121 - Nbs 1ers, applicat°.

[Rombaldi]
[Sp]
[Perrin]
[Gourdon]
[FGN agreg 1]
[FGN al 1]
Combes au Ulmer

I - Théorème fondamental de l'arith.

[R] **Def 1** : Soit $p \in \mathbb{Z}$, on dit que p est 1er si $p \geq 2$ et si ses seuls diviseurs positifs sont 1 et p. On note $\mathcal{P}$ l'ensemble des nombres 1ers.

Prop 1 bis : Les 1ers de $\mathbb{Z}$ sont exact les irred.

[R] **Ex 2** : 2, 31 ou 65537 sont 1ers mais 123 n'est pas 1er.

[R] **Thm (Euclide) 3** : $\forall n \in \mathbb{Z} \setminus \{-1, 0, 1\}$: n a un diviseur 1er.

[R] **Cor 4** : $\mathcal{P}$ est infini

[R] **Thm 5 (fondamental de l'arithmétique)** $\forall n \geq 2$, n se décompose de manière unique sous la forme $n = q_1^{\alpha_1} \cdots q_k^{\alpha_k}$ où les q_i sont des 1ers tq $2 \leq q_1 < q_2 \cdots < q_k$ et $\alpha_i \in \mathbb{N}^* \ \forall i$.

Ex 6 : $105 = 7 \times 3 \times 5$, $322 = 23 \times 7 \times 2$

II - Recherche de nombres 1ers : [G]

Thm 6 (Fermat) Soit p 1er et $a \in \mathbb{Z}$ alors $a^p \equiv a \bmod p$ et si $p \nmid a$ $a^{p-1} \equiv 1 \ (p)$

[R] **Ex 7** : $n = 561 = 3 \times 11 \times 17$ non premier mais si $a \in \mathbb{Z}$ et $a \wedge 561 = 1$ alors a^2, a^{10} et $a^{17} \equiv a \bmod 3, 11, 17$ et ainsi $a^{560} \equiv 1 \bmod 3, 11, 17$. Par le thm chinois : $a^{560} \equiv 1 \bmod 561$

Thm 8 (Wilson) p est 1er $\Leftrightarrow (p-1)! \equiv -1 \ (p)$

Prop 9 : Soit $n \geq 2$ tq $\exists a \in \mathbb{Z}$ vérifiant $a^{n-1} \equiv 1 \bmod n$ et $\forall q \mid n-1$ $q \neq n-1$ $a^q \not\equiv 1 \ (n)$. Alors n est 1er.

III - Répartit° des nbs 1ers :

[Rex] **Prop 10** Soit $n \geq 2$, on peut trouver n entiers consécutifs non 1ers.

Rq 11 : Cela signifie qu'$\exists$ des trous arbit. gd entre les nombres 1ers.

Th 14 puis géné [FGN 1] → **Lemme 12** : Soit p un nombre 1er, $a \in \mathbb{Z}$, $n \in \mathbb{N}$ et Φ_n le n-ième poly cyclotomiq alors si $p \mid \Phi_n(a)$ mais $p \nmid \Phi_d(a)$ $\forall d$ diviseur strict de a, alors $p \equiv 1 \bmod n$

[FGN 1] **Thm 13 (Dirichlet faible)** Soit $n \in \mathbb{N}^*$ il existe une infinité de nbs 1ers congrus à 1 mod n.

[R] **Thm 14** Il existe une infinité de nbs 1ers de la forme $6n-1$, $n \in \mathbb{N}$.

[R] **Thm 15 (admis)** Si $\pi(x)$ désigne le nb de 1ers $\leq x$, on a $\pi(x) \sim \frac{x}{\ln(x)}$

IV - Applications en arithmétique

a) Thm de Sophie Germain. [FGN 1]

Lemme 16 : Soit $k \geq 2$, soit a et b 2 entiers naturels $\neq 0$. Si $\exists c \in \mathbb{N}$ tq $ab = c^k$ et si a et b sont 1ers entre eux alors a et b sont eux aussi des puissances k-ièmes.

Def 17 : Un nombre p 1er est dit de Sophie Germain si $q = 2p+1$ est 1er

Ex 18 2, 3, 11 sont des nbs 1ers de Sophie Germain.

