(1) $\mathbb{Z}$ & STRs

Entiers relatifs

$\mathbb{Z} = \{\ldots, -n, \ldots, -3, -1, 0, +1, \ldots, n, \ldots\}$

$(\mathbb{Z}, \leq)$ TOT ordonné

...i unitené

SOMMAIRE

$\mathbb{Z}$ DIVISEURS MULTIPLES

CONGRUENCES NUMÉRATION

(1) $\mathbb{Z}$ & STRs

Entiers relatifs

$\mathbb{Z} = \{\ldots, -n, \ldots, -3, -1, 0, +1, \ldots, n, \ldots\}$

$(\mathbb{Z}, \leq)$ TOT ordonné

$\mathbb{N} \subset \mathbb{Z}$

$(\mathbb{Z}, +)$ G abelien

$(\mathbb{Z}, \times)$ ~~Groupe~~

$(\mathbb{Z}, +, \times)$ Anneau commutatif unitaire

2) Division euclidienne

peut pas déf ÷ par 0
tous diviseurs sont non nuls

Ds $\mathbb{Z}$ a par b = opération qui consiste à

trouver q et r tels que :

$$a = bq + r \qquad 0 \leq r < |b|$$

$a \in \mathbb{Z}$ (dividende), $b \in \mathbb{Z}^*$ (diviseur), $q \in \mathbb{Z}$ (quotient), $r \in \mathbb{N}$

P lorsque (a, b) est donné (q, r) est unique

quotient d'1 nb n par un produit
peut obtenir ainsi
÷ n par a puis ÷ ce quotient par b ou...
dernier quotient est le quotient recherché
dernier reste n'est pas le r cherché
en gén.

D a est divisible par b
lorsque $a = bq$
division de a par b donne
un reste nul

a divisible par b)) *
a multiple de b
b divise a
b diviseur de a

P Si un nb divise chaque terme d'1
somme, il divise la somme

Si un nb divise a, il divise tt multiple
de a

nb div par 2 ssi écriture décimale
se termine par 0, 2, 4, 6, 8 pair

3 ssi somme chiffres
de son é.d. est divisible par 3

5 0 ou 5

Notation $p\mathbb{Z}$:

ensemble des multiples de p
où p est fixé ($p \neq 0$)
s'exprime par ~~$\{kp, k \in \mathbb{C}$~~
$\{kp\ ,\ k \in \mathbb{Z}\}$

str $(p\mathbb{Z}, +)$ SG abélien de $(\mathbb{Z}, +)$
$(p\mathbb{Z}, +, \times)$ sous Anneau
com de $\mathbb{Z}$

(tt sous G ou sous A
de $\mathbb{Z}$ est de type $p\mathbb{Z}$)

3) NBS PREMIERS $\mathbb{N}$

D $p \geq 2$ et les seuls diviseurs de p sont 1 et p

T Si $n \geq 2$ non premier il est multiple de nbs premiers

PS donc possède un diviseur autre que 1 et n soit p

$n = pq$

∞

noc si p est premier 2 ne't

T Wilson

p premier $\Leftrightarrow$ p divise $(p-1)!+1$

crible Erastosthène

on cherche le + gd entier x tq $x^2 \leq n$

on essaie diviseurs de n

nbr premiers 2, 3, 5

jusqu'à celui x' qui est immédiatement $< x$ si aucun n est premier

79

$x^2 \leq 79 \Rightarrow x < 9$

ici $x' = 7$ aucune ÷ par 2 3, 5 7

ne "tombe juste"

. T FERMAT

Si p premier ne divise pas a alors p divise $a^{p-1} - 1$

. Si p premier divise un produit p divise au moins un facteur

. ens diviseurs 1 et n est unique

. card est ens on lit

$n = 540 = 2^2 \times 3^3 \times 5$

n possède autant de diviseurs qu'il y a de termes ds dvpt

$(2^0+2^1+2^2)(3^0+3^1+3^2)(5^0+5^1)$

soit $(2+1)(3+1)(1+1)$ soit 24 2 autres Gurri

(4) PGCD et Notions Associées

les diviseurs

~~Soint~~ Soient

$a_1, a_2, \dots, a_n$

le PGCD de ces nbs

noté pgcd$(a_1, a_2, \dots, a_n)$

il est au moins égal à 1 (donc positif)

