Exemples d'équations en arithmétique

126

I/ Equations diophantiennes

Proposition 1: (Identité de Bezout) Soit $(a,b)\in\mathbb{Z}^2$. Il existe un couple $(u,v)\in\mathbb{Z}^2$, tels que $au+bv=a\wedge b$. Un tel couple est appelé un couple de coefficients de Bezout pour a et b

Remarque 2: Un couple de coefficient de Bezout n'est pas unique

Exemple 3: $(-4,3)$ et $(-7,5)$ sont des couples de Bezout pour 2 et 3

Théorème 4: (Bezout) Deux entiers a et b sont premiers entre eux si et seulement si $\exists(u,v)\in\mathbb{Z}^2$, tel que $au+bv=1$

Exemple 5: $\forall n\in\mathbb{Z}$, on a $(n+1)\times 1 + n\times(-1) = 1$ ce qui montre que deux 2 entiers consécutifs sont premiers entre eux.

Théorème 6: (Gauss) Soit $(a,b,c)\in\mathbb{Z}^3$. Si $a\mid bc$ et $a\wedge b=1$ alors $a\mid c$.

Définition 7: On appelle équation diophantienne à 2 inconnues une équation de la forme $ax+by=c$ (E) où $(a,b,c)\in\mathbb{Z}^3$ avec x et y les inconnues dans $\mathbb{Z}^2$

Proposition 8:
* Si c n'est pas divisible par $a\wedge b$, l'équation (E) n'a pas de solution dans $\mathbb{Z}^2$
* Si c est divisible par $a\wedge b$, alors l'équation (E) n'a pas de solution dans $\mathbb{Z}^2$

Proposition 9: Si (x_0,y_0) est une solution particulière de (E). Alors l'ensemble des solutions de (E) est: $S=\{(x_0+b'k, y_0-a'k), k\in\mathbb{Z}\}$ où a' et b' sont: $a=(a\wedge b)a'$, $b=(a\wedge b)b'$

Remarque 10: En remontant l'algorithme d'Euclide, on peut trouver une solution particulière de (E).

Exemple 11: L'équation $29x-11y=1$ admet comme solution $S=\{(-3+11k, -8+29k), k\in\mathbb{Z}\}$.

Exemple 12: En multipliant mon jour de naissance par 12 et mon mois de naissance par 31, j'obtiens par addition 442. Alors je suis né le 11 octobre.

II/ Système de Congruence.

Exemple 13: L'équation $x\equiv 1\ [8]$ admet comme solutions: $\{(1+7k)\mid k\in\mathbb{Z}\}$

Théorème 14: (Reste chinois) Soient $(m,n)\in\mathbb{N}^2$, tel que $m\wedge n=1$ alors $\mathbb{Z}/mn\mathbb{Z}\simeq\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$

Application 15: Le système $\begin{cases} x\equiv 6\ [12] \\ x\equiv 13\ [19] \end{cases}$ admet comme solution $S=\{222+228k \mid k\in\mathbb{Z}\}$

Théorème 16: Soient $m,n\in\mathbb{N}^*$ et $\delta=m\wedge n$ et $\mu=m\vee n$. Alors si $\overline{a}^{\delta}=\overline{b}^{\delta}$ (dans $\mathbb{Z}/\delta\mathbb{Z}$), le système (S) $\begin{cases} x\equiv a\ [m] \\ x\equiv b\ [n] \end{cases}$ à pour solution $\{x_0+k\mu, k\in\mathbb{Z}\}$

où $x_0=\frac{1}{\delta}(avn+bum)$ où $u,v\in\mathbb{Z}$ tq $um+vn=\delta$.

Exemple 17: $\begin{cases} x\equiv 2\ [21] \\ x\equiv 11\ [35] \end{cases}$ n'a pas de solution

Exemple 18: $\begin{cases} x\equiv 3\ [21] \\ x\equiv 10\ [35] \end{cases}$ a pour solution $\{45+105k \mid k\in\mathbb{Z}\}$

D1

Théorème 19 (Dirichlet Faible) Soit $n \geq 1$
L'équation $p \equiv 1 \ [n]$ où p est premier admet une infinité de solutions

III/ Théorème des deux carrés.

Définition 20: On note $\Sigma = \{n \in \mathbb{N} \mid n = a^2 + b^2, a, b \in \mathbb{N}\}$

Exemple 21: $0, 1, 2, 4, 5, 8, 9, 10 \in \Sigma$.

Contre-exemple 22: $3, 6, 7, 11 \notin \Sigma$

Définition 23: On définit l'application $N : \mathbb{Z}[i] \to \mathbb{N}$, $z = a+ib \mapsto |z|$

Proposition 24: $\forall (z, z') \in \mathbb{Z}[i]$, $N(zz') = N(z)N(z')$

Théorème 25: 1) $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

2) L'anneau $\mathbb{Z}[i]$ est euclidien pour le stathme N.

Lemme 26: Soit $p \in \mathbb{N}$ un nombre premier.
On a $p \in \Sigma \iff p$ n'est pas irréductible dans $\mathbb{Z}[i]$.

Lemme 27: Pour $p > 2$ premier, $|\mathbb{F}_p^{*2}| = \frac{p-1}{2}$

$$|\mathbb{F}_p^2| = \frac{p+1}{2}$$

Lemme 28: Soit $p > 2$ premier, $x \in \mathbb{F}_p^{*2} \iff x^{\frac{p-1}{2}} = 1$

Corollaire 29: Soit $p > 2$ premier, alors $-1 \in \mathbb{F}_p^{*2} \iff p \equiv 1 \ [4]$

Théorème 30: Soit $p \in \mathbb{N}$, premier, $p \in \Sigma \iff p = 2$ ou $p \equiv 1 \ [4]$

IV/ Réciprocité quadratique.

Définition 31: Soit p premier impair et $a \in \mathbb{F}_p$. On définit le symbole de Legendre par : $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = \begin{cases} 1 \text{ si } a \text{ est carré dans } \mathbb{F}_p^* \\ -1 \text{ si } a \text{ n'est pas carré dans } \mathbb{F}_p^* \\ 0 \text{ si } a = 0. \end{cases}$

Proposition 32: Soit p premier impair, soit $a \in \mathbb{F}_p^*$. On a
$|\{x \in \mathbb{F}_p, ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right)$

Application 33: Soit $p \geq 5$ premier.
L'équation $6x^2 + 5x + 1 = 0$ admet 2 solutions dans $\mathbb{Z}/p\mathbb{Z}$.

Application 34: L'équation $x^2 + 2x + 2 = 0$ n'a pas de solution dans $\mathbb{Z}/3\mathbb{Z}$

Théorème 35 (Réciprocité quadratique)

Remarque 36: Ce thm donne le lien entre les racines de $x^2 = p$ dans $\mathbb{F}_q$ et $x^2 = q$ dans $\mathbb{F}_p$.

⋮

Application 37: 23 n'est pas un carré dans $\mathbb{Z}/59\mathbb{Z}$.