Thm 19 : Soit p 1 nb 1er de Sophie Germain ; il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ tq $x^p + y^p + z^p = 0$.

b) Cryptage RSA [G]

Thm 20 : Soit $p < q$ 2 nbs 1ers et $n = pq$. On choisi $c < \varphi(n)$ tq $c \wedge \varphi(n) = 1$. On calcule $d < \varphi(n)$ tq $cd \equiv 1 \ (\varphi(n))$. Si $t \in \mathbb{Z}$ alors $t^{cd} \equiv t \bmod n$.

Appli 21 $g : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ s'appelle f° de chiffrement et $\varphi : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$, $t \longmapsto t^d$ f° de déchiffrement. Par le thm $\varphi \circ g(t) = t \ \forall t$.
On appelle le couple (n, c) la clef publique : à partir de celle-ci tout le monde peut crypter un message + ...

d est la clef privée, elle permet de décrypter le message via φ. La sécurité de ce chiffrement repose sur la difficulté de factorisat° de n pour n assez gd.

c) Décomposit° d'1 nb en somme de carrés (P)

Thm 22 Soit p nbr, alors p s'écrit comme la somme de 2 carrés $\in \mathbb{N}$ ssi p est pair ou $p \equiv 1 \bmod 4$.

Cor 23 Soit $n \in \mathbb{N}$, et $n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$ sa décomposition en nb nbrs premiers. Alors n est une somme de 2 carrés $\in \mathbb{N}$ ssi $\forall p \equiv 3 \bmod 4$ premier, $v_p(n)$ est pair.

V- Applicat° à l'irréductibilité de polyn (P)

Thm 24 Soit $P(X) = a_n X^n + \dots + a_0 \in \mathbb{Z}[X]$ et p nbr tel que
1) $p \nmid a_n$
2) $p \mid a_i \ \forall i \in [\![0, n-1]\!]$
3) $p^2 \nmid a_0$.

Alors P est irréductible sur $\mathbb{Q}$

Ex 25: $X^5 + 6X + 3$ est irréductible sur $\mathbb{Z}$

Soit $p \in \mathbb{P}$, $X^{p-1} + X^{p-2} + \dots + X^2 + X + 1$ est irréd sur $\mathbb{Z}$

(P) **Thm 26 (réduct° modulo p)** Soit $P \in \mathbb{Z}[X]$, $P(X) = a_n X^n + \dots + a_0$ et $p \in \mathbb{P}$. On note $\overline{P}$ la réduct° de P ds $\mathbb{Z}/p\mathbb{Z}[X]$ on suppose $\overline{a_n} \neq 0$. Alors si P est irréductible ds $\mathbb{Z}/p\mathbb{Z}[X]$, il l'est dans $\mathbb{Q}[X]$.

(P) **Ex 27**: $X^3 + 462\,X^2 + 2433\,X - 67691$ est irréd sur $\mathbb{Z}$ (en réduisant modulo 2)

(P) **Prop 28**: $X^4 + 1$ est irréd sur $\mathbb{Q}$ mais est réductible sur $\mathbb{F}_p$ $\forall p$ nbr.

VI- Nombres premiers et groupes (Sp)

Prop 28 Tout groupe d'ordre nbr est cyclique

Ex 29: Un groupe d'ordre 23 est $\mathbb{Z}/23\mathbb{Z}$

Prop 30 Soit G un groupe et p le plus petit nbr qui divise $|G|$. Alors si H est un sous groupe de G d'indice p, H est distingué.

Rq 31 En particulier un sous groupe d'indice 2 est toujours dist.

Ex 32 Si G est un p-groupe d'ordre p^n tout sous groupe d'ordre p^{n-1} est distingué dans G.

Prop 33 Le centre d'un p groupe est non trivial

Appli 34: Tout p-groupe d'ordre p^2 est abélien par ex tout groupe d'ordre 49 est abélien

Thm 35 Soit G un p-groupe et X un ensemble fini. Si G agit sur X et si on note $X^G = \{x \in X,\ g \cdot x = x \ \forall g \in G\}$ alors $|X| \equiv |X^G| \bmod p$

Appli 36 Si $p \mid |X|$ il existe un point fixe pour l'action de G sur X.

