1 Divisão de inteiros

Teorema 1.1 (Teorema de divisão de Euclides)**.**
Dados $n \in \mathbb{Z}$ *e* $d \in \mathbb{N}$, *existe uma única dupla* $q \in \mathbb{Z}$, $r \in \{0, ..., d-1\}$ *tal que*

$$n = qd + r$$

Dizemos que a **divisão entre inteiros** n/d tem **quociente q** e **resto r**, (**d** é dito **divisor**).

Em C, se n e d são integer (positivos), $q = n/d$, $r = n\%d$

Definição: Dados $n \in \mathbb{Z}$ e $d \in \mathbb{N}$, definimos **n modulo d:**

$$n \ (mod \ d) := r$$

sendo r o dado pelo teorema.
Para abreviar usaremos a notação $nM_d = n \ (mod \ d)$.

2 Aritmética módulo d

Lema 2.1. *Dados* $d \in \mathbb{N}$ *e* $a, b \in \mathbb{Z}$

- $aM_d = (a + kd)M_d$ *para qualquer* $k \in \mathbb{Z}$
- $(a + b)M_d = [(aM_d) + (bM_d)] \, M_d$
- $(ab)M_d = [(aM_d)(bM_d)] \, M_d$

3 O conjunto $\mathbb{Z}_d$

Seja $d \in \mathbb{N}$ e considere a relação de equivalência em $\mathbb{Z}$:

$$zRw \iff (z-w)(mod\ d) = 0\,;$$

seja $[z]_d$ a classe se equivalência de z.

Definimos

$$\mathbb{Z}_d := \{\ [z]_d\ \}_{z\in\mathbb{Z}}\ .$$

Então o Teorema de divisão diz que

$$n\ (mod\ d) = r \text{ implica } [n]_d = [r]_d$$

$$[n]_d = [r]_d \text{ e } r \in \{0, ..., d-1\} \text{ implica } n\ (mod\ d) = r$$

No conjunto $\mathbb{Z}_d$ podemos definir[1] as operações

- $[a]_d +_d [b]_d := [a+b]_d$, $\forall a, b \in \mathbb{Z}$ (**adição em $\mathbb{Z}_d$**)
- $[a]_d \cdot_d [b]_d := [ab]_d$, $\forall a, b \in \mathbb{Z}$ (**produto em $\mathbb{Z}_d$**)

Definição alternativa: $Z_d := \{0, 1, ..., d-1\}$, com as operações

- $a +_d b := (a+b)M_d$, onde $a, b \in Z_d$ (**adição módulo d**)
- $a \cdot_d b := (ab)M_d$, onde $a, b \in Z_d$ (**produto módulo d**)

[1] Isso não é obvio!!

Lema 3.1. *As operações* $+_d$ *e* $\cdot_d$ *definidas em* $\mathbb{Z}_d$ *satisfazem as propriedades comutativa, associativa, e distributiva do produto com respeito à adição.*

Além disso,

$[0]_d +_d \gamma = \gamma,\ \forall \gamma \in \mathbb{Z}_d$: $[0]_d$ *é elem. neutro da adição*

$[1]_d \cdot_d \gamma = \gamma,\ \forall \gamma \in \mathbb{Z}_d$: $[1]_d$ *é elem. neutro do produto*

$[a]_d +_d [d-a]_d = [0]_d,\ \forall a \in \mathbb{Z}$: $[d-a]_d$ *é o oposto de* $[a]_d$

($[0]_d \cdot_d \gamma = [0]_d,\ \forall \gamma \in \mathbb{Z}_d$ *)*

Notação:

- Quando for claro quem é d vamos retirar da notação.

