126 : éq en arithmétique

Déf$_1$: éq dioph.] [CON] p. 274

Rem$_2$: Dans cette leçon on va s'intéresser à des éq dioph, système d'éq dioph. ; et leur résolution modulaire également.

I) Équations linéaires, entières :

trouver un meilleur titre...

A) Éq. linéaires en ~~1 ou~~ 2 variables sur $\mathbb{Z}$:

THM$_3$: Division eucli sur $\mathbb{Z}$

Rem$_4$: $\mathbb{Z}$ euclidien, donc principal et donc factoriel :

THM$_5$: Unicité déc de n en facteurs 1er

THM$_6$: Bézout

THM$_7$: Gauss

Cor$_8$: Euclide

Prop$_9$: $a,b \in \mathbb{Z}\setminus\{0\}$, $c \in \mathbb{Z}$. $ax+by=c$ a des solutions ssi $\text{pgcd}(a,b) \mid c$

Méth$_{10}$: Pour résoudre l'éq précédente, on se ramène au cas où $c=1$ et $\text{pgcd}(a,b)=1$, on trouve (x_0,y_0) sol particulière via une relat de Bézout, puis par an-synth, on montre que $S=\{(x_0+bk, y_0-ak) \mid k \in \mathbb{Z}\}$

Ex$_{11}$: (E) $931x+513y=19$, $S_{(E)}=\{(-11+27k, 20-49k) \mid k \in \mathbb{Z}\}$.

[LiR] p. 290 ~

B) Éq. lin à n variables : ← trouver mieux comme partie...

Prop : $a_1,\dots,a_p \in (\mathbb{N}^*)^p$, on a (par récurrence) $\text{pgcd}(a_1,\dots,a_p) = \text{pgcd}(\text{pgcd}(a_1,\dots,a_{p-1}), a_p)$

Et : $\exists u_1,\dots,u_p \in \mathbb{Z}$ tq $a_1u_1+\dots+a_pu_p = \text{pgcd}(a_1,\dots,a_p)$

Rem : C'est une gén. de l'identité de Bézout

[LiR] exos

Prop : Si les a_i sont 1ers entre eux dans leur ensemble, $n \in \mathbb{N}$, on note S_n le nbre de sol $(n_1,\dots,n_p) \in \mathbb{N}^p$ de $a_1n_1+\dots+a_pn_p = n$.

Alors $S_n \underset{n\to+\infty}{\sim} \frac{n^{p-1}}{a_1\dots a_p\,(p-1)!}$

(pas facile mais pour du contexte...)

[GOU] An. p 261 exo 7

Rem : + généralement, si on a n éq lin à n variables, on peut l'écrire $AX=B$ où $A,B \in \mathcal{M}_n(\mathbb{Z})$. Et A inversible dans $\mathbb{Z}$ $\Leftrightarrow \det(A) = \pm 1$

Donc on a ~~des~~ une unique solution entière $\Leftrightarrow \det(A) = \pm 1$.

↳ + mettre un exemple ; dire que la sol s'obtient comme avec le pivot

II) Équations modulaires :

A) Système de congruences :

THM : Restes Chinois (avec réciproque)

[GOU]

Rem : Reformulat° par 2 entiers

Appli : permet de résoudre des système de congruences :

ex : si $m \wedge n = 1$, $a,b \in \mathbb{Z}$ $\begin{cases} x \equiv a\ [m] \\ x \equiv b\ [n] \end{cases}$, on cherche une relat de Bez entre m et n : $um+vn=1$ et une sol part est $x = a+um(b-a)$

+ Généralement

[ROM] Prop : méthode gén. ROM (on peut tjr réduire)

Ex $\begin{cases} x \equiv 2\ [4] \\ x \equiv 3\ [5] \\ x \equiv 1\ [9] \end{cases}$

Rem : si les n_i ne sont pas 1er entre eux c'est + délicat :

ex (E) $\begin{cases} x \equiv a_1\ [n_1] \\ x \equiv a_2\ [n_2] \end{cases}$ où $S = n_1 \wedge n_2 \geq 2$. (E) a des sol $\Leftrightarrow S \mid a_2-a_1$ (facile) + ens des sol° (et si on a + que 2 lignes ???)