Appli 37 (Cauchy) Soit G un groupe fini et p nbr tq $p \mid |G|$. Alors il existe dans G au moins un element d'ordre p. (Corollaire)

Thm 38 (Sylow) Soit G un groupe et p nbr tq $p^n \mid |G|$ alors
- Gadmet au moins 1 p-sylow
- Tous les p sylow de G sont conjugués.
- Si n_p désigne le nombre de p-sylow de G $n_p \mid |G|$ et $n_p \equiv 1 \bmod p$.

Cor 39: Un p-sylow est distingué dans G ssi il est le seul p-sylow de G.

Appli 40 Des groupes d'ordre 63 ou 30 ne sont pas simples.

Appli 41: Un groupe d'ordre 45 est soit $\mathbb{Z}/9\pi \times \mathbb{Z}/5\pi$ ou $(\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/5\mathbb{Z}$

VII Corps et corps finis (P)

Prop 42: Soit $\mathbb{K}$ un corps alors soit $\mathrm{car}(\mathbb{K}) = 0$ (et $\mathbb{K}$ infini dans ce cas) soit $\mathrm{car}(\mathbb{K}) = p$ nbr et $\mathrm{car}(\mathbb{Q}) = 0$.

Ex 43: $\mathrm{car}(\mathbb{Z}/p\mathbb{Z}) = p$ nbr premier et $\mathrm{car}(\mathbb{Q}) = 0$.

Prop 44: Soit $\mathbb{K}$ un corps commutatif de caract p nbr, alors $F : \mathbb{K} \to \mathbb{K}$, $x \mapsto x^p$ est un morphisme de corps appelé le mph de Frobenius. Si $\mathbb{K}$ est fini c'est un automorphisme. Si $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$ c'est l'identité

Prop 45 Soit $\mathbb{K}$ un corps fini de car p alors $\mathbb{K}$ est de cardinal p^n pour un $n \in \mathbb{N}$

Ex 46: il n'existe pas de corps de cardinal 6

Thm 47: Soit $q = p^n$ avec $n \in \mathbb{N}$.
Alors
- Tout corps de décomposit° de $X^q - X$ est un corps à q elements.
- Tout corps à q elements est corps de décomposition de $X^q - X$.

En particulier, il existe un corps à q elements et celui-ci est unique à isomorphisme près.

Ex 48 $\dfrac{\mathbb{F}_2(X)}{(X^2+X+1)}$ est le corps à 4 elts.

VIII - Fonction arithmétique de Möbius et appli aux polynômes irréductibles sur $\mathbb{F}_q$ [FGN Agreg 1] [Rombaldi]

Def 49 : Soit $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ où p_i premiers et $\alpha_i \in \mathbb{N}^*$. On définit la fonction de Möbius par $\mu(n) = \begin{cases} 1 \text{ si } n = 1 \\ (-1)^k \text{ si } \alpha_i = 1 \ \forall i \\ 0 \text{ sinon.} \end{cases}$

Ex 50 $\mu(45) = 0$
$\mu(105) = -1$

Prop 51 Soit $n \in \mathbb{N}^*$ $\sum_{d \mid n} \mu(d) = \begin{cases} 0 \text{ si } n \neq 1 \\ 1 \text{ si } n = 1 \end{cases}$

Prop 52 : Soit $(f_n)_{n \geq 1}, (g_n)_{n \geq 1}$ suites de réels tq $\forall n \ f_n = \sum_{d \mid n} g(d)$
alors $\forall n \in \mathbb{N}^* \ g(n) = \sum_{d \mid n} \mu(n/d) f(d)$

Thm 53 : Le nombre de polynômes irréductibles de degrés n sur $\mathbb{F}_q$ unitaires est donné par $\frac{1}{n} \sum_{d \mid n} \mu(n/d) q^d$

Ex 54 : Il y a 1 seul polynôme de degré 2 irréductible sur $\mathbb{F}_2$: c'est $X^2 + X + 1$
Il y a 6 polynômes unitaires irréductibles de degré 4 sur $\mathbb{F}_2$.