126 EXEMPLES D'ÉQUATIONS EN ARITHMÉTIQUE.

Définition d'une équation diophantienne [Com98, §12.7, p273]

I. Équations diophantiennes linéaires [Rom17, §10.4, p288]

Cas de l'équation $ax = b$
PGCD d'une famille d'éléments, algorithme d'Euclide, théorème de Bachet-Bézout
Lemmes d'Euclide, de Gauss sur la divisibilité d'un produit
Équation $ax + ny = c$, réécrite $ax \equiv c \mod n$: ensemble des solutions, existence ssi $a \wedge n \mid b$, dans ce cas une solution particulière est donnée par l'identité de Bézout, exemples
Soient $n, m \geq 2$.

Théorème 1. *Soit $a \in \mathbb{N}^*, b \in \mathbb{Z}$. On note $\delta = a \wedge n$ et on écrit $a = \delta a'$ et $n = \delta n'$. L'équation $ax \equiv b \mod n$ a des solutions entières si et seulement si $\delta \mid b$ et dans ce cas, si $b = \delta b'$, les solutions sont les $b'x_0' + kn'$ avec $k \in \mathbb{Z}$ et x_0' est une solution particulière de $a'x \equiv 1 \mod n'$.*

Généralisation à $\sum a_i x_i = b$: calcul par récurrence d'une solution
Équivalent du nombre de solutions S_n de $\sum \alpha_i n_i = n$ [Gou08, §4.4, p249]

II. Systèmes de congruence [Rom17, §10.3-4, p283–290]

Théorème 2. [Théorème des restes chinois]
Soient $n_1, \dots, n_r \in \mathbb{N}$ des entiers distincts. Ces entiers sont premiers entre eux si et seulement si $\mathbb{Z}/n\mathbb{Z}$ et $\prod_{j=1}^r \mathbb{Z}/n_j\mathbb{Z}$ sont isomorphes, où $n = \prod_{j=1}^r n_j$. Plus précisément, l'application $\phi : \overline{k}_n \longmapsto (\overline{k}^{n_i})_{1 \leq i \leq r}$ est un isomorphisme d'anneaux.

Exemple 3. $\mathbb{Z}/4\mathbb{Z}$ n'est pas isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.

Théorème 4. *L'isomorphisme inverse est donné par $(\overline{k_i}^{n_i})_{1 \leq i \leq r} \longmapsto \overline{\sum_{j=1}^r k_j u_j \frac{n}{n_j}}^n$ où l'on a choisit $(u_j)_{1 \leq j \leq r}$ tels que $\sum_{j=1}^r u_j \frac{n}{n_j} = 1$.*

Soient $n, m \geq 2$.

Application 5. Soit $a, b \in \mathbb{Z}$ et $(\mathscr{S})$ le système d'équations $\begin{cases} x \equiv a \mod n \\ x \equiv b \mod m \end{cases}$ d'inconnue $x \in \mathbb{Z}$. Si $n \wedge m = 1$, alors

- on cherche une relation de Bézout $un + vm = 1$ avec $u, v \in \mathbb{Z}$,
- on a alors une solution particulière de $\mathscr{S}$: $x_0 = unb + vma$,
- les solutions de $\mathscr{S}$ sont les $(x_0 + knm)_{k \in \mathbb{Z}}$.

Exemple 6. Les solutions de $\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 4 \mod 5 \end{cases}$ sont les $(14 + 15k)_{k \in \mathbb{Z}}$.

III. Nombres premiers et équations diophantiennes

Théorème de Dirichlet (faible) : existence d'un nombre infini de nombres premiers d'une certaine forme

III. A. Réduction [Rom17, §13.6-7, p429–436] [Per96, §3.2, p72–76]

Soit $p \in \mathcal{P}$. On peut regarder l'équation modulo p.
S'il n'y a pas de solution dans $\mathbb{Z}/p\mathbb{Z}$, il n'y en a pas non plus sur $\mathbb{Z}$.
Soit $p \in \mathcal{P}$. On note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$, puis $\mathbb{F}_p^2 = \{x^2 \mid x \in \mathbb{F}_p\}$ et $\mathbb{F}_p^{*2} = \mathbb{F}_p^2 \cap \mathbb{F}_p^*$.

Proposition 7. *Si $p = 2$, alors $\mathbb{F}_p^2 = \mathbb{F}_p$. Sinon, on a $\left|\mathbb{F}_p^2\right| = \frac{p+1}{2}$.*

On suppose dans la suite p impair.