D | pgcd$(a_1, a_2, \dots, a_n) = d$
lorsque d divise chaque a_i et
d le + grand possible

Lorsque $d = 1$ on dit que nbs sont premiers entre eux

______ et que chaque pgcd(a_i, a_j) est 1 ______ donc 2 à 2 ______ entre eux

16 24 39 premiers entre eux 2 à 2 ? non premiers entre eux

30 18 25 ______ non

~~Si pgcd)~~

Si pgcd$(a, b) = 1$
on dit aussi a est premier avec b
ou b ______ a

pgcd : | $\mathbb{Z} \to \mathbb{Z}$ (ou $\mathbb{N}^*$)
$(a, b) \to$ pgcd(a, b)

Lien $\mathbb{Z} \subset A$
→ de bornes 2 nbs

en pratique 2 nbs +
trouver pgcd$(a, b) > 0$
2 méthodes possibles

1 Facteurs premiers communs

$825 = 3 \times 5^2 \times 11$

$2625 = 3 \times 5^3 \times 7$

pgcd est $3 \times 5^2 = 75$
[illegible] des exposants

2 Algorithme Euclide (÷ successives)

- Soit a le plus grand des nbs a et b
on divise a par b
d'où $a = bq + r$ et $0 \leq r < b$

• Si $pgcd(a,b) = d$
néc^T $d = pgcd(b,r)$
car d divise a càd $bq+r$
— bq ou d divise,
d'où donc diviseur commun à b et r
• on recommence par b et r
$b = rq' + r'$ $\quad 0 \leq r' < r$
or néc^t $d = pgcd(r, r')$
on cont^u r successifs
décroissant
$pgcd(a,b)$ est le dernier reste non nul

$pgcd(825, 2625) = 75$
$2625 = \underline{825} \times 3 + \underline{150}$
$825 = \underline{150} \times 5 + 75$
$150 = 75 \times 2 + 0$
dernier reste non nul : 75

Rem $pgcd(ka, kb) = k \times pgcd(a,b)$
— $\left(\frac{a}{k}, \frac{b}{k}\right) = \frac{pgcd(a, b)}{k}$ lorsque k divise a et b
— $\frac{a}{d}$ $\frac{b}{d}$ $= 1$ si d $pgcd$ de a et b

quotients
de nuls
par leur pgcd
sont premiers entre eux

(5) PPCM & T DIVERS

$\neq 0$ $a_1, a_2, \dots, a_n$

PPM positif, c noté ppcm(, . .)

D ~~ppcm~~

ppcm$(a_1, a_2, \dots, a_n) = m$ ~~lorsq~~ lorsque

m est multiple de chaque a_i et

m est le plus petit positif possible

ppcm : $\mathbb{Z}^* \times \mathbb{Z}^* \to \mathbb{Z}^*$ (ou $\mathbb{N}^*$)

$(a, b) \to$ ppcm(a, b)

Li c A → bornes 2 ... >0

Trouver ppcm(a, b)

