[PE] Rq 19: $\mathbb{Z}/p^\alpha\mathbb{Z}$ n'est pas le corps à p^α éléments et $(\mathbb{F}_{p^\alpha})^\times$ est cyclique.

[PE] Prop 20: $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$, $(\mathbb{Z}/2^2\mathbb{Z})^\times = \{-1, 1\} \simeq \mathbb{Z}/2\mathbb{Z}$

Pour $\alpha \geq 3$, $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$

[PE] Rq 21: Pour $\alpha \geq 3$, $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ n'est pas cyclique.

Prop 22: (Lemme chinois)
Si p et q sont des entiers premiers entre eux, on a un isomorphisme:
$\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$

Contre ex 23: $\mathbb{Z}/4\mathbb{Z} \not\simeq (\mathbb{Z}/2\mathbb{Z})^2$

Prop 24: Soit n un entier, $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec les p_i premiers distincts et les $\alpha_i \in \mathbb{N}^*$. Alors:
1) On a un isomorphisme d'anneaux: $\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$
2) On a un isomorphisme de groupes: $(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$

App 25: Résoudre le système de congruence: $\begin{cases} x \equiv 2 [3] \\ x \equiv 3 [5] \\ x \equiv 2 [7] \end{cases} \Longrightarrow x \equiv 23 [105]$.

II – Arithmétique dans $\mathbb{Z}$

1 – Nombres premiers.

[CO] Thm 26: (Théorème d'Euler)
Soient a et n deux entiers naturels non nuls tels que $a \wedge n = 1$
Alors: $a^{\varphi(n)} \equiv 1 [n]$

[CO] Thm 27: (Petit théorème de Fermat)
Soient p un nombre premier et $a \in \mathbb{N}^*$ non divisible par p.
Alors: $a^{p-1} \equiv 1 [p]$

[CO] App 28: Trouver le chiffre des unités de $N = 27^{1995}$. Il s'agit de 3.

[GO] App 29: Chiffrement RSA

[GO] Def 30: Un entier $n \geq 2$ est appelé nombre de Carmichael si n n'est pas un nombre premier et si pour tout a, $a^n \equiv a [n]$

[GO] Prop 31: Si $n = p_1 \cdots p_k$ où les p_i sont des nombres premiers distincts et si $p_i - 1 | n - 1$ pour tout i, alors n est un nombre de Carmichael.

Ex 32: Le plus petit nombre de Carmichael est $561 = 3 \times 11 \times 17$ [GO]

Thm 33: (Théorème de Wilson) [RB]
$p \geq 2$ est un nombre premier ssi $(p-1)! \equiv -1 [p]$

Lemme 34: (Lemme de Gauss) [PE]
Si $a | bc$ et $a \wedge b = 1$ alors $a | c$.

Thm 35: (Chevalley-Warning)
Soient p un nombre premier, $r \in \mathbb{N}^*$. On note $q = p^r$. Soit A ensemble fini tel que $\forall a \in A$, $f_a \in \mathbb{F}_q[X_1, \dots, X_n]$, et $\sum_{a \in A} \deg f_a < n$.
On note $V = \{(x_1, \dots, x_n) \in \mathbb{F}_q^n$ tels que $\forall a \in A, f_a(x_1, \dots, x_n) = 0\}$
Alors: $\# V \equiv 0 [p]$.

DEV 1

Thm 36: (Erdös-Ginzburg-Ziv).
Soit p un nombre premier, soient $a_1, \dots, a_{2p-1} \in \mathbb{Z}$.
Parmi ces $(2p-1)$ nombres entiers, on peut en trouver p dont la somme est divisible par p.

2 – Carrés et résidus quadratiques.

Def 37: Pour $q = p^n$ fixé (p premier et $n \in \mathbb{N}^*$), on a: [RB]
$(\mathbb{F}_q)^2 = \{x \in \mathbb{F}_q$ tel que $\exists y \in \mathbb{F}_q, y^2 = x\}$ et $(\mathbb{F}_q^*)^2 = \mathbb{F}_q^* \cap (\mathbb{F}_q)^2$

Prop 38: Si $p = 2$, on a $(\mathbb{F}_q)^2 = \mathbb{F}_q$ [RB]
Si $p > 2$, on a $|(\mathbb{F}_q)^2| = \frac{q+1}{2}$ et $|(\mathbb{F}_q^*)^2| = \frac{q-1}{2}$.

