Arithmétique dans $\mathbb{Z}$

الحسابيات في $\mathbb{Z}$

📚 Résumé du cours

I. Rappels : divisibilité et division euclidienne

Divisibilité

Pour $a \in \mathbb{Z}$, $b \in \mathbb{Z}^*$, on dit que b divise a ($b|a$) s'il existe $k \in \mathbb{Z}$ tel que $a = bk$.

Division euclidienne

Pour tout $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, il existe un unique $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$ avec $0 \leq r < b$.

II. Congruences modulo n (approfondissement)

Définition

Soit $n \in \mathbb{N}^*$. $a \equiv b[n] \Leftrightarrow n|(a-b) \Leftrightarrow a$ et b ont le même reste dans la division par n.

Opérations compatibles

Si $a \equiv a'[n]$ et $b \equiv b'[n]$, alors :

- $a + b \equiv a' + b'[n]$
- $a \cdot b \equiv a' \cdot b'[n]$
- $a^k \equiv a'^k[n]$ pour tout $k \in \mathbb{N}$
- $P(a) \equiv P(a')[n]$ pour tout polynôme P à coefficients entiers

Simplification dans une congruence

$ac \equiv bc[n]$ n'implique pas $a \equiv b[n]$ en général. Mais :

$$\textbf{Si } \operatorname{pgcd}(c, n) = 1 : ac \equiv bc[n] \Rightarrow a \equiv b[n]$$

III. PGCD, PPCM — rappels et approfondissements

Propriétés du PGCD

- $\operatorname{pgcd}(a, b) = \operatorname{pgcd}(b, a - bq)$ pour tout $q \in \mathbb{Z}$ (base de l'algorithme d'Euclide).
- Tout diviseur commun de a et b divise $\operatorname{pgcd}(a, b)$.
- $\operatorname{pgcd}(ka, kb) = |k| \cdot \operatorname{pgcd}(a, b)$.

Caractérisation du PGCD

$d = \operatorname{pgcd}(a, b) \Leftrightarrow d \geq 0$, $d|a$, $d|b$, et tout diviseur commun de a et b divise d.

Relation PGCD × PPCM

$$\operatorname{pgcd}(a, b) \times \operatorname{ppcm}(a, b) = |a \times b|$$

IV. Théorème de Bézout

Identité de Bézout

Pour tous $a, b \in \mathbb{Z}$ non tous deux nuls, il existe $u, v \in \mathbb{Z}$ tels que :

$$au + bv = \text{pgcd}(a, b)$$

Forme caractéristique (nombres premiers entre eux)

$\text{pgcd}(a, b) = 1 \Leftrightarrow \exists u, v \in \mathbb{Z}, au + bv = 1$

Algorithme d'Euclide étendu

Les coefficients u, v s'obtiennent par **remontée** des divisions successives de l'algorithme d'Euclide.

V. Théorème de Gauss

Énoncé

Si $a|bc$ et $\text{pgcd}(a, b) = 1$, alors $a|c$.

Corollaires utiles

- Si $a|n$, $b|n$ et $\text{pgcd}(a, b) = 1$, alors $ab|n$.
- Si $\text{pgcd}(a, n) = 1$ et $\text{pgcd}(b, n) = 1$, alors $\text{pgcd}(ab, n) = 1$.
- Si $\text{pgcd}(a, b) = 1$, alors $\text{pgcd}(a^k, b^m) = 1$ pour tous $k, m \in \mathbb{N}$.

VI. Nombres premiers — approfondissement

Lemme d'Euclide

Si p est premier et $p|ab$, alors $p|a$ ou $p|b$.

Théorème fondamental de l'arithmétique

Tout $n \geq 2$ se décompose, de manière **unique** (à l'ordre près), en produit de facteurs premiers :

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$$

Nombre de diviseurs

Si $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, le nombre de diviseurs positifs de n est :

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_k + 1)$$

VII. Petit théorème de Fermat

Énoncé

Soit p un nombre **premier** et a un entier.

- **Si p ne divise pas a :** $a^{p-1} \equiv 1[p]$
- **Pour tout a :** $a^p \equiv a[p]$

Applications

- Calcul rapide de restes de puissances élevées modulo un nombre premier.
- Critères d'irréductibilité, tests de primalité (test de Fermat).
- Résolution d'équations du type $a^n = b[p]$.

Exemple

Calculer $3^{2024} \bmod 7$. Comme 7 est premier et $7 \nmid 3$: $3^6 \equiv 1[7]$. Or $2024 = 6 \cdot 337 + 2$. Donc $3^{2024} = (3^6)^{337} \cdot 3^2 \equiv 1 \cdot 9 \equiv 2[7]$.

VIII. Équations diophantiennes ax + by = c

Critère d'existence de solutions

$ax + by = c$ admet des solutions $(x, y) \in \mathbb{Z}^2$ **si et seulement si** $\text{pgcd}(a, b) | c$.

