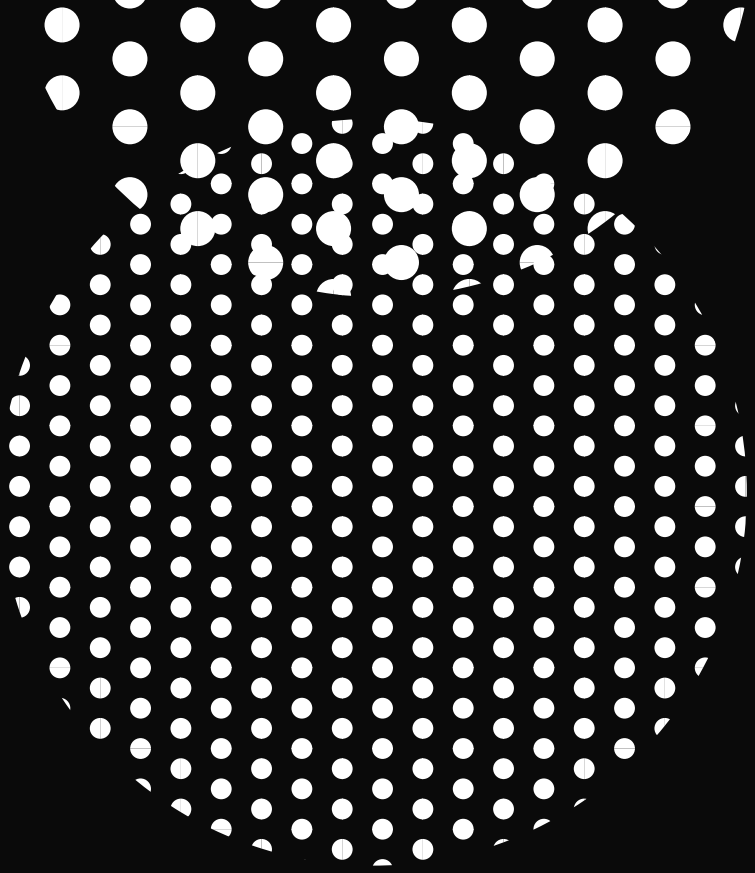


126	35
105	3
21	

Division euclidienne:

$126 = 3 \cdot 35 + 21$

Soient $0 \leq a \leq b \in \mathbb{N}$, alors $\exists\, q, r \in \mathbb{N}$ avec
$a = qb + r$ et $0 \leq r \leq b-1$

si $r \geq b$, on peut augmenter q.

Déf: Soient $a, b \in \mathbb{Z}$. On dit a divise b
si $\exists\, u \in \mathbb{Z}$ avec $au = b$

noter $a \mid b$

~~$\frac{\bullet}{0}$~~ $\quad \frac{0}{\bullet}$

Obs: $0 \mid b$ impossible
sauf si $b = 0$
pv: $0a = b = 0$
donc $0 \mid 0$ □

Obs! $a \mid 0 \quad \forall a \in \mathbb{Z}$
pv! Trouver $u \in \mathbb{Z}$
tq $au = 0$
$u = 0$

Ex: $2 \mid 4 \qquad 17 \mid 323 \qquad -2 \mid 20$

$|x| = \max(x, -x) \quad \forall x \in \mathbb{Z}$

Lm: $a \mid b$ avec $b \neq 0 \Rightarrow |a| \leq |b|$
pv: $a^{\exists} u = b$ d'où $|a| \cdot |u| = |b|$ dlleurs $u \neq 0$, sinon
si $u = 0$ $q \cdot 0 = b = 0$
on a supposé $b \neq 0$

donc $|u| \geq 1$
donc $|a| = |a| \cdot 1 \leq |a| \cdot |u|$
$\leq |a \cdot u| = |b|$