Prop 39: (Critère d'Euler) [RB]
$x \in (\mathbb{F}_q^*)^2 \iff x^{\frac{q-1}{2}} \equiv 1 [q]$

Ex 40: 3 n'est pas un carré dans $\mathbb{F}_7$. [RB]

Thm (admis) 41: (Loi de réciprocité quadratique) [RB]
Soient p, q 2 entiers premiers impairs distincts.
Alors: $p^{\frac{q-1}{2}} q^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

App 42: La résolution d'équations de congruences du type $ax^2 + bx + c \equiv 0 [p]$ où $a, b, c \in \mathbb{Z}$ équivaut à résoudre sur le corps $\mathbb{Z}/p\mathbb{Z}$ l'équation $\bar{a}X^2 + \bar{b}X + \bar{c} = \bar{0}$. L'équation a des solutions si $\Delta = \bar{b}^2 - 4\bar{a}\bar{c}$ est un carré. [CO]

120 - Anneaux $\mathbb{Z}/n\mathbb{Z}$, applications.

Cadre : $n \in \mathbb{N}^*$, p nombre premier et on a $p^n = q$ dans la suite.

I - Structure de $\mathbb{Z}/n\mathbb{Z}$

1) Le groupe $\mathbb{Z}/n\mathbb{Z}$ [R-B]

Def 1 : Le groupe $\mathbb{Z}/n\mathbb{Z}$ est le quotient de $\mathbb{Z}$ par le sousgroupe distingué $n\mathbb{Z}$. Le morphisme canonique $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ fait fait correspondre un entier x à sa classe $\bar{x}$ modulo n. $\bar{x} = x + n\mathbb{Z}$.

Rq2 : Le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique, abélien, d'ordre n.

Prop 3 : Tout groupe monogène est isomorphe : soit à $(\mathbb{Z},+)$, soit à $(\mathbb{Z}/n\mathbb{Z},+)$ pour un entier $n>0$. En particulier, tout groupe cyclique est isomorphe à un groupe $(\mathbb{Z}/n\mathbb{Z},+)$ avec $n>0$.

[CO] **Ex 4 :** Le groupe multiplicatif $U_n = \{1, \xi, \dots, \xi^{n-1}\}$ des racines n-ièmes de l'unité dans $\mathbb{C}$, est engendré par $\xi = \exp\left(\frac{2i\pi}{n}\right)$. Il est cyclique d'ordre n et on a $U_n \simeq \mathbb{Z}/n\mathbb{Z}$.

Prop 5 : Tout sous groupe d'un groupe cyclique est cyclique. Plus précisément, soit n un entier supérieur à 1.

1) Tout sous groupe de $\mathbb{Z}/n\mathbb{Z}$ est cyclique engendré par la classe $\bar{b}$ d'un diviseur b de n. Ce sous groupe est d'ordre $a = \frac{n}{b}$.
2) Soit $a>0$ un diviseur de n, $b = \frac{n}{a}$. Il existe alors un unique sous groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre a. Ce sous groupe est engendré par la classe de b modulo n ; il est formé de l'ensemble des éléments de $\mathbb{Z}/n\mathbb{Z}$ dont l'ordre divise a.

Ex 6 : sous groupe de $\mathbb{Z}/6\mathbb{Z}$: $6 = 3\times 2$, d'où $H_1 = \{\bar{0}\}$ d'ordre 1, $H_2 = \{\bar{0}, \bar{3}\}$ d'ordre 2 et $H_3 = \{\bar{0}, \bar{2}, \bar{4}\}$ d'ordre 3 et $H_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ d'ordre 6.

[CO] **Prop 7 (Admis) :** Soit G groupe abélien fini d'ordre $n \geq 2$. Il existe des entiers q_1 supérieur ou égal à deux, q_2 multiple de q_1, ..., q_k multiple de q_{k-1}, uniques tels que G soit isomorphe à $(\mathbb{Z}/q_1\mathbb{Z}) \times \dots \times (\mathbb{Z}/q_k\mathbb{Z})$.

2) L'anneau $\mathbb{Z}/n\mathbb{Z}$ [R-B]

Le sous groupe $n\mathbb{Z}$ de $\mathbb{Z}$ étant aussi un idéal, le groupe $(\mathbb{Z}/n\mathbb{Z},+)$ est muni canoniquement d'une structure d'anneau induite par celle de $\mathbb{Z}$.

