Arithmétique dans $\mathbb{Z}$: Cours

1 Généralités

Rappels utiles

Soient $a, b, c \in \mathbb{Z}^*$,
-) On dit que a divise b, et on note $a|b$ ssi $\exists k \in \mathbb{Z}, b = ak$.
-) On a $a \equiv b[c]$ ssi $c|(a-b)$
-) $a \equiv b[c] \implies a^n \equiv b^n[c]$ pour $n\mathbb{N}$.
-) Si $a = bq + r$ avec $0 \leqslant r < |b|$ alors q s'appelle le quotient et r s'appelle le reste de la division euclidienne de a par b.
-) On dit que a est premier ssi ses seuls diviseurs sont $\pm a, \pm 1$ et $|a| \neq 1$. (1 et -1 ne sont pas premiers). On note $\mathbb{P}$ l'ensemble des nombres premiers.
-) On appelle pgcd de a et b le plus grand diviseur commun de a et b, on le note $a \wedge b.(\geqslant 0)$. Par convention on pose : $0 \wedge 0 = 0$.
-) On appelle ppcm de a et b le plus petit multiple commun positif de a et b et on le note $a \vee b$.
-) Si $c|a$ et $c|b$ alors c divise toute combinaison linéaire de a et b.
-) Si $c|a$ et $c|b$ alors : $c|a \wedge b$.
-) $c|a$ et $c|b \Leftrightarrow c|a \wedge b$.
-) Si $a|b$ et $b|a$ alors $|a| = |b|$.
-) Si $a \wedge b = 1$ alors a est premier avec tous les diviseurs de b.

2 Division euclidienne

Théorème

Soient $a, b \in \mathbb{Z}$ avec $b \neq 0$. Alors :

$$\exists!(q, r) \in \mathbb{Z}^2 \text{ tel que : } a = bq + r \text{ et } 0 \leqslant r < |b|.$$

Dans ce cas, q s'appelle le quotient et r s'appelle le reste de la division euclidienne de a par b.

3 PGCD

Théorème d'Euclide

Soient $a, b \in \mathbb{Z}$ avec $b \neq 0$ et r le reste dans la division euclidienne de a par b. Alors :

$$a \wedge b = b \wedge r$$

$\rightarrow$ Preuve : Par ***double divisibilité*** : on écrit d'abord : $a = bq + r$. Alors :
-) On a : $a \wedge b | a$ et $a \wedge b | b$ donc $a \wedge b | a - bq = r$ donc $a \wedge b | b \wedge r$.
-) On a aussi : $b \wedge r | b$ et $b \wedge r | r$ donc $b \wedge r | bq + r = a$ donc $b \wedge r | a \wedge b$.
De plus ces deux entiers sont tous les deux positifs donc : $a \wedge b = b \wedge r$.

Relation de Bézout

Soient $a, b \in \mathbb{Z}$, Alors :

$$\exists (u, v) \in \mathbb{Z}^2, au + bv = a \wedge b.$$

On a encore :

$$a \wedge b = 1 \Leftrightarrow \exists (u, v) \in \mathbb{Z}^2, au + bv = 1.$$

Théorème de Gauss

Soient $a, b, c \in \mathbb{Z}^*$, alors :

$$\begin{cases} c | ab \\ c \wedge b = 1 \end{cases} \implies c | a$$

Corollaire

Soient $a, b, c, d \in \mathbb{Z}^*$, alors :

$$c \wedge d = 1 \implies ac \wedge bd = a \wedge b.$$

Propositions

Soient $a, b \in \mathbb{Z}^*$ et $n \in \mathbb{N}$,
-) $na \wedge nb = n(a \wedge b)$
-) $a^n \wedge b^n = (a \wedge b)^n$.

