

# Arithmétique sur $\mathbb{Z}$

Dans ce qui suit quand l'appartenance de nombres à des ensembles n'est pas précisée, on considèrera qu'il s'agit de nombres de  $\mathbb{Z}$ .

## Division Euclidienne

- Toute partie non vide de  $\mathbb{N}$  a un plus petit élément
- Division euclidienne: tout  $(a,b) \exists (q,r)$  uniques  $| a=bq+r$  avec  $0 \leq r < b$
- $b$  divise  $a$  si  $\exists q \in \mathbb{Z}$  tel que  $a = bq$
- $(a-1)$  divise  $a^n - 1$ ?
- sous quelle condition  $n+1$  divise  $n^2 + 1$

## Nombres premiers

- $p$  premier si  $p \geq 2$  et les seuls diviseurs positifs de  $p$  sont 1 et  $p$
- tout entier  $\geq 2$  est divisible par au moins un nombre premier.
- l'ensemble  $P$  des nombres premiers est infini  
En effet s'il est fini  $\{p_1, \dots, p_n\} \rightarrow (p_1 \dots p_n) + 1$  ne doit pas être premier et doit être divisible par un nombre premier  $pr$ . Et comme  $(p_1 \dots p_r \dots p_n)$  est divisible par  $pr$ , 1 doit l'être aussi
- **Lemme d'Euclide** : si  $p$  premier divise  $ab$  alors  $p$  divise  $a$  ou  $b$ .
- Tout entier est décomposable de façon unique en produit de facteurs premiers  $p_1^{e_1} \dots p_n^{e_n}$ .
- **Petit théorème de Fermat**  
si  $1 \leq k \leq p-1$  et  $p$  premier alors  $p$  divise  $C_p^k$ .  
par récurrence sur  $a$  on en déduit que si  $p$  premier, il divise  $a^p - a$   
S'il existe un entier naturel  $a$  tel que  $n$  ne divise pas  $a^n - a$ , c'est que  $n$  n'est pas premier.
- Les nombres de Carmichael sont tels que  $n$  non premier et pour tout  $a$   $a^n - a$  divisible par  $n$  (infinité de **nombres de Carmichael** : 561, 1105, ...)
- On peut prouver que si pour tout  $n \rightarrow p=6n+1, q=12n+1$  et  $r=18n+1$  sont premiers alors  $pqr$  est un nombre de Carmichael.
- Démontrer: Si  $2^n - 1$  est premier (**nombre de Mersenne**) alors  $n$  est premier.
- Démontrer: Si  $2^{2^n} + 1$  est premier (**nombre de Fermat**) alors  $n$  est une puissance de 2
- Rechercher : tous les premiers  $p$  tels que  $p$  divise  $2^p + 1$  (utiliser Fermat)
- test de primalité si  $n \geq 2$  n'est pas premier alors  $n$  possède un diviseur premier vérifiant  $p^2 \leq n$
- **crible d'Erastosthène**: on vérifie que  $n$  n'est pas divisible par  $k$  et on barre tous les multiples de  $k$  pour tout  $k \leq \sqrt{n}$ . Si le test est négatif,  $n$  est premier.

## Valuation p-adique d'un entier relatif

- définition:  $v_p(n)$  est la valuation p-adique de  $n$  si  $v_p(n)$  est l'exposant de  $p$  dans la décomposition en facteurs premiers de  $n$ .  $v_p(n) \in \mathbb{N} \cup \{+\infty\}$
- On pose  $v_p(0) = +\infty$ ,  $v_p(1) = 0$  et  $v_p(-n) = v_p(n)$
- Si  $p$ , premier, ne divise pas  $n$  on a  $v_p(n) = 0$ .
- Exemple  $539000 = 2^3 5^7 7^2$  et donc  $v_5(539000) = 7$  et  $v_{13}(539000) = 0$ .
- tout  $n = \varepsilon \prod p_i^{v_p(n)}$  avec  $\varepsilon = \pm 1$  pour le signe
- $a$  et  $b$  premiers entre eux s'il n'existe pas de nombre premier divisant à la fois  $a$  et  $b$ .  
Autrement dit pour tout  $p$  premier,  $\min(v_p(a), v_p(b)) = 0$ .
- Lemme de Gauss : si  $a$  divise  $bc$  et  $a$  premier avec  $b$ , alors  $a$  divise  $c$ .
- Si  $r, s$  premiers entre eux et  $a$  divisible par  $r$  et par  $s$ , alors  $a$  divisible par  $rs$ .
- Soient  $p$  et  $q$  premiers montrer que  $pq$  divise  $p^{q-1} + q^{p-1} - 1$ .