Prop 8 : Soient $n>1$ et a deux entiers, $\bar{a}$ la classe de a modulo n. Les conditions suivantes sont équivalentes :
1) $a \wedge n = 1$
2) $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ où $(\mathbb{Z}/n\mathbb{Z})^\times$ est l'ensemble des inversibles de $\mathbb{Z}/n\mathbb{Z}$.
3) $\bar{a}$ engendre le groupe $(\mathbb{Z}/n\mathbb{Z},+)$

Déf 9 : Pour $n \geq 2$, on note $\varphi(n)$ le nombre de générateurs distincts du groupe $\mathbb{Z}/n\mathbb{Z}$ ($\varphi(n)$ est aussi l'ordre de $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$). Il s'agit du nombre d'entiers a tels que $1 \leq a < n$ et $a \wedge n = 1$. On pose par convention $\varphi(1) = 1$. La fonction φ s'appelle l'indicatrice d'Euler.

Prop 10 : Soit $n = \prod_{i=1}^{k} p_i^{v_i}$, les p_i étant des nombres premiers et les v_i des nombres entiers positifs, on a : $\varphi(n) = \prod_{i=1}^{k} (p_i - 1) p_i^{v_i - 1}$ et $\varphi(p_i^{v_i}) = (p_i - 1) p_i^{v_i - 1}$.

Ex 11 : Le nombre de générateurs de $\mathbb{Z}/6\mathbb{Z}$ est $\varphi(6) = \varphi(2\times 3) = 2$. Ce sont $\bar{1}$ et $\bar{5}$ puisque ce sont les seuls entiers entre 1 et 5 à être premier avec 6.

Prop 12 : Soit G groupe cyclique d'ordre n. Alors $\forall d > 0$ tel que $d \mid n$, il y a dans G exactement $\varphi(d)$ éléments d'ordre d. [CO]

Ex 13 : dans U_4, il y a un élément d'ordre 1 ($\varphi(1) = 1$) qui est 1, un élément d'ordre 2 ($\varphi(2) = 1$) qui est $e^{i\pi}$ et deux éléments d'ordre 4 ($\varphi(4) = 2$) qui sont $e^{i\frac{\pi}{2}}$ et $e^{i\frac{3\pi}{2}}$.

Coro 14 : Soit $n \in \mathbb{N}^*$, la fonction φ vérifie la relation : $\sum_{d \mid n} \varphi(d) = n$.

Coro 15 : Soit G groupe cyclique d'ordre n. Le groupe $\mathrm{Aut}(G)$ est d'ordre $\varphi(n)$ et ses éléments sont les applications $\alpha_k : x \mapsto x^k$ où $k \in [\![0, n-1]\!]$ est premier avec n. [CO]

Coro 16 : L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est un nombre premier. On note alors $\mathbb{F}_n$ ce corps.

Lemme 17 : Si p est un nombre premier, on a un isomorphisme : [PE]
$(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$

Prop 18 : Si p est un nombre premier supérieur ou égal à 3 et α un entier supérieur ou égal à 2, on a : [PE]

$$(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/\varphi(p^\alpha)\mathbb{Z} \simeq \mathbb{Z}/(p-1)p^{\alpha-1}\mathbb{Z}$$

RB] **Coro 43:** Soient $p>2$ nombre premier, n un entier et $q=p^n$.
Alors $(-1)\in(\mathbb{F}_q)^2 \iff q\equiv 1[4]$.

:O] **App 44:** Soit p premier congru à 3 modulo 4, alors $x^2+y^2=pz^2$ n'a pas de solutions non triviales.

:O] **App 45:** Il existe une infinité de nombres premiers de la forme $4m+1$.

RB] **Def 46:** $a\in\mathbb{Z}$ est dit résidu quadratique modulo n si l'image $\bar{a}\in\mathbb{Z}/n\mathbb{Z}$ est un carré.

RB] **Ex 47:** Dans $\mathbb{Z}/6\mathbb{Z}$, on a

x	0	1	2	3	4	5
x^2	0	1	4	3	4	1

de sorte que a est un résidu quadratique modulo 6 si et seulement si $a\equiv 0,1,3,4[6]$.

Thm 48: (Théorème des deux carrés)
Soit $p\in\mathbb{N}$ un nombre premier. On a alors:
$p\in\Sigma=\{n\in\mathbb{N} \text{ tel que } n=a^2+b^2;\ a,b\in\mathbb{N}\} \iff p=2$ ou $p\equiv 1[4]$.

Thm 49: Soit $n\in\mathbb{N}^*$, $n\neq 1$, on décompose n en facteurs premiers: $n=\prod_{p\in\mathcal{P}} p^{v_p(n)}$. Alors on a : $n\in\Sigma \iff v_p(n)$ est pair pour $p\equiv 3[4]$.

