz de sabendo n (aprox. 200 dígitos) determinar a sua decomposição em factores primos em tempo útil.

2. Enviar e descodificar mensagens

Pode-se supor que qualquer mensagem é naturalmente (p. ex código ASCII) um número natural $m < n$ (mensagens maiores do que n são transmitidas em "bocados" menores do que n).

Utilizador 1. Quer enviar a mensagem $m,\ m < n$ para o Utilizador 2.

Envia a mensagem encriptada: $E(m) = m^e (mod\ n)$

Utilizador 2. Recebe $E(m)$ e descodifica-a ou desencripta-a usando o expoente de desencriptação d. O expoente de desencriptação d é um número

natural que satisfaz a congruência:

$$(m^e)^d \equiv m(mod\ n)$$

Pelo Corolário B do teorema de Euler basta escolher $ed \equiv 1(mod\ \Phi(n))$, ou seja determinar o inverso de $\overline{e}$ em $\mathbb{Z}_{\Phi(n)}$, o que se determina "rápidamente" usando o Algoritmo de Euclides.

Determinado d, recuperar a mensagem inicial m reduz-se a calcular o resto da potência $E(m)^d$ $(= (m^e)^d)$ por n.

Determinar uma potência módulo n é um problema simples mesmo para grandes números e grandes expoentes. O Utilizador 2 consegue pois descodificar rápidamente a mensagem. (Tal como o Utilizador 1 a conseguiu encriptar fácilmente).

Resolução dos Exercícios 24,25 ("miniaturas" de utilização do sistema RSA.)

10. Geometrias Finitas

Como $\mathbb{Z}_p$, *p primo* é um corpo, o produto cartesiano $\mathbb{Z}_p^n := \{(\overline{x_1}, \ldots, \overline{x_n}) : \overline{x_i} \in \mathbb{Z}_p\}$ é um espaço vectorial de dimensão n, com a soma e multiplicação por um escalar definidas a partir da soma e multiplicação de $\mathbb{Z}_p$:

$$(\overline{x_1}, \ldots, \overline{x_n}) + (\overline{y_1}, \ldots, \overline{y_n}) = (\overline{x_1} + \overline{y_1}, \ldots, \overline{x_n} + \overline{y_n})$$

$$\overline{\alpha}(\overline{x_1}, \ldots, \overline{x_n}) = (\overline{\alpha}.\overline{x_1}, \ldots, \overline{\alpha}.\overline{x_n}), \forall \overline{\alpha} \in \mathbb{Z}_p$$

$\mathbb{Z}_p^n$ é um espaço vectorial com p^n vectores.

Associado ao espaço vetorial $\mathbb{Z}_p^n$ está o espaço afim $\mathbb{Z}_p^n$ cujos pontos são também os n-uplos de elementos de $\mathbb{Z}_p$.

Tudo o que foi dado em Álgebra Linear sobre (in)dependência linear, nomeadamente, resolução e discussão de sistemas de equações lineares, subespaços vetoriais e afins - retas, planos , etc... - é válido para estes espaços vetoriais.

Neste parágrafo olhamos com algum cuidado para os planos afins $\mathbb{Z}_p^2$. Definimos o plano projectivo associado. E mostramos como o estudo destes objectos tem a ver com códigos detetores e corretores da teoria de informação.

Plano afim $\mathbb{Z}_p^2$

Os **pontos** do plano afim $\mathbb{Z}_p^2$ são os pares $\mathbf{x} = (x, y) \in \mathbb{Z}_p^2$.

As **retas** são os conjuntos de pontos de *equação vectorial*:

$$(V) \qquad (x, y) = (\overline{p_1}, \overline{p_2}) + \overline{\alpha}(\overline{u_1}, \overline{u_2}), \quad \overline{\alpha} \in \mathbb{Z}_p$$

onde $\mathbf{p} = (\overline{p_1}, \overline{p_2})$ é um ponto da reta e $\mathbf{u} = (\overline{u_1}, \overline{u_2}) \in \mathbb{Z}_p^2$, $\mathbf{u} \neq \mathbf{0}$ é um vetor diretor da reta. A equação cartesiana da reta definida pela equação (V) é, a menos de multiplicação por constante não nula, a equação:

$$(C) \qquad \overline{u_2}x - \overline{u_1}y = \overline{u_2}.\overline{p_1} - \overline{u_1}.\overline{p_2},$$