Lemme 8. *On a $x \in \mathbb{F}_p^{*2} \iff x^{\frac{p-1}{2}} = 1$.*

Exemple 9. Dans $\mathbb{Z}/7\mathbb{Z}$, 2 est un carré mais par 3.

On aimerait savoir rapidement si un entier a donné est un carré modulo p, donc savoir si $x^2 \equiv a \mod p$ admet ou non une solution entière.

Définition 10. [Symbole de Legendre]
Soit $a \in \mathbb{Z}$, on appelle symbole de Legendre (de a modulo p) l'entier :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } x^2 \equiv a \mod p \text{ est résoluble et } p \nmid a \\ 0 & \text{si } p \mid a \\ -1 & \text{sinon} \end{cases}$$

Proposition 11. *On a $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$ pour tout $a \in \mathbb{Z}$.*

Exemple 12. -1 est un carré modulo p si et seulement si $p \equiv 1 \mod 4$. Donc $x^2 + 1 = p$ n'a pas de solution pour $p \equiv 3 \mod 4$.

Proposition 13. $\left(\frac{a}{p}\right) = \left(\frac{a+kp}{p}\right)$ *pour tout* $a, k \in \mathbb{Z}$. *On peut donc définir* $\overline{x} \in \mathbb{F}_p \longmapsto \left(\frac{x}{p}\right)$. *C'est l'unique morphisme de groupes non trivial de* $(\mathbb{F}_p^*, \times)$ *vers* $(\{\pm 1\}, \times)$.

Application 14. Pour $a \in \mathbb{Z}$, le nombre de solutions de $x^2 = \overline{a}$ dans $\mathbb{F}_p$ est $1 + \left(\frac{a}{p}\right)$.

Application 15. Pour $a, b \in \mathbb{F}_p^*$ et $c \in \mathbb{F}_p$, $ax^2 + by^2 = c$ admet des solutions dans $\mathbb{F}_p$.

Exemple : $x^2 + y^2 = pz^2$ selon $p \mod 4$ [Com98, §12.7, p275]

Théorème 16. [Loi de réciprocité quadratique]
Soient $p \neq q$ *des nombres premiers impairs. Alors* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Proposition 17. *Pour* p *premier impair, on a* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. *Ainsi* 2 *est un carré modulo* p *si et seulement si* $p \equiv \pm 1 \mod 8$.

On peut donc calculer $\left(\frac{n}{p}\right)$ pour tout entier n.

Exemple 18. $\left(\frac{26}{307}\right) = \left(\frac{2}{307}\right)\left(\frac{13}{307}\right) = -(-1)^{\frac{13-1}{2}\frac{307-1}{2}}\left(\frac{307}{13}\right) = -\left(\frac{8}{13}\right) = -\left(\frac{2}{13}\right)\left(\frac{4}{13}\right) = -1$
Ainsi 26 n'est pas un carré modulo 307.

$x^2 + py = r$ avec p premier impair er $p \nmid r$, alors on a une solution si et seulement si $\left(\frac{q}{p}\right) = 1$ et dans ce cas on a une paramétrisation de l'ensemble des solutions

IV. Équations diophantiennes non linéaires

IV. A. Exemples de résolutions

[Com98, §12.7, p273] [FGN07, §4.39, p167]

Solutions de $x^2 + y^2 = z^2$
Méthode de descente infinie, exemple de $x^4 + y^4 = z^2$ ou z^4
Autre exemple [FGN07, §4.38, p165]

Théorème 19. [Théorème de Sophie Germain]
Soit p *un nombre premier impair tel que* $q = 2p + 1$ *est premier. Alors il n'existe pas de triplet* $(x, y, z) \in \mathbb{Z}^3$ *tel que* $p \nmid xyz$ *et* $x^p + y^p + q^p = 0$.

Théorème de Fermat

IV. B. L'anneau des entiers de Gauss

[Per96, §2.3, p50] [Rom17, §9.4.3, p263]

Définition 20. On note $\mathbb{Z}[i] = \{a + ib \,|\, a, b \in \mathbb{Z}\}$ l'ensemble des entiers de Gauss.

Proposition 21. *Muni du stathme* $N(a + ib) = a^2 + b^2$, $\mathbb{Z}[i]$ *est euclidien.*

Proposition 22. $\mathbb{Z}[i]^\times = N^{-1}(\{1\}) = \{\pm 1, \pm i\}$.