- Quando for claro que estamos trabalhando em $\mathbb{Z}_d$ retiraremos também os colchetes:

exemplo fixado $d = 5$,

$[4]_5 +_5 [3]_5 = [7]_5 = [7]_5$

podemos escrever $[4] + [3] = [7] = [2]$ em $\mathbb{Z}_5$

ou também $4 + 3 = 7 = 2$ no sentido de $\mathbb{Z}_5$

ou também $4 + 3 = 2$ no sentido de Z_5 (cuidado, $7 \notin Z_5$)

4 Definição de Anel e Corpo

$(\mathbb{K}, +, \cdot)$, isto é, um conjunto $\mathbb{K}$ com uma operação $+$ dita *adição* e outra operação $\cdot$ dita *produto*, é um **Anel comutativo com unidade** se valem as propriedades:

(A1) (associativa da adição) $(x+y)+w = x+(y+w)$, para quaisquer $x, y, w \in \mathbb{K}$;

(A2) (comutativa da adição) $x+y = y+x$, para quaisquer $x, y \in \mathbb{K}$;

(A3) (elemento neutro da adição) existe $z \in \mathbb{K}$ tal que $x+z = x$ para todo $x \in \mathbb{K}$;

(A4) (oposto da adição) para todo $x \in \mathbb{K}$ existe $y \in \mathbb{K}$ tal que $x+y = z$;

(P1) (associativa do produto) $(x \cdot y) \cdot w = x \cdot (y \cdot w)$, para quaisquer $x, y, w \in \mathbb{K}$;

(P2) (comutativa do produto) $x \cdot y = y \cdot x$, para quaisquer $x, y \in \mathbb{K}$;

(P3) (elemento neutro do produto) existe $u \in \mathbb{K}$ tal que $x \cdot u = x$ para todo $x \in \mathbb{K}$;

(D) (distributiva) $(x+y)\cdot w = x\cdot w + y\cdot w$, para quaisquer $x, y, w \in \mathbb{K}$.

$(\mathbb{K}, +, \cdot)$ é um **Corpo** se valem as propriedades acima mais

(P4) (inverso do produto) para todo $x \in \mathbb{K}$ com $x \neq z$, existe $y \in \mathbb{K}$ tal que $x \cdot y = u$;

Algumas propriedades que seguem das propriedades acima:

- os neutros são únicos (logo indicaremos com 0 e 1);
- oposto e inverso (se existirem) são únicos (notação $\overline{x}$ e x^{-1});
- $x \cdot 0 = 0 \quad$ e $\quad \overline{x} = \overline{1} \cdot x$
- $x \cdot w = 0$ implica x e/ou w não é invertível

Chamamos **invertível** um elemento $x \in \mathbb{K}$ pelo qual existe $y \in \mathbb{K}$ tal que $x \cdot y = u$;

Resumindo

$(\mathbb{Z}_d, +_d, \cdot_d)$ é um anel comutativo com unidade.

- A propriedade (A4) permite definir **subtração**: $x - y := x + \overline{y}$
- A propriedade (P4) permite definir **divisão**: $x/y := x \cdot y^{-1}$ (se $y \neq 0$)
- Ainda podemos definir x/y em um anel sempre que existir y^{-1}.

Perguntas:

- quando $n \in \mathbb{Z}_d$ possui inverso?
- quando $\mathbb{Z}_d$ é um corpo?
- é difícil calcular o inverso de $n \in \mathbb{Z}_d$ (quando existe)?

Lema 4.1. *Dados $d \in \mathbb{N}$ e $a \in \mathbb{Z}$, vale a equivalência:*

$$\exists\, [a]_d^{-1} \text{ (em } \mathbb{Z}_d) \iff \exists\, i, j \in \mathbb{Z} : \quad ia + jd = 1\,.$$

Se for o caso, $[a]_d^{-1} = [i]_d$

5 Números primos e fatoração

Definição:

- $p \in \mathbb{Z} \setminus \{\pm 1\}$ é dito **primo** se os únicos $d \in \mathbb{Z}$ que dividem p são ± 1 e $\pm p$.
- $c \in \mathbb{Z} \setminus \{\pm 1\}$ é dito **composto** se não for primo.

Teorema 5.1 (Fatoração única)**.** *Todo $n \in \mathbb{N}$, $n \geq 2$ pode ser decomposto de forma única como*

$$n = \prod p_i^{e_i}$$

onde os p_i são primos positivos e $e_i \in \mathbb{N}$.

6 MCD e algoritmo de Euclides

Definição: dados $a, b \in \mathbb{Z}$ definimos:

- **Máximo Comum Divisor de a e b** (abrev $MCD(a, b)$): é o maior $M \in \mathbb{N}$ que divide a e b;.
- Se $MCD(a, b) = 1$ dizemos que **a e b são relativamente primos**.