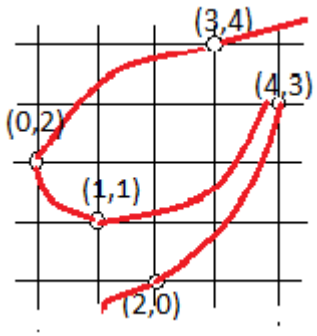
Exemplo. Na Figura está representado o plano afim $\mathbb{Z}_5^2$, os seus $5^2 = 25$ pontos e a reta r:

$$r: \quad \mathbf{x} = (\overline{2}, \overline{0}) + \lambda(\overline{2}, \overline{3}), \quad \lambda \in \mathbb{Z}_p$$

ou eqivalentemente a reta cuja equação cartesiana é

$$r: \quad \overline{3}x - \overline{2}y = \overline{1} \iff \overline{3}x + \overline{3}y = \overline{1}.$$

A reta r contem 5 pontos, como qualquer outra reta de $\mathbb{Z}_5^2$.



Duas retas do plano afim r, s são **paralelas** se têm os mesmos vetores diretores, isto é a mesma direção. Duas retas paralelas ou não têm pontos comuns ou têm todos os pontos em comum e, neste caso, são a mesma reta. Uma **classe de paralelismo** é o conjnto de todas as retas paralelas, com uma mesma direção.

Num plano afim, duas retas que não são paralelas têm um único ponto em comum e dizem-se **retas concorrentes**.

Proposição 1 (Retas do plano afim $\mathbb{Z}_p^2$)

As retas do plano afim $\mathbb{Z}_p^2$ têm as seguintes propriedades:

1) Qualquer reta contem p pontos do plano. Por esta razão $\mathbb{Z}_p^2$ é um **plano afim de ordem** *p.*

2) Cada classe de paralelismo contem exatamente p retas.

3) $\mathbb{Z}_p^2$ contem exatamente $(p+1)$ classes de retas paralelas.

4) O n^o de retas de $\mathbb{Z}_p^2 = p^2 + p$.

Dem. 1) Direto a partir da equação vetorial de uma reta.

2) Considere-se uma reta r de equação vetorial $\mathbf{r}: \quad \mathbf{x} = \mathbf{p} + \lambda\mathbf{u}, \quad \lambda \in \mathbb{Z}_p$.

Seja $\mathbf{v}$ um vetor linearmente independente de $\mathbf{u}$ e considere os pontos $\mathbf{p}_\alpha = \mathbf{p} + \alpha\mathbf{v},\ \alpha \in \mathbb{Z}_p$. As p retas $\mathbf{r}_\alpha :\quad \mathbf{x} = \mathbf{p}\alpha + \lambda\mathbf{u},\quad \alpha, \lambda \in \mathbb{Z}_p$ são diferentes e estão todas na classe de paralelismo de r. Como cada uma dessas retas tem p pontos, diferentes, as p retas paralelas a r contêm todos os p^2 pontos do plano pelo que são a totalidade de retas na classe de paralelismo de r.

3) Se uma reta tem vetor de direção $\mathbf{u}$ entã os $p-1$ múltiplos $\alpha\mathbf{u}, com\ \alpha \in \mathbb{Z}_p, \alpha \neq 0$ são vetores diretores da mesma reta. Há no total p^2-1 possíveis vetores diretores (o vetor nulo excluido). Cada um desses vetores tem $p-1$ múltiplos definindo a mesma direção, pelo que há $\frac{p^2-1}{p-1} = p+1$ direções diferentes e portanto $p+1$ classes de paralelismo.

4) O n^o de retas de $\mathbb{Z}_p^2$ = n^o de classes de paralelsimo $\times$ n^o de retas em cada classe $p = (p+1)p = p^2 + p$.