III - Polynômes irréductibles

1 - Irréductibilité dans $\mathbb{Z}/p\mathbb{Z}[X]$ [GOZ]

Thm 50: Soient p premier, $n\in\mathbb{N}^*$. Notons $q=p^n$.
Alors on a $\mathbb{F}_q=\mathbb{F}_p[X]/(\pi)$ où π est un polynôme irréductible quelconque de degré n sur $\mathbb{F}_p$.

Thm 51: Soient p premier, $n\in\mathbb{N}^*$. Notons $q=p^n$.
Pour $j\in\mathbb{N}^*$, on note $K(p,j)$ l'ensemble des polynômes irréductibles unitaires de degré j sur $\mathbb{F}_p$.
Alors $X^{p^n}-X=\prod_{d|n}\prod_{Q\in K(p,d)} Q(X)$

Thm 52: Soient p premier, $n\in\mathbb{N}^*$. Notons $q=p^n$. Pour $j\in\mathbb{N}^*$ on note $I(p,j)=\mathrm{Card}(K(p,j))$ le nombre de polynômes irréductibles unitaires de degré j sur $\mathbb{F}_p$. Alors $p^n=\sum_{d|n} d\,I(p,d)$

Ex 53: Factorisation de X^8-X sur $\mathbb{F}_2[X]$:
$X^8-X=X(X-1)(X^3+X+1)(X^3+X^2+1)$.

Thm 54: Soit $P\in\mathbb{F}_p[X]$, de degré $n>0$. Alors P est irréductible sur $\mathbb{F}_p$ si et seulement si P n'a pas de racines dans les extensions K de $\mathbb{F}_p$ qui vérifient $[K:\mathbb{F}_p]\leq\frac{n}{2}$. [PE]

Ex 55: X^4+X+1 est irréductible sur $\mathbb{F}_2$. [PE]

2 - Irréductibilité dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$. [PE]

Prop 56: $P(X)$ est irréductible sur $\mathbb{Z}$ ssi il l'est sur $\mathbb{Q}$ et si son contenu est 1 où le contenu de P est le pgcd de ses coefficients.

Thm 57:
Soit A anneau factoriel et $K=\mathrm{Fr}(A)$. Soit I un idéal premier de A et $B=A/I$ qui est un anneau intègre de corps de fraction L. Soit $P(X)=a_nX^n+\dots+a_0$ un polynôme de $A[X]$ et $\bar{P}$ sa réduction modulo I. On suppose $\bar{a}_n\neq 0$ dans B.
Alors si $\bar{P}$ est irréductible sur B ou L, P est irréductible sur K

3 - Polynômes cyclotomiques [PE]

K corps, $n\in\mathbb{N}^*$, on considère $P_n(X)=X^n-1$. On note K_n le corps de décomposition de P_n sur K, $\mu_n(K_n)$ l'ensemble des racines n-ième de l'unité sur K_n et $\mu_n^*(K_n)$ celui des racines primitive n-ième de l'unité.

Def 58: le n-ième polynôme cyclotomique $\Phi_{n,K}\in K_n[X]$ est:
$\Phi_{n,K}(X)=\prod_{\xi\in\mu_n^*(K_n)}(X-\xi)$

Prop 59: $X^n-1=\prod_{d|n}\Phi_d(X)$

Thm 60: $\Phi_n(X)$ est irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$.

Biblio : F. Combes, Algèbre et géométrie [CO]
I. Gozard, Théorie de Galois [GOZ]
D. Perrin, Cours d'Algèbre. [PE]
J.J. Risler - P. Boyer, Groupes, anneaux, corps [R-B]
Gourdon, Algèbre [GO]

Plan I) Structure de groupe., ppu
→ gr
→ anneau
II) Arithmétique
1) Nb premier
2) Carrés, residus quad
III) Poly irre $\mathbb{F}_q[X]$
$\mathbb{Z}[X]$
$\mathbb{Q}[X]$...

