104 : Nombres premiers.

Prérequis : Bézout, Gauss, indicatrice d'Euler φ
On considèrera uniquement les nombres premiers positifs.

I- Définitions et exemples

Déf : $p \in \mathbb{N}$ est premier s'il a exactement 2 diviseur : 1 et p. Dans le cas contraire on dit qu'il est composé. On note $\mathbb{P}$ l'ensemble des nombres premiers.

Prop : Soit un entier composé $n \geqslant 2$ alors il existe $p \in \mathbb{P}$ tel que $p|n$ et $p \leqslant \sqrt{n}$

Appli : Crible d'Eratosthène.

Prop : $Card(\mathbb{P}) = +\infty$

Th (fond. de l'arith.) : Tout $n \in \mathbb{N}^* \backslash \{1\}$ s'écrit de manière unique à l'ordre près : $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ avec : $\forall i \quad p_i \in \mathbb{P}, \quad \alpha_i \in \mathbb{N}^*$.

Appli : PGCD et PPCM de deux entiers.

Exo : Mq les nombres premiers $p \equiv -1 \pmod 6$ sont infinis. Gd p.13
Même chose avec $p \equiv 3 \pmod 4$. X-ENS p.134

Exemples : Gd p. 11

Nombres de Mersenne : $a^n - 1 \in \mathbb{P} \Rightarrow \ a = 2, n \in \mathbb{P}$
Réciproque fausse : $2^{11} - 1 = 23 \times 89$.
On ne sait pas s'il y en a une infinité.

Nombres de