- on decomp en facteurs premiers

on prend chacun des ______

avec le + gd ~~exposant~~ écrit

$825 = 3 \times 5^2 \times 11$

$2625 = 3 \times 5^3 \times 7$

ppcm → $3 \times 5^3 \times 7 \times 11 =$

$(825, 2625) = 28875$

$\simeq$ prop

ppcm$(ka, kb) = k \times$ ppcm(a, b)

et $\frac{a}{k} \frac{b}{k}$ = ppcm $\frac{(a, b)}{k}$

ST

- si ppcm$(a, b) = m$

$\frac{m}{a}$ et $\frac{m}{b}$ sont premiers entre eux

on pgcd $\left(\frac{m}{a}, \frac{m}{b}\right) = 1$

- produit de a et b positifs

est égal à celui de leur ppcm

et pgcd $ab = md$

.T BEZOUT

Si a et b premiers entre eux

on pgcd$(a, b) = 1$

ssi on peut trouver u et v de $\mathbb{Z}$

tel que $ua + vb = 1$

.T GAUSS

(6) CONGRUENCES MODULO n.
ENSEMBLES $\mathbb{Z}/n\mathbb{Z}$

multiples d'un entier ~~fixé~~ n fixé
$n \geq 2$ forment une partie de $\mathbb{Z}$
dont elts (nommés) "vont de n en n"
tables multiplication $\mathbb{Z}$

D : l'entier n étant fixé, $n \geq 2$
la congruence modulo n
est la relation d'équivalence $\mathcal{R}$ définie
ds $\mathbb{Z}$ par
$a \mathcal{R} b$
signifie "$a-b$ est multiple de n"

$a \mathcal{R} b$ $\quad a \equiv b \pmod{n}$
a et b sont congrus modulo n

ex pour $n = 2$:
2 nbs pairs sont congrus $\pmod 2$
puisque leur différence est paire
(ou multiple de 2)
de m̄ pr 2 nbs impairs (différence paire)

. Classes d'équivalence et ensemble-quotient (mod n)

Supposons $a \equiv b \pmod{n}$

divisons a et b par n
on obtient

$a = nq_1 + r_1$
$b = nq_2 + r_2$
alors $a - b \equiv r_1 - r_2 \pmod{n}$
donc a congru à b (mod n) signifie $r_1 = r_2$

... À revoir !

7) Syst de numération

représenter nbs entiers sous des formes aussi condensées que possible, on veut conçues pour opérations

Pour cela on se donne un certain nb de symboles avec règles d'écriture (ou une seule règle)

ens symboles & règles écriture = sys numération

nb = **base**

Sys décimal ou de base dix

0, 1, 2, 3, 4, 5, 6, 7, 8, 9 chiffres

base s'écrit grâce aux second et premier symbole côte à côte, soit 10

on la désigne par b on écrit $b = 10$ "b égale dix"

. Un entier naturel se décompose d'une manière unique à l'aide de la base b sous la forme

$$n = a_p b^p + a_{p-1} b^{p-1} + \dots + a_1 b + a_0$$

où les a_i sont des chiffres

règle écriture décimale ->

écrire côte à côte

$a_p a_{p-1} \dots a_1 a_0$ (ds cet ordre)

ex quatre mille quatre vingt quinze se décompose en

$$4 \cdot 10^3 + 0 \cdot 10^2 + 9 \cdot 10 + 5$$

on écrit 4095

Cas littéral on se contente d'écrire

$$n = \overline{a_p a_{p-1} \dots a_1 a_0}$$

ou $[a_p a_{p-1} \dots a_1 a_0]$

cas numérique supprimé surligné ou [ ]

- Connaissant écriture nb en base b reconstituer signif inverse de règle écrit

7901340 représ $n = 7 \cdot 10^6 + 9 \cdot 10^5 + 10^3 + 3 \cdot 10^2 + 4 \cdot 10$

terme court

$0 \cdot b^4 = 0$

$1 \cdot b^3 = 10^3$

supprime +0 à la fin

· Sys linéaire ~~[illegible]~~ base deux

0, 1

$b = 10$ "b égale deux"

admis

2 — condition formelle
ne pas exploser
2 autrement

$n = a_p b^p + a_{p-1} b^{p-1} + \dots + a_1 b + a_0$

où $a_i \in \{0, 1\}$

cinquante et un

$2^5 + 2^4 + 2 + 1$ — 110011

$b^5 + b^3 + b^2$

$32 + 8 + 4$