Q° : Enoncer thm Lagrange.
A pp° Thm Chinois : compter en armée

Théorèmes de Chevalley-Warning et d'Erdös-Ginzburg-Ziv

Leçons : 120[62], 123, 142, 144, 121, 126, 190

426

[Ser], paragraphe 1.2
[Zav], problème 7.II

Théorème (*Chevalley-Warning*)

Soient p un nombre premier, $r \in \mathbb{N}^*$; on note $q = p^r$.
Soient $f_1, \dots, f_s \in \mathbb{F}_q[X_1, \dots, X_n]$, tels que $\sum_{i=1}^{s} \deg f_i < n$.
On note $V = \left\{ (x_1, \dots, x_n) \in \mathbb{F}_q^n \middle| \forall i \in [\![1,s]\!], f_i(x_1, \dots, x_n) = 0 \right\}$.
Alors on a : $\#V \equiv 0\,[p]$.

Démonstration :

Posons $P = \prod_{i=1}^{s} \left(1 - f_i^{q-1}\right)$ et soit $\underline{x} = (x_1, \dots, x_n) \in \mathbb{F}_q^n$.

- Si $\underline{x} \in V$, alors $\forall i \in [\![1,s]\!], f_i(\underline{x}) = 0$ et donc $P(\underline{x}) = 1$.
- Si $\underline{x} \notin V$, alors $\exists i_0 \in [\![1,s]\!], f_{i_0}(\underline{x}) \neq 0$ puis $f_{i_0}(\underline{x})^{q-1} = 1$ d'où $P(\underline{x}) = 0$.

Ainsi, en posant $S(f) = \sum_{\underline{x} \in \mathbb{F}_q^n} f(\underline{x})$ pour $f \in \mathbb{F}_q[X_1, \dots, X_n]$, on a : $S(P) = \sum_{\underline{x} \in V} 1 + 0 \equiv \#V\,[p]$.

On veut désormais montrer que $S(P) = 0$.

Lemme

Soit $u \in \mathbb{N}$, vérifiant $u = 0$ ou $(q-1) \nmid u$.
On pose $s(X^u) = \sum_{x \in \mathbb{F}_q} x^u$, et on a alors $s(X^u) = 0$, avec la convention $0^0 = 1$.[63]

Démonstration :

Si $u = 0$, alors $\forall x \in \mathbb{F}_q, x^u = 1$ et $s(X^u) = 0$.
Si $(q-1) \nmid u$, on écrit la division euclidienne $u = (q-1)k + r$, où $k \in \mathbb{N}$ et $0 < r < q-1$.
Soit y un générateur de $\mathbb{F}_q^\times$, qui est cyclique[64].

On a donc $y^u = \left(y^{q-1}\right)^k y^r = y^r \neq 1$ car y est d'ordre $(q-1)$ et $0 < r < q-1$.
Ainsi on a :

$$s(X^u) = \sum_{x \in \mathbb{F}_q} x^u = \sum_{x \in \mathbb{F}_q^\times} x^u = \sum_{x \in \mathbb{F}_q^\times} (xy)^u = y^u \sum_{x \in \mathbb{F}_q^\times} x^u = y^u s(X^u)$$

Donc $(1 - y^u)\, s(X^u) = 0$, puis par intégrité de $\mathbb{F}_q$, $s(X^u) = 0$ car $1 - y^u \neq 0$. ∎

On a $\deg P = \sum_{i=1}^{s} (q-1) \deg f_i < n(q-1)$ et donc $P = \sum_{|\underline{u}| < n(q-1)} \alpha_{\underline{u}} \underline{X}^{\underline{u}}$ où $|\underline{u}| = \sum_{j=1}^{n} u_j$ et $\alpha_{\underline{u}} \in \mathbb{F}_q$.

D'où $S(P) = \sum_{\underline{x} \in \mathbb{F}_q^n} \sum_{|\underline{u}| < n(q-1)} \alpha_{\underline{u}} \underline{x}^{\underline{u}} = \sum_{|\underline{u}| < n(q-1)} \alpha_{\underline{u}} S(\underline{X}^{\underline{u}})$.

Or, pour $|\underline{u}| < n(q-1)$, $S(\underline{X}^{\underline{u}}) = \sum_{(x_1, \dots, x_n) \in \mathbb{F}_q^n} x_1^{u_1} \dots x_n^{u_n} = \sum_{x_1 \in \mathbb{F}_q} x_1^{u_1} \dots \sum_{x_n \in \mathbb{F}_q} x_n^{u_n} = \prod_{j=1}^{n} s(X^{u_j})$.

Mais $\sum_{j=1}^{n} u_j < n(q-1)$ impose $\exists j_0 \in [\![1,n]\!], u_{j_0} < q-1$ donc $(q-1) \nmid u_{j_0}$ ou $u_{j_0} = 0$.