## PGCD

- DEF. Le PGCD de a et b est l'unique entier d vérifiant: 1) d divise a et b 2) tout diviseur commun de a et de b divise d. On a  $d = \prod p^{\min(v_p(a), v_p(b))}$  (produit des facteurs premiers communs avec leur exposant minimum). Noté PGCD(a,b) ou  $a \wedge b$
- $\frac{a}{d}$  et  $\frac{b}{d}$  sont premiers entre eux

- ▣  $a \geq 2$  et  $m \geq 1$  montrer que  $\text{PGCD}\left(\frac{a^m - 1}{a - 1}, a - 1\right) = \text{PGCD}(a - 1, m)$
- ▣ déterminer  $\{(x, y)\}$  tels que  $x + y - 1 = \text{PGCD}(x, y)$
- ▣ montrer que  $\text{PGCD}(\text{PGCD}(a, b), c) = \text{PGCD}(a, \text{PGCD}(b, c))$

- **BEZOUT**:  $\exists (u, v)$  tels que  $ua + vb = \text{PGCD}(a, b)$
- a et b premiers entre eux  $\Leftrightarrow \exists (u, v)$  tels que  $ua + vb = 1$
- ▣ Montrer que pour tout n,  $12n + 5$  et  $5n + 2$  sont premiers entre eux
- On peut généraliser ces définitions et résultats à une famille finie d'entiers non nuls  
BEZOUT généralisé :  $d = u_1 a_1 + u_2 a_2 + \dots + u_n a_n$   
 $\text{PGCD}(a, b, c) = \text{PGCD}(\text{PGCD}(a, b), c)$

## L'algorithme d'Euclide

- $r_0 = a$   $r_1 = b$   $r_2 =$ reste de la division euclidienne de  $r_0$  par  $r_1$   
 $r_3 =$ reste de la division euclidienne de  $r_1$  par  $r_2$   
 $r_4 =$ reste de la division euclidienne de  $r_2$  par  $r_3$

et ainsi de suite jusqu'à  $r_n = 0$ .

On a  $\text{PGCD}(r_{i-1}, r_i) = \text{PGCD}(r_i, r_{i+1})$

Les  $r_i$  constituent une suite décroissante et  $r_{n-1}$  dernier reste avant  $0 = \text{PGCD}(a, b)$ .

- détermination de u, v de Bezout (dans ce qui suit remplacer f(x, y) par "en fonction de x et y")

de  $a = bq_1 + r_2$  on tire  $r_2 = f(a, b)$

de  $b = r_2q_2 + r_3$  on tire  $r_3 = f(b, r_2) = f(a, b)$

de  $r_2 = r_3q_3 + r_4$  on tire  $r_4 = f(r_2, r_3) = f(a, b)$

et ainsi de suite jusqu'à  $r_{n-1} = f(a, b)$  qui donne Bezout

- ▣ soit  $n \geq 1$  déterminer  $\text{PGCD}(9n + 4, 2n - 1)$
- ▣ soit  $a \geq 1$  et  $b \geq 1$  déterminer  $\text{PGCD}(2^a - 1, 2^b - 1)$
- ▣ déterminer les n de 4 chiffres tels que les restes de  $21685:n$  soit 37 et de  $33509:n$  soit 53

## L'équation $ax + by = c$

Soit  $S = \{(x, y) \text{ entiers relatifs}\}$  tels que pour 3 entiers donnés, a, b, c, on ait  $ax + by = c$

Soit  $d = \text{PGCD}(a, b)$ . Posons  $a' = \frac{a}{d}$  et  $b' = \frac{b}{d}$

- $S$  non vide  $\Leftrightarrow d$  divise c
- Si  $S$  non vide et  $ax_0 + by_0 = c$  alors  $S = \{(x_0 + kb', y_0 - ka') \mid k \in \mathbb{Z}\}$
- ▣ déterminer  $\{(x, y) \in \mathbb{Z} \mid 47x + 111y = 1\}$

## PPCM

Définition 1)  $m = \text{PPCM}(a,b) =$  multiple commun de  $a$  et de  $b$

2) tout multiple commun de  $a$  et de  $b$  est un multiple de  $m$ .

$m =$  produit de tous les facteurs premiers de  $a$  et de  $b$  avec leur plus grand exposant

●  $\text{PGCD}(a,b) \cdot \text{PPCM}(a,b) = |ab|$

● On peut étendre la notion de PPCM à une famille finie d'entiers mais on n'a pas

$$\text{PGCD}(2,3,4) \cdot \text{PPCM}(2,3,4) = 2 \cdot 3 \cdot 4 = 24$$

## Numération en base b

● DEF Soit  $x \in \mathbb{N}$  non nul, on peut l'écrire de manière unique  $x = a_n b^n + a_{n-1} b^{n-1} + \dots + a_0 b^0$  avec  $0 \leq a_i \leq b-1$  on dit que  $x = a_n \dots a_0$  est l'écriture de  $x$  en base  $b$  ou  $x = (a_n \dots a_0)_b$

Exemple  $1101$  en base  $2 = 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 = 1 + 0 + 4 + 8 = 13$  en base  $10$ .