Cor:
Lm: $a \mid b$ et $b \mid a \Rightarrow |a| = |b|$ i.e $b = \pm a$ □

Lm: Si $a \mid b$ alors $\forall k \in \mathbb{Z}$ $\forall l \in \mathbb{Z}$ on a
$a \mid (ka + lb)$

pv: Hyp: $au = b$ $(\exists u \in \mathbb{Z})$ d'où $ka + lb = ka + lau$
$= (k + l \cdot u) \cdot a$
u

donc $ka + lb = a \cdot U$

Lm: $a \mid a$ $\forall a \in \mathbb{Z}$ pv: $a \cdot 1 = a$

Lm: $(a \mid b$ et $b \mid c) \Rightarrow a \mid c$

pv: $\begin{matrix} a^3u = b \\ b^3v = c \end{matrix} \Big) v \Rightarrow$ $au\underbrace{v} = bv = c$
w

$aw = c$ j'ai trouvé un $w \in \mathbb{Z}$ tq $aw = c$ □

Congruence:

Def: $a \equiv b \mod n$ (a est congru à b modulo n)
déf $\Leftrightarrow$ $n \mid (a - b)$ $\Rightarrow$ $a - b = un \Leftrightarrow a = b + un$
$\Leftrightarrow$ $\exists k \in \mathbb{Z}$ tq $a = b + kn$

$35 \equiv 2 \mod 3$

$35 = 2 + 11 \cdot 3$

Thm: Soit $a, b, d \in \mathbb{Z}$ tq $a > b$, $d \mid a$ et $d \mid b$

Alors d divise reste de la division de a et b

pv: Soit $a, b \in \mathbb{Z}$
On suppose que $\exists d \in \mathbb{Z}$ tq $d \mid a$ et $d \mid b$

Alors $\exists k_1 \in \mathbb{Z}$ tq $a = k_1 \cdot d$ et $\exists k_2 \in \mathbb{Z}$ tq $b = k_2 d$
Par la division euclidienne $\exists q, r \in \mathbb{Z}$ tq $a = qb + r$
$a = qb + r \Leftrightarrow k_1 d = q(k_2 \cdot d) + r \Leftrightarrow k_1 \cdot d = d \cdot (k_2 \cdot q) + r$
$\Leftrightarrow r = d(k_1 - k_2 \cdot q)$
donc d divise reste de la division de a et b

Prop : $a \equiv 0 \mod n \iff n \mid a \iff a$ est multiple de n

Prop : $\cdot \equiv \cdot \mod n$ est une relation d'équivalence, càd

(1) Réflexivité $a \equiv a \mod n \quad \forall a \in \mathbb{Z}$

(2) Symétrie : $a \equiv b \mod n \Rightarrow b \equiv a \mod n \quad \forall a, b \in \mathbb{Z}$

(3) Transitivité : $(a \equiv b \mod n$ et $b \equiv c \mod n) \Rightarrow a \equiv c \mod n$

pv : (1) $a - a = 0 = 0 \cdot n$

(2) Hyp : $a - b = {}^{\exists} k n \Rightarrow b - a = (-k) n = {}^{\exists} \ell n$

(3) $a - b = {}^{\exists} k n$, $b - c = {}^{\exists} \ell n$

$\overline{a + b + b - c = kn + \ell n}$ càd $a - c = (k + \ell) n =$ mult de n □

Rappel $(\mathbb{Z}, +, \times)$ anneau commutatif

$\{$entiers mod $n\} =: \mathbb{Z} / n\mathbb{Z}$ on peut faire $+$ et $\times$

EURÊKA

Prop : Pour $n \geq 1$ fixé et $\forall a, b, a', b' \in \mathbb{Z}$ avec

$a \equiv b \mod n$ « $a = b$ » dans $\mathbb{Z}/n\mathbb{Z}$

$a' \equiv b' \mod n$ « $a' = b'$ »