Plano projectivo $P\mathbb{Z}_p^2$, associado ao plano afim $\mathbb{Z}_p^2$

O plano projectivo $P\mathbb{Z}_p^2$ é o plano que se obtem ampliando o plano afim $\mathbb{Z}_p^2$ com :

- p+1 pontos, cada um deles "o ponto do infinito" de uma classe de retas paralelas e que pertence a todas elas em $P\mathbb{Z}_p^2$.

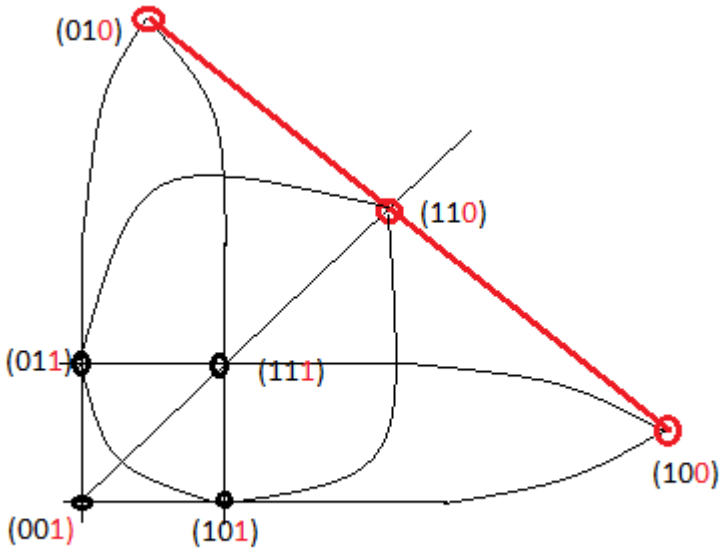
- uma reta $\mathbf{r}_\infty$ constituida pelos $p+1$ novos pontos.

Repare que $P\mathbb{Z}_p^2$ tem no total p^2+p+1 pontos e p^2+p+1 retas. Cada reta contem $p+1$ pontos e cada ponto está contido em $p+1$ retas e é por isso um plano projectivo de ordem p.

Exemplo. Plano de Fano - plano projectivo associado ao plano afim $\mathbb{Z}_2^2$.

Na figura seguinte representámos a preto os pontos e retas do plano afim $\mathbb{Z}_2^2$ e a vermelho a sua ampliação com a reta do infinito constituida pelos 3 pontos do infinito de classe de paralelismo.

.



Definição. (Plano projectivo de ordem n, $n \geq 2$)

É um par $\mathbf{P} = (\mathcal{P}, \mathcal{R})$, em que $\mathcal{P}$ é um conjunto, o conjunto dos **pontos** do plano projectivo, e $\mathcal{R}$ é uma família de subconjuntos de $\mathcal{P}$ satisfazendo as seguintes condições:

P1) Quaisquer dois pontos estão contidos numa e numa só reta.

P3) Qualquer par de retas distintas intersecta-se num único ponto.

P2) Qualquer reta contem exatamente $n + 1$ pontos.

P4) Qualquer ponto está contido em exatamete $n + 1$ retas.

Problema em aberto. Sabe-se que existem planos afins e projectivos de ordem p^k, potência de um primo p.

Para que outros $n \in \mathbb{N}, n \geq 3$, além desses existem planos afins ou projectivos dessa ordem?

Os primeiros valores para os quais podem eventualmente não existir planos

afins ou projectivos dessa ordem são pois: $6, 10$ e 12. Foi provado que não existem planos projectivos de ordem 6 (Tarry , 1901) nem de ordem 10 (Lam etal. 1980's) por via computacional. Mas não se sabe mais nada.

Planos afins e projectivos sobre corpos finitos generalizam-se a espaços afins e projectivos de dimensão mais elevada (ver exerc'ico 70) assim como a sistemas puramente combinatórios tais como os Sistemas de Steiner (ver exerccio 71).

O estudo destas geometrias finitas está intimamente relacionado com a estdo e escolha de códigos detectores e corretores de erros de Teoria da Informação que definem sistemas de sequências de $0's$ e $1's$ que permitam codificar de forma a conseguir detetar e até corrigir eventuais erros na transmisso de mensagens (sequencias de $0's$ e $1's$) atravs de canais com rudo.