■ écrire  $7456$  en base  $3$

■ soit  $n$  un entier naturel. À quelle condition est il divisible par  $3$ ? par  $9$ ?

■ soit  $n = (a_k \dots a_0)_{10}$ . Montrer  $n$  divisible par  $11 \Leftrightarrow \sum_{i=0}^k (-1)^i a_i = 0$

■ Quels nombres de  $2$  chiffres s'écrivent vu en base  $10$  et  $uv$  en base  $7$ ?

### ● Calcul rapide de la puissance d'un entier

Pour calculer  $x^n$  il faut faire  $n - 1$  multiplications

or en base  $2$  on a  $n = a_n 2^{i_k} + \dots + a_0 2^{i_0}$  (avec  $a_i = 0$  ou  $1$ ) et pour calculer  $x^{2^{i_k}}$  on calcule aussi les autres  $x^{2^{i_j}}$

( $i_k$  multiplications) et pour calculer  $x^n$ , il faut multiplier  $x^{2^{i_0}} \dots x^{2^{i_k}}$  ( $k$  multiplications) donc en tout  $i_k + k$  multiplications.

On a  $k \leq i_k$  et  $2^{i_k} \leq n$

donc  $i_k \leq \frac{\log n}{\log 2}$  et  $k + i_k \leq \frac{2 \log n}{\log 2}$  soit moins de  $n - 1$  multiplications

■ combien de multiplications pour calculer  $x^{101}$  ?

### ● Formule de Legendre donnant $v_p(n!)$

Démontrer: Soit  $(a_k \dots a_0)_p$  l'écriture de  $n$  en base  $p$ . On a  $v_p(n!) = \frac{n-S}{p-1}$  avec  $S = \sum_{i=0}^k a_i$

1) avec  $\text{PE}() =$  partie entière on a  $\text{PE}\left(\frac{a+1}{b}\right) - \text{PE}\left(\frac{a}{b}\right) = 0$  si  $b$  divise  $a+1$  ou  $1$  dans le cas contraire

2) pour tout entier  $N \geq 1$  on pose  $S_N = \sum_{i \geq 1} \text{PE}\left(\frac{N}{p^i}\right)$ . C'est une somme finie car  $\text{PE}() = 0$  si  $i$  grand.

3) pour tout entier  $N \geq 1$  on a  $v_p(N!) = S_N$  car

$$\text{PE}\left(\frac{N+1}{p^i}\right) - \text{PE}\left(\frac{N}{p^i}\right) = 0 \text{ si } i \text{ inférieur ou égal à l'exposant de } p \text{ dans } N+1 \text{ (sinon } = 1)$$

$$\text{d'où } S_{N+1} - S_N = \sum_{1 \leq i \leq v_p(N+1)} 1 = v_p(N+1)$$

$$\text{Et comme } v_p((N+1)!) = \sum_{j=1}^{N+1} v_p(j) = v_p(N!) + v_p(N+1).$$

$$\text{Par récurrence } v_p((N+1)!) = S_N + v_p(N+1) = S_{N+1}$$

4) Par ailleurs On a  $n = a_k p^k + \dots + a_1 p + a_0$  avec  $0 \leq a_i < p$  d'où  $\text{PE}\left(\frac{n}{p^j}\right) = a_k p^{k-j} + \dots + a_j$

comme  $n < p^{k+1}$  on a  $\text{PE}\left(\frac{n}{p^j}\right) = 0$  pour  $j > k$ .

$$\text{On a donc } v_p(N!) = S_N = \sum_{i \geq 1} \text{PE}\left(\frac{N}{p^i}\right).$$

$$\text{soit } v_p(n!) = a_1 + a_2(p+1) + a_3(p^2+p+1) + \dots + a_k(p^{k-1} + p^{k-2} + \dots + p + 1)$$

$$v_p(n!) = \frac{1}{p-1} (a_1(p-1) + a_2(p^2-1) + a_3(p^3-1) + \dots + a_k(p^k-1)) = \frac{n-S}{p-1}$$

■ Application:  $100 = (1100100)_2 = (400)_5$ . Donc  $v_2(100!) = 97$  et  $v_5(100!) = 24$ .  $100! = 2^{97} \cdot 5^{24} = 2^{73} \cdot 10^{24}$ .  $100!$  se termine par  $24$  zéros en base  $10$ .