$a + a' \equiv b + b' \mod n$

et $a \times a' \equiv b \times b' \mod n$

pv : $a = b + {}^{\exists} k \cdot n$

Hyp $a' = b' + {}^{\exists} k' \cdot n$

Add

$a + a' = b + b' + (k + k') n$

ℓ

Mult

$a \cdot a' = (b + kn)(b' + k' n)$

$= bb' + bk'n + knb' + knk'n$

$= bb' + [bk' + kb' + kk'n] n$

L □

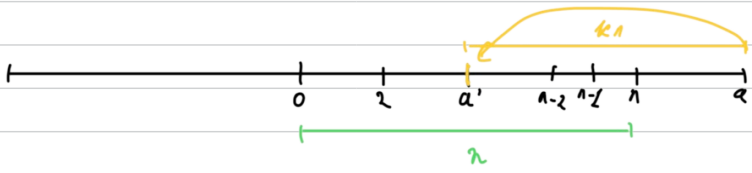
$\{a \mod n\} = \{a + kn : \forall k \in \mathbb{Z}\} = \bar{a}$ Exc : $a = 3$ $n = 5$ $\bar{a} = \{3, 8, 13, 18, 23, -2, -7 \ldots\}$

Prop : Fixer $n \geq 2$. Alors $\forall a \in \mathbb{Z}$ il existe $a' \in \mathbb{Z}$ avec

(1) $0 \leq a' \leq n - 1$

(2) $a \equiv a' \mod n$

MARMITE



Prp: Les n entiers $0, 1, 2, \dots, n-2, n-1, n$ sont (bijection) distincts deux à deux mod n

↪ $\Leftrightarrow$ $\forall k, \ell \in \{0, 1, \dots, n-1, n\}$, où $k \neq \ell$, $k \not\equiv \ell \bmod n$

Pv: $a \neq a'$ avec $0 \leq a \leq n-1$ $\Rightarrow$ $0 \leq a \leq n-1$

$-(0 \leq a' \leq n-1)$ $\quad -(n-1) \leq -a' \leq -0$ +

$-(n-1) \leq a - a' \leq n-1$

$\Rightarrow |a - a'| \leq n-1$

Par l'absurde, si on avait $a \equiv a' \bmod n$ (on a supp $a \neq a'$)

càd $a - a' = k \cdot n$ $(\exists k \in \mathbb{Z})$

$\Rightarrow k \neq 0$, sinon, si $k = 0$, on aurait $a - a' = 0$

donc $|a - a'| = |k| \cdot n$ $[\forall k \in \mathbb{Z}, |k| \geq 1]$

$\geq n$

Contradiction

CCL: $a \equiv a' \bmod n$ □

Bilan: n el^{ts} distincts dans $\mathbb{Z}/n\mathbb{Z}$

Déf: $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \dots, \overline{n-2}, \overline{n-1}\} = \{a \in [\![0, n-1]\!] \bmod n\}$

$\bar{a} = a \bmod n$

33 – 35 Poly

Ex: $n = 17$ $\quad \overline{20} = \bar{3}$ $\quad \bar{7} + \overline{13} = \overline{20} = \bar{3}$

$\bar{7} \cdot \overline{13} = \overline{91} = \bar{6}$

car $91 = 5 \cdot 17 + 6$

Dans $\mathbb{Z}/n\mathbb{Z}$: $+, \times$ dans $\mathbb{Z}$ ↷ reste dans $[\![0, n-1]\!]$

Ex: $\mathbb{Z}/17\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{16}\}$

Thm$^{*?}$ $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif, ∀ pour tout $n \geq 2$

↓ ↓ mod n

Thm: [Division euclidienne dans $\mathbb{Z}$] Soient $a, b \in \mathbb{Z}$ avec $b \neq 0$

avec un reste

$a = qb + r$

$5 = 2 \cdot 2 + 1$

cas 1: $b \geq 1$

cas 2: $b \leq -1$

Alors, il existe $q, r \in \mathbb{Z}$ tq

(1) $a = qb + r$

(2) $0 \leq r < |b|$ $\quad$ **Ex:** $b = n$

$\leq |b| - 1$

↳ car si $r \geq b$ donc $\exists \ell$ tq $r = b + \ell$ donc $a = qb + b + \ell = (q+1)b + \ell$

si $r < b$ donc on a $a = qb + b = (q+1)b$

De plus, q et r sont uniques

Pr: Comme $b \neq 0$, deux cas.