Lema 6.1. *Dados $n, d, q, r \in \mathbb{Z}$ tais que $n = dq + r$,*

$$MCD(d, n) = MCD(d, r)$$

Baseado no Lema, temos o **Algoritmo de Euclides** para o cálculo de $MCD(n_1, n_2)$ (com $n_1 > n_2 > 0$):

1) Troca por $MCD(n_2, n_3) = MCD(n_2, n_1 M_{n_2})$,
2) Repete até chegar em $MCD(n_i, n_{i+1})$ com n_i múltiplo de n_{i+1}
3) $MCD(n_1, n_2) = n_{i+1}$

Observação:
Um algoritmo para fatorar n demora $\simeq \sqrt{n}$.
O algoritmo de Euclides para $MCD(m, n)$ demora $\simeq 2 \log_2 n$.

Analizando o algoritmo deduzimos:

Lema 6.2. *Dados $n, d \in \mathbb{N}$, o $MCD(n, d)$ é combinação linear de n e d. Isto é, $\exists i, j \in \mathbb{Z}$: $MCD(n, d) = in + jd$*

OBS: i, j podem ser calculados junto com o MCD (**Algoritmo de Euclides estendido**).

Juntando os resultados anteriores obtemos:

Teorema 6.3. *Dados* $n, d \in \mathbb{N}$,

$$MCD(n,d) = 1 \quad \iff \quad \exists\, i,j \in \mathbb{Z} : \ in + jd = 1$$

Corolário 6.4. *Dado* $d \in \mathbb{N}$,

- *dado* $a \in \mathbb{Z}$,

  $$[a]_d \text{ é invertível em } \mathbb{Z}_d \quad \iff \quad MCD(a,d) = 1.$$

  Além disso, $[a]_d^{-1}$ *pode ser calculado pelo alg. de Euclide estendido.*

- $\mathbb{Z}_d$ *é corpo* $\iff$ d *é primo.*

7 Resultados sobre primos

Lema 7.1. *Se* $a, b, c \in \mathbb{N}$ *com* $MCD(a, b) = 1$ *então*

- b *divide* $ac \implies b$ *divide* c
- a *divide* c *e* b *divide* $c \implies ab$ *divide* c

Se $a, b, p \in \mathbb{N}$ *com* p *primo então*

- p *divide* $ab \implies p$ *divide* a *ou* b

8 Resultados importantes para o RSA

Lema 8.1. *Se $p \in \mathbb{N}$ é primo então, para todo $\gamma \in \mathbb{Z}_p \setminus \{[0]\}$, a lista*

$$\gamma_i := i \cdot_p \gamma, \quad i \in \mathbb{Z}_p \setminus \{[0]\}$$

é uma permutação de $\mathbb{Z}_p \setminus \{[0]\}$.

Teorema 8.2 (Pequeno Teorema de Fermat)**.**
Se $p \in \mathbb{N}$ é primo então $a^{p-1}(mod\ p) = 1$ para todo $a \in Z_p \setminus \{0\}$.

Formulações equivalentes: Se $p \in \mathbb{N}$ é primo então

- $\gamma^{p-1} = [1]_p$ para todo $\gamma \in \mathbb{Z}_p \setminus \{[0]\}$.
- $a^{p-1}(mod\ p) = 1$ para todo $a \in \mathbb{Z}$ que não seja múltiplo de p.

Corolário 8.3. *Nas hipóteses do Teorema, $\gamma^{-1} = \gamma^{p-2}$.*

Lema 8.4. *Se $d \in \mathbb{N} \setminus \{1\}$ não é primo e $\gamma \in \mathbb{Z}_d$ não possui inverso, então*

$$\gamma^{d-1} \neq [1]_d$$

Teorema 8.5 (Teorema Chinês do resto)**.** *Se $c, d \in \mathbb{N}$ são relativamente primos, então o sistema*

$$\begin{cases} x(mod\ c) = a \\ x(mod\ d) = b \end{cases}$$

com $a \in Z_c,\ b \in Z_d$, possui uma única solução $x \in Z_{cd}$.

A solução é $x = (bic + ajd)\ (mod\ cd)$ onde $ic + jd = 1$.