On définit $\Sigma = \{n \in \mathbb{N} \,|\, \exists a, b \in \mathbb{N} \,|\, n = a^2 + b^2\}$. On cherche à quelle(s) condition(s) $n \in \Sigma$.

Exemple 23. $0, 1, 2, 4, 5, 8, 9, 10 \in \Sigma$ mais pas $3, 6, 7, 11$.

Lemme 24. Σ *est stable par produit.*

Lemme 25. *Si* $p \in \mathcal{P}$, *alors* $p \in \Sigma \iff p \equiv 1, 2 \mod 4$.

Théorème 26. [Théorème des deux carrés de Fermat]
$n \in \Sigma$ *si et seulement si pour tout* $p \in \mathcal{P}$ *tel que* $p \mid n$ *et* $p \mid 3 \mod 4$, *alors* $2 \mid v_p(n)$.

Proposition 27. *Les irréductibles de* $\mathbb{Z}[i]$ *sont :*
- *les* $p \in \mathcal{P}$ *tels que* $p \equiv 3 \mod 4$,
- *les* $a + ib$ *tels que* $a^2 + b^2 \in \mathcal{P}$.

Généralisation : anneaux quadratiques [Duv07, Ch5, p47]
Ou encore théorème des quatre carrés de Lagrange : tout nombre entier est somme de 4 carrés. [Duv07, §6.6, p73] [FGN07, §4.36, p162]

QUESTIONS

Q On s'intéresse à $y^2 = x^3 - x$ et au nombre de points de cette courbe sur $\mathbb{F}_p$. On note N_p le nombre de solutions. Montrer que $N_p = p + \sum_{x\in\mathbb{F}_p} \left(\frac{x^3-x}{p}\right)$. Calculer N_7. Montrer en fait que pour $p \equiv 3 \mod 4$, on a $N_p = p$.

R On utilise le fait que $\mathrm{card}(\{y^2 = a \,|\, y \in \mathbb{F}_p\}) = 1 + \left(\frac{a}{p}\right)$. On a :

$$N_p = \sum_x \mathrm{card}(\{y^2 = x^3 - x\} \mid y \in \mathbb{F}_p) = \sum_x 1 + \left(\frac{x^3-x}{p}\right) = p + \sum_{x\in\mathbb{F}_p} \left(\frac{x^3-x}{p}\right)$$

Pour calculer N_7, on calcule les $\left(\frac{x^3-x}{7}\right)$ pour $x \in \mathbb{F}_7$, on obtient dans l'ordre pour $x = 0, \dots, 6$: $0, 1, -1, -1, 1, 1, -1$, d'où $N_7 = 7$.
Si $p \equiv 3 \mod 4$, on a pour f impaire : $\left(\frac{f(-x)}{p}\right) = \left(\frac{-f(x)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{f}{p}\right) = -\left(\frac{f(x)}{p}\right)$ ce qui assure que la somme est nulle dans la formule de N_p, et ainsi $N_p = p$.

Q Que dire de $f : x \longrightarrow \frac{1+x}{1-x}$ pour $x \in \mathbb{F}_p \setminus \{1\}$.

R L'application est-elle injective ? si $f(x) = f(y)$, on a $(1+x)(1-y) = (1-x)(1+y)$ donc $2x = 2y$ puis $x = y$ si $p \geq 3$. Supposons $p \geq 3$. L'application est injective et son image est $\mathbb{F}_p$ privée d'un point : -1 puisque $1 + x = x - 1$ n'a pas de solution.

Q En déduire le nombre de solutions de $x^2 + y^2 = 1$?

R Écrivons $x^2 = 1 - y^2 = \frac{1+y}{1-y}(1-y)^2$. Donc :

$$N_p = p + \sum_y \left(\frac{1-y^2}{p}\right) = p + 0 + \sum_{y\neq 1} \left(\frac{\frac{1+y}{1-y}}{p}\right) = p + \sum_{z\neq -1} \left(\frac{z}{p}\right) = p - \left(\frac{-1}{p}\right)$$

BIBLIOGRAPHIE

[Com98] F. Combes : *Algèbre et géométrie*. Bréal, 1998.

[Duv07] D. Duverney : *Théorie des nombres*. Dunod, 2007.

[FGN07] S. Francinou, H. Gianella et S. Nicolas : *Oraux X-ENS - Algèbre 1*. Cassini, 2007.

[Gou08] X. Gourdon : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[Per96] D. Perrin : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. Rombaldi : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.