Donc $s\left(X^{u_{j_0}}\right) = 0$, d'où $S(P) = 0$ puis $\#V \equiv 0\,[p]$. ∎

62. On passera le lemme permettant de démontrer le théorème de Chevalley-Warning et on détaillera le cas non-premier du théorème d'Erdös-Ginzburg-Ziv.

63. On peut montrer que si $u \geqslant 1$ et $(q-1) | u$, alors $s(X^u) = -1$.
En effet, $\exists k \in \mathbb{N}^*, u = (q-1)k$ et pour $x \in \mathbb{F}_q^\times$, $x^u = \left(x^{q-1}\right)^k = 1^k = 1$.
En outre $0^u = 0$, donc $s(X^u) = (q-1) \times 1 + 0 = -1$ dans $\mathbb{F}_q$.

64. Pour la cyclicité de $\mathbb{F}_q^\times$, on renvoie à la page 139.

Théorème (*Erdös-Ginzburg-Ziv*)

> Soit p un nombre premier, et soient $a_1, \dots, a_{2p-1} \in \mathbb{Z}$.[65]
> Parmi ces $(2p-1)$ nombres entiers, on peut en trouver p dont la somme est divisible par p.

Démonstration :

Pour $a \in \mathbb{Z}$, on note $\overline{a}$ sa classe modulo p.

On considère les polynômes $P_1 = \sum_{k=1}^{2p-1} X_k^{p-1}, P_2 = \sum_{k=1}^{2p-1} \overline{a_k} X_k^{p-1} \in \mathbb{F}_p\left[X_1, \dots, X_{2p-1}\right]$.

On a : $\deg P_1 + \deg P_2 = 2p-2 < 2p-1$, et $(0, \dots, 0)$ est une racine commune à ces deux polynômes ; donc, par le théorème de Chevalley-Warning, ils admettent une autre racine commune $\left(x_1, \dots, x_{2p-1}\right) \in \mathbb{F}_p^{2p-1}$.
De $P_1\left(x_1, \dots, x_{2p-1}\right) = 0$, il vient que parmi $x_1, \dots, x_{2p-1}$, exactement p d'entre eux sont non-nuls, et on les note $x_{n_1}, \dots, x_{n_p}$.

De $P_2\left(x_1, \dots, x_{2p-1}\right) = 0$, il vient ensuite que $\sum_{i=1}^{p} \overline{a_{n_i}} = 0$.

On a donc trouvé p éléments $a_{n_1}, \dots, a_{n_p}$ dont la somme est divisible par p. ■

Références

[Ser] J.-P. SERRE – *Cours d'arithmétique*, 1e éd., Presses Universitaires de France, 1970.
[Zav] M. ZAVIDOVIQUE – *Un max de maths*, Calvage & Mounet, 2013.

65. Ce résultat reste vrai pour n'importe quel $n \in \mathbb{N}^*$. On opère par récurrence forte.
   - Si $n = 1$, le résultat est trivial.
   - Soit $n > 1$, on suppose le résultat jusqu'au rang $(n-1)$. Soient $a_1, \dots, a_{2n-1} \in \mathbb{Z}$.
     - Si n est premier, c'est l'objet du développement.
     - Sinon, on écrit $n = pn'$, avec p premier et $n' \in \mathbb{N}^*$.
       On a alors : $2n - 1 = 2n'p - 1 = (2n'-1)p + p - 1$.
       Pour i allant de 1 à $2n'-1$, on construit par récurrence les ensembles suivants appelés E_i :
       $$E_i \text{ est un ensemble de } p \text{ éléments parmi } \left\{a_j \middle| j \in [\![1, (i+1)p-1]\!]\right\} \setminus \bigcup_{k=1}^{i-1} E_k \text{, dont la somme est divisible par } p.$$
       La construction de ces ensembles utilise le résultat démontré dans le développement, car $\#\left\{a_j \middle| j \in [\![1, (i+1)p-1]\!]\right\} \setminus \bigcup_{k=1}^{i-1} E_k = 2p-1$.
       Puis, pour $i \in [\![1, 2n'-1]\!]$, S_i désigne la somme des éléments de E_i et $S'_i = \frac{S_i}{p} \in \mathbb{Z}$.
       Par hypothèse de récurrence, parmi les $(2n'-1)$ entiers S'_i, il en existe n' dont la somme est divisible par n', et on les note $S'_{k_1}, \dots, S'_{k_{n'}}$.
       On pose alors $E = \bigsqcup_{i=1}^{n'} E_{k_i}$, et $\#E = n'p = n$ et $\sum_{x \in E} x = \sum_{i=1}^{n'} S_{k_i} = p \sum_{i=1}^{n'} S'_{k_i}$.
       Or $n' \left| \sum_{i=1}^{n'} S'_{k_i} \right.$ donc $n = pn' \left| \sum_{x \in E} x \right.$.