$\rightarrow$ Preuve :
-) La 1ère propriété est facile par double divisibilité.
-) On utilise une récurrence sur n :
+) Pour $n = 0$ le résultat est vrai.
+) Si le résultat est vrai pour $n \in \mathbb{N}$, montrons que : $a^{n+1} \wedge b^{n+1} = (a \wedge b)^{n+1}$.
On pose : $a = (a \wedge b)k$ et $b = (a \wedge b)k'$ avec $k \wedge k' = 1$.

Alors on a : $a^{n+1} \wedge b^{n+1} = (a \wedge b)a^n k \wedge (a \wedge b)b^n k' = (a \wedge b)(a^n k \wedge b^n k')$

Puisque $k \wedge k' = 1$ on a : $a^n k \wedge b^n k' = a^n \wedge b^n \overset{\text{HR}}{=} (a \wedge b)^n$.

D'où le résultat.

Proposition

Pour $a, b \in \mathbb{Z}^*$ on a $|ab| = (a \wedge b)(a \vee b)$.

4 Nombres premiers

Proposition : un critère de primalité

Soit $n \geqslant 2$, alors si n n'est pas premier , $\exists p \in \mathbb{P}, p \leqslant \sqrt{n}$ et $p|n$.
Ou aussi : si $\forall d \leqslant \sqrt{n}, d \nmid n$ alors $n \in \mathbb{P}$.

Théorème fondamental

Soit $n \geqslant 2$, alors n s'écrit de façon unique sous la forme : $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$
avec $p_1 < \cdots < p_k \in \mathbb{P}$ et $k, \alpha_1, \cdots, \alpha_k \in \mathbb{N}^*$.
On appelle $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ la décomposition en produit de facteurs premiers de n.

Propositions

Soit $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \geqslant 2$. On note d_n le nombre de diviseurs>0 de n et s_n leur somme.
On pose aussi $\mathcal{D}_n$ l'ensemble des diviseurs positifs de n. Alors on a :
$\mathcal{D}_n = \{p_1^{\beta_1} \cdots p_k^{\beta_k} | 0 \leqslant \beta_i \leqslant \alpha_i \text{ pour } 1 \leqslant i \leqslant k\}$

Alors $d_n = card(\mathcal{D}_n) = \sum_{\beta_1=0}^{\alpha_1} \cdots \sum_{\beta_k=0}^{\alpha_k} 1 = \prod_{i=1}^{k} \sum_{\beta_i=0}^{\alpha_i} 1 = \prod_{i=1}^{k} (\alpha_i + 1)$.

et : $s_n = \sum_{\beta_1=0}^{\alpha_1} \cdots \sum_{\beta_k=0}^{\alpha_k} p_1^{\beta_1} \cdots p_k^{\beta_k} = \prod_{i=1}^{k} \sum_{\beta_i=0}^{\alpha_i} p_i^{\beta_i} = \prod_{i=1}^{k} \frac{1 - p_i^{\alpha_i+1}}{1 - p_i}$

Théorème

$\mathbb{P}$ est infini.

$\rightarrow$ Preuve : Sinon, on note $\mathbb{P} = \{p_1, \cdots, p_n\}$ et on pose $N = p_1 \cdots p_n + 1 \notin \mathbb{P}$.
Alors N admet un diviseur premier qu'on note p_i. Alors $p_i|1$ ce qui est absurde.
Donc $\mathbb{P}$ est infini.

Petit Théorème de Fermat

Soient $n \in \mathbb{N}^*$ et $p \in \mathbb{P}$.
Alors

$$n^p \equiv n[p]$$

Si de plus on a $n \wedge p = 1$ alors d'après Gauss on a : $n^{p-1} \equiv 1[p]$

→ Preuve : Par récurrence sur n.