Cas 1: $b \geq 1$

Introduire $E := [m \in \mathbb{Z} : mb \leq a]$ $= \{m \in \mathbb{Z} : a - mb \geq 0\}$

Assertion: $E \neq \emptyset$, E est majoré

Rappel: $r = a - mb$ (r: écart, a: écart, mb: écart)

Deux sous-cas.

Sous-cas 1.1 $a \geq 0$

J'affirme $0 \in E$, oui

$0 \cdot b \leq a$ [sous-cas 1.1]

$b \geq 1$ (par hyp)

J'affirme que $m \leq a$ $\forall m \in E$ càd a est un majorant de E

Sinon, par l'absurde, s'il existait $m_* \in E$ avec $m_* \geq a+1$

$[\text{Cas 1 } b \geq 1]$ $a+1 \leq m_* \cdot b$ ($b \geq 1$, $m_* \in E$ donc ≤ 0)

$[m_* \in E]$ $\leq a$ Contradiction

CCL: $m \leq a$ $\forall m \in E$

$\mathbb{R}$

Sous-cas 1.2: $a \leq -1$ $b \geq 1$ (par hyp)

J'affirme que $a \in E$, oui car $b \geq 1$ et $a \leq a$

$\Rightarrow ab \leq a$

$m \in E$

donc $E \neq \emptyset$

J'affirme que $0 \in E$ est un majorant de E

Sinon, par l'abs, si $\exists\, m_* \geq 1$ avec $m_* \in E$, alors

$[\text{Cas 1 où } b \geq 1]$ $1 \leq m_* b$

$[m_* \in E]$ $\leq a$ (≤ -1, ≥ 1)

[Sous-cas 1.2] ≤ -1 Contr.

CCL: $m \leq 0$ $\forall m \in E$

□

Thm vu: Soit $q \in E$ le plus grand élt

d'où $qb \leq a$

Assertion: $E \neq \emptyset$, E est majoré

mais $q+1 \notin E$ càd on n'a pas $(q+1)b \leq a$

$\Leftrightarrow$ $a < (q+1)b$

donc $(qb \leq a < (q+1)b) - qb$ Cas 1

$0 \leq \underbrace{a - qb}_{r} < b$ Pour $r := a - qb$ satisfait (1) et (2)

Cas 2: $b \leq -1$ Diviser a par $-b$ grace au cas 1

$$a = q(-b) + r \quad \text{avec } 0 \leq r < -b = |b|$$

$$= (-q) \cdot b + r$$

□ } доказали, що q та r існують за допомогою cas 1

→ доказуємо що q, r uniq

Unicité de (q,r) : Si (q,r) et (q',r') satisfont

$$a = qb + r \quad \text{avec } 0 \leq r < |b|$$

$$- \quad a = q'b + r' \quad (0 \leq r' < |b|)$$

$$0 \leq r < |b|$$

$$-|b| < -r' \leq 0$$

$$-|b| < r - r' < |b|$$

$$|r - r'| < |b|$$

Par ailleurs, soustraire

$$a - a = 0 = qb - q'b + r - r'$$

$$\Leftrightarrow -(q - q')b = r - r'$$

Si $q \neq q'$ alors $|q - q'| \geq 1$ donc

$$|b| \leq |q - q'| \cdot |b| = |r - r'|$$

$$|b| \leq |r - r'|$$ Contr donc $q = q'$

$$0 = r - r'$$

□