B) Résidus quadratiques : $p \in \mathcal{P}$, $p \geq 2$

Déf : Résidu quad

Rem : Résolut° de $ax^2+bx+c=0$ dans $\mathbb{F}_p$ revient à chercher si $\Delta = \bar{b}^2 - 4\bar{a}\bar{c}$ est un carré de $\mathbb{F}_p$ ou non

[ROM] THM : nbre de carrés dans $\mathbb{F}_p^*$ + $\bar{x}$ carré $\Leftrightarrow x^{\frac{q-1}{2}} = 1$ (readable aussi dans $\mathbb{F}_{p^n}$...)

Cor : x de 2 carré = carré ... (cor ROM)

Déf : symbole Legendre

THM : $\left(\frac{\bar{a}}{p}\right) = a^{\frac{p-1}{2}}$ dans $\mathbb{F}_p^\times$, morphisme...

[CAL] Lemme $\left|\left\{x \in \mathbb{F}_p \mid ax^2=1\right\}\right| = \left(\frac{a}{p}\right)+1$

[LiR] THM : Loi de récip quad.

Appli : ex de calcul [GOZ] ou [LIR]

C) Éq. polyn. et réd. mod p :

[PER] THM : Eisenstein (sur $\mathbb{Q}[X]$ puis $\mathbb{Z}[X]$)

THM : Réduct° : $\bar{P}$ irréd sur $\mathbb{F}_p[X]$ $\Rightarrow$ P irréd. sur $\mathbb{Q}$ puis $\mathbb{Z}$...

Ex : $X^3+462X^2+2433X-67691$ irréd sur $\mathbb{Z}$

126 suite

III) Équations non linéaires, méthodes de résolution :

A) Descente infinie : COM / LIR

Méthode : Pour montrer qu'une éq dioph. n'a pas de solution non triviale : par l'absurde, on ~~suppo~~ considère une solution non triviale avec un paramètre minimal, on arrive à une contradiction en construisant une autre solut° de paramètre plus petit.

Appli : $x^4+y^4=z^2$ et $x^4+y^4=z^4$ n'ont pas de solution non triviale. (sur $\mathbb{Z}$) [pas facile et utilise les sol de $x^2+y^2=z^2$ d'écrivent... prop 1]

Rem : Wiles démontre en 1995 (grâce à la théorie des fct elliptiques) que : $\forall n \geq 3$, $x^n+y^n=z^n$ n'a pas de solution non triviale.

B) Exemple d'utilisation d'un anneau particulier pour la résolut° d'éq dioph

→ Tout ce qu'il faut pour dév $x^2+2=y^3 \rightarrow \mathbb{Z}[i\sqrt{2}]$

Rem : Introduire des anneaux du type $\mathbb{Z}[x]$ est classique pour résoudre des éq. de ce type. Comme l'éq de Pell-Fermat $x^2-dy^2=1$ ($d \in \mathbb{N}^*$ non carré). On introduit $\mathbb{Z}[\sqrt{d}]$ Cette éq. a une infinité de sol car $\mathbb{Z}[\sqrt{d}]^\times$ est infini.

C) Un autre exemple : les entiers de Gauss :

Déf $\mathbb{Z}[i]$ + N + N multiplicative

Prop : $\mathbb{Z}[i]^\times = \{\pm 1\}$

Prop : $\mathbb{Z}[i]$ euclidien

Lemme : $-1 \in \mathbb{F}_p^{\times 2} \Leftrightarrow p=1[4]$ ou $p=2$

Déf : Σ + rem Σ stable par $\times$

Rem : On cherche les élémt de Σ ← peut-être à mettre au déb. pr justifier cette partie

Prop : $p \in \mathbb{N}$ 1er, $p \in \Sigma \Leftrightarrow p$ ~~réd~~ $=2$ ou $p \equiv 1(4)$ $\Leftrightarrow p$ réduct. dans $\mathbb{Z}[i]$ (Dév 2)

THM : $n \in \mathbb{N}^*_{\geq 2}$, $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$. $n \in \Sigma \Leftrightarrow \forall p \equiv 3(4)$, $v_p(n)$ pair

[COM] [LIR] [PER] P 56 S 8

Réf :

[LIR] - Liret - Arithmétique ← I + III B

([GOU_An]) ([GOU_Alg] = [GOU]) } on peut s'en passer

[ROM] ← par sujet de congru et $\mathbb{F}_p^{\times 2}$

[CAL] ← pr dév 1

[COM] - Combes III A

[PER] ← III C) + I B