- Pour $n = 1$ le résultat est vrai.
- Si on a $n^p \equiv n[p]$, alors :

$$\begin{aligned}(n+1)^p &\equiv \sum_{k=0}^{p} \binom{p}{k} n^k [p] \\ &\equiv 1 + n^p + \sum_{k=1}^{p-1} \binom{p}{k} n^k [p] \\ &\overset{\text{H.R}}{\equiv} 1 + n + \sum_{k=1}^{p-1} \binom{p}{k} n^k [p]\end{aligned}$$

Or on a pour $1 \leqslant k \leqslant p-1$: $\binom{p}{k} = \dfrac{p(p-1)\cdots(p-k+1)}{k!}$ donc $p | k! \binom{p}{k}$.
Et on a $p \nmid k!$ (car $k! = 2 \times 3 \cdots \times k$ et $k < p$) et $p \in \mathbb{P}$ donc $p \wedge k! = 1$.
Donc d'après Gauss on a : $p | \binom{p}{k}$. D'où $(n+1)^p \equiv n + 1[p]$.

Exercice 1 :

Soient $a, b, c \in \mathbb{Z}^*$ tels que $b \wedge c = 1$. Montrer que

$$ac \wedge b = a \wedge b.$$

→ Solution : Par double divisibilité.

- On a clairement $a \wedge b | ac \wedge b$.
- Et : $ac \wedge b | ac$ et on a : $b \wedge c = 1$ et $ac \wedge b | b$ donc $(ac \wedge b) \wedge c = 1$.

D'après Gauss on a : $ac \wedge b | a$ donc $ac \wedge b | a \wedge b$.
D'où $ac \wedge b = a \wedge b$.

Exercice 2 :

On sait que $\mathbb{P}$ est infini. Ici on montre que E est infini, où $E = \{p \in \mathbb{P}/p \equiv 1[4]\}$.

1. Soient $x \in \mathbb{N}$ et $p \in \mathbb{P}^+$ impair tel que $x^2 + 1 \equiv 0[p]$.
   Montrer que $p \in E$.
2. On suppose que E est fini. On pose alors $E = \{p_1, ..., p_n\}$.
   (a) On considère $N = (2p_1...p_n)^2 + 1$. Soit p un diviseur premier de N.
   Montrer que p n'est pas dans E.
   (b) Trouver une contradiction. (Utiliser la question1).
3. Conclure.

→ Solution :

1. p premier impair donc $p \equiv 1[4]$ ou $p \equiv 3[4]$. Si par absurde on a : $p \equiv 3[4]$, alors on écrit $p = 4k + 3$. D'après Fermat on a : $x^{4k+3} \equiv x[p]$, or $x^{4k+3} \equiv (x^2)^{2k}x^3 \equiv x^3 \equiv -x[p]$.
Donc $2x \equiv 0[p]$, par Gauss on a : $x \equiv 0[p]$, absurde car $x^2 + 1 \equiv 0[p]$ et $p \in \mathbb{P}$.
Finalement : $p \in E$.
Le reste de l'exercice est facile.

Exercice 3 :

Soient $a, b, n \in \mathbb{N}^*$ tel que $a \equiv b[n]$.

1. Montrer que $a^n - b^n = (a - b)\sum_{k=0}^{n-1} a^k b^{n-k-1}$.
   Si $b \notin \{0, a\}$, trouver une démonstration, autre que la récurrence, à cette question.
2. Déduire que $a^n \equiv b^n[n^2]$.

→ Solution :

1. On a :

$$(a - b)\sum_{k=0}^{n-1} a^k b^{n-k-1} = \sum_{k=0}^{n-1} a^{k+1}b^{n-(k+1)} - a^k b^{n-k} \overset{\text{téléscopage}}{=} a^n - b^n$$

2. Il suffit de montrer que $\sum_{k=0}^{n-1} a^k b^{n-k-1} \equiv 0[n]$.
En effet : $\sum_{k=0}^{n-1} a^k b^{n-k-1} \equiv \sum_{k=0}^{n-1} a^{n-1} \equiv na^{n-1} \equiv 0[n]$.
D'où $a^n \equiv b^n[n^2]$.