Méthode complète

1. Calculer $d = \text{pgcd}(a, b)$. Si $d \nmid c$: pas de solution.
2. Diviser par d : $a'x + b'y = c'$ avec $\text{pgcd}(a', b') = 1$.
3. Chercher une solution particulière (x_0, y_0) par Bézout.
4. Solution générale : $x = x_0 + b' \cdot k, y = y_0 - a' \cdot k$ pour $k \in \mathbb{Z}$.

IX. Systèmes de congruences — théorème chinois

Théorème chinois des restes

Soient $m, n \in \mathbb{N}^*$ avec $\text{pgcd}(m, n) = 1$. Pour tous $a, b \in \mathbb{Z}$, le système :

$$\{x \equiv a[m] \text{ et } x \equiv b[n]\}$$

admet une **unique solution modulo** mn.

Résolution pratique

1. Écrire $x = a + mk$ pour un $k \in \mathbb{Z}$.
2. Reporter dans la deuxième : $a + mk \equiv b[n] \Rightarrow mk \equiv b - a[n]$.
3. Comme $\text{pgcd}(m, n) = 1$, m est inversible modulo n : $k \equiv m^{-1}(b - a)[n]$.
4. Remonter : $x = a + mk = a + m \cdot [m^{-1}(b - a) \bmod n] \bmod mn$.

X. Critères de divisibilité (applications)

- **Par 3 ou 9 :** un entier est divisible par 3 (resp. 9) ssi la somme de ses chiffres l'est. *(Car* $10 \equiv 1[3]$ *et* $[9]$*.)*
- **Par 11 :** somme alternée des chiffres divisible par 11. *(Car* $10 \equiv -1[11]$*.)*
- **Par 7 :** le nombre formé en soustrayant $2\times$ le dernier chiffre au nombre privé de son dernier chiffre est divisible par 7.
- **Par 4 :** les 2 derniers chiffres forment un nombre divisible par 4.
- **Par 8 :** les 3 derniers chiffres forment un multiple de 8.

🎯 Formules clés

- **Division euclidienne :** $a = bq + r,\ 0 \leq r < b$
- **Congruences :** $a \equiv b[n] \Leftrightarrow n|(a-b)$ · stable par $+,\ \times,\ ^k$
- **Algorithme d'Euclide :** $\text{pgcd}(a,b) = \text{pgcd}(b, a \bmod b)$
- **Bézout :** $\text{pgcd}(a,b) = 1 \Leftrightarrow \exists u, v : au + bv = 1$
- **Gauss :** $a|bc$ et $\text{pgcd}(a,b) = 1 \Rightarrow a|c$
- **Petit Fermat :** p premier, $p \nmid a \Rightarrow a^{p-1} \equiv 1[p]$
- **Fermat (forme générale) :** $a^p \equiv a[p]$
- **Chinois :** $\text{pgcd}(m,n) = 1 \Rightarrow \{x \equiv a[m], x \equiv b[n]\}$ unique mod mn
- $ax + by = c$ **:** solutions $\Leftrightarrow \text{pgcd}(a,b)|c$ · générale : $(x_0 + b'k, y_0 - a'k)$
- $\tau(n)$ **:** si $n = \prod p_i^{\alpha_i}$, alors $\tau(n) = \prod(\alpha_i + 1)$

💡 Astuces & méthodes

🔴 Pièges classiques

❌

Petit Fermat : p **ne doit pas diviser** a **:** le théorème dit $a^{p-1} \equiv 1[p]$ seulement si $\text{pgcd}(a,p) = 1$. Si $p|a$, alors $a \equiv 0[p]$ et $a^{p-1} \equiv 0[p]$, pas 1 !

❌

Congruences et division : on ne peut pas « diviser » des deux côtés d'une congruence sauf si le diviseur est premier avec le modulus. $6 \equiv 2[4]$ ne donne pas $3 \equiv 1[4]$ après division par 2 (car $\text{pgcd}(2,4) \neq 1$) !

❌

Théorème chinois : vérifier $\text{pgcd}(m,n) = 1$ **:** le théorème des restes chinois exige que m et n soient premiers entre eux. Si $\text{pgcd}(m,n) > 1$, le système peut ne pas avoir de solution.

🟢 Astuces de pros

✅

Calcul de $a^n \bmod p$ **:** utiliser le petit Fermat + décomposition de n en quotient-reste par $p-1$. Ex : $3^{100} \bmod 7$: $3^6 \equiv 1[7]$ (Fermat), $100 = 6 \times 16 + 4$, donc $3^{100} \equiv 3^4 = 81 \equiv 4[7]$.

✅

Trouver $\tau(n)$ **rapidement :** décompose $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots$ puis $\tau(n) = (\alpha_1+1)(\alpha_2+1)\ldots$ Ex : $\tau(12) = \tau(2^2 \cdot 3) = 3 \times 2 = 6$ diviseurs (1, 2, 3, 4, 6, 12).

💡

Algorithme de Bézout : remonte les étapes d'Euclide pour exprimer $\text{pgcd}(a,b) = ua + vb$. Cette combinaison linéaire donne une solution particulière de l'équation diophantienne $ax + by = \text{pgcd}(a,b)$.