On peut même montrer un résultat d'optimalité : prenons un ensemble de $(2n-2)$ entiers composé de $(n-1)$ fois 0, et de $(n-1)$ fois 1. Un sous-ensemble de n entiers parmi ceux-ci sera de somme comprise entre 1 et $n-1$, donc non-divisible par n.

Théorème des deux carrés

120, 121, 122, 123
126

Leçons : 120, 121, 122, 126

[Per], partie II.6
[Duv], partie 6.1

Théorème

Soit p un nombre premier impair, on note $\Sigma = \{n \in \mathbb{N} | \exists a, b \in \mathbb{N}, n = a^2 + b^2\}$.
On a : $p \in \Sigma \Leftrightarrow p \equiv 1\,[4]$.

Démonstration :

Pour commencer, quelques mots sur $\mathbb{Z}[i]$: on définit la "norme" N : $\left| \begin{array}{ccc} \mathbb{Z}[i] & \to & \mathbb{N} \\ z = a+ib & \mapsto & z\bar{z} = a^2+b^2 \end{array} \right.$;
alors N est multiplicative, ce qui signifie que $N(zz') = N(z)N(z')$ pour tous $z, z' \in \mathbb{Z}[i]$.

Lemme 1

On a : $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Démonstration du lemme 1 :

$\subset$ Si $z \in \mathbb{Z}[i]^\times$, alors $N(z)N(z^{-1}) = N(1) = 1$, donc $N(z) = 1$.
Or $z = a + ib$, avec $a, b \in \mathbb{Z}$, donc $a^2 + b^2 = 1$ et on a ($a = 0$ et $b = \pm 1$) ou ($a = \pm 1$ et $b = 0$).

$\supset$ Cette vérification est immédiate... ■

Lemme 2

On a l'équivalence : $p \in \Sigma \Leftrightarrow p$ est réductible dans $\mathbb{Z}[i]$.

Démonstration du lemme 2 :

$\Rightarrow$ Si $p = a^2 + b^2$, alors dans $\mathbb{Z}[i]$, $p = (a+ib)(a-ib)$.
Comme $N(a+ib) = N(a-ib) = p > 1$, on sait que $a+ib$, $a-ib \notin \mathbb{Z}[i]^\times$ et donc p est réductible.

$\Leftarrow$ Si $p = zz'$ dans $\mathbb{Z}[i]$ avec $z, z' \notin \mathbb{Z}[i]^\times$, on a : $N(p) = N(z)N(z') = p^2$.
Mais on sait que $N(z) \neq 1 \neq N(z')$, donc $N(z) = p$. ■

Comme $\mathbb{Z}[i]$ est factoriel [60], par le lemme d'Euclide, on a :

$$p \text{ réductible dans } \mathbb{Z}[i] \Leftrightarrow (p) \text{ non-premier dans } \mathbb{Z}[i] \Leftrightarrow \mathbb{Z}[i]/(p) \text{ non-intègre}$$

Mais comme $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2+1)$, on a les isomorphismes suivants :

$$\mathbb{Z}[i]/(p) \underset{61}{\simeq} \mathbb{Z}[X]/(X^2+1, p) \simeq \left(\mathbb{Z}[X]/(p)\right)/\left(\overline{X^2+1}\right) \simeq \mathbb{F}_p[X]/(X^2+1)$$

En conséquence, p est réductible dans $\mathbb{Z}[i] \Leftrightarrow \mathbb{F}_p[X]/(X^2+1)$ non-intègre
$\Leftrightarrow X^2 + 1$ réductible dans $\mathbb{F}_p[X]$
$\Leftrightarrow X^2 + 1$ a une racine dans $\mathbb{F}_p$
$\Leftrightarrow -1$ est un carré dans $\mathbb{F}_p$
$\Leftrightarrow (-1)^{\frac{p-1}{2}} = \left(\frac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1\,[4]$ ■

60. Le plus simple pour montrer la factorialité, c'est de montrer que $\mathbb{Z}[i]$ est euclidien pour la norme N, puis de dire que les anneaux euclidiens sont factoriels (voir en page 136).

61. Je tape les explications pour un isomorphisme, adaptez ceci pour trouver les autres. Ce passage me semble absolument indispensable à savoir rédiger pour pouvoir présenter ce développement.
Notons $\pi_{X^2+1} : \mathbb{Z}[X] \to \mathbb{Z}[X]/(X^2+1)$ et $\pi_{\overline{p}} : \mathbb{Z}[X]/(X^2+1) \to \left(\mathbb{Z}[X]/(X^2+1)\right)/(\overline{p})$ les projections canoniques.
Alors $\operatorname{Ker} \pi_{\overline{p}} \circ \pi_{X^2+1} = \left\{f \in \mathbb{Z}[X] \middle| \exists u \in \mathbb{Z}[X], \overline{f} = \overline{pu}\right\} = \{f \in \mathbb{Z}[X] | \exists u, v \in \mathbb{Z}[X], f = pu + (X^2+1)v\} = (p, X^2+1)$.
En conséquence, $\mathbb{Z}[X]/(p, X^2+1) \simeq \left(\mathbb{Z}[X]/(X^2+1)\right)/(\overline{p}) \simeq \mathbb{Z}[i]/(p)$.

~~Corollaire~~ THM DES 2 CARRÉS

Soit $n \in \mathbb{N}^*$, qu'on décompose en facteurs premiers : $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$ (où $\mathcal{P}$ désigne l'ensemble des nombres premiers).
On a l'équivalence : $n \in \Sigma \Leftrightarrow \left(\forall p \in \mathcal{P}, p \equiv 3\,[4] \Rightarrow v_p(n) \equiv 0\,[2]\right)$.

Démonstration :

Lemme 3

Σ est stable par multiplication.

Démonstration du lemme 3 :
En effet, on sait déjà que $n \in \Sigma \Leftrightarrow \exists z \in \mathbb{Z}[i], n = N(z)$.
En conséquence, si $n, n' \in \Sigma$, alors $nn' = N(z)N(z') = N(zz') \in \Sigma$. ∎

$\Leftarrow$ On décompose n de la façon suivante :

$$n = \underbrace{\left(\prod_{\substack{p \in \mathcal{P} \\ p \equiv 3\,[4]}} p^{\frac{v_p(n)}{2}} \right)^2}_{\text{Carré parfait}} \underbrace{\left(\prod_{\substack{p \in \mathcal{P} \\ p \not\equiv 3\,[4]}} p^{v_p(n)} \right)}_{\substack{\text{Somme de 2 carrés} \\ \text{(lemme 3)}}}$$

$\Rightarrow$ Soit $n = a^2 + b^2 \in \Sigma$, on note $\delta = a \wedge b$, $a' = \frac{a}{\delta}$ et $b' = \frac{b}{\delta}$.
Ainsi, $a' \wedge b' = 1$ et $n = \delta^2\left(a'^2 + b'^2\right)$.
Soit p un diviseur premier impair de $a'^2 + b'^2$; alors dans $\mathbb{Z}[i]$, on a : $p | (a' + ib')(a' - ib')$.

- Par l'absurde, supposons p irréductible dans $\mathbb{Z}[i]$.
  Le lemme d'Euclide nous indique que $p | (a' + ib')$ ou que $p | (a' - ib')$; mais par passage au conjugué, si p divise l'un, alors p divise l'autre.
  Donc p divise les deux, puis par somme et différence, on obtient : $p | 2a'$ et $p | 2ib'$ dans $\mathbb{Z}[i]$.
  En passant à la norme, on en déduit : $p^2 | 4a'^2$ et $p^2 | 4b'^2$, dans $\mathbb{Z}$.
  Mais on sait que p est impair, et donc $p | a'$ et $p | b'$.
  Contradiction !
- On peut donc écrire $p = xy$ dans $\mathbb{Z}[i]$, avec en plus $N(x) \neq 1 \neq N(y)$ (ce qui signifie, rappelons-le, que x et y peuvent être pris non-inversibles).
  En passant à la norme, on obtient : $p^2 = N(x)N(y)$; puis, p étant premier, on obtient : $p = N(x)$.
  En conséquence, $p \in \Sigma$, d'où $p \equiv 1\,[4]$.

Ainsi, on a montré que les facteurs premiers congrus à 3 modulo 4 sont "dans" le δ^2, c'est-à-dire d'exposant pair. ∎

Références

[Per] D. PERRIN – *Cours d'algèbre*, Ellipses, 1996.
[Duv] D. DUVERNEY – *Théorie des nombres*, 2e éd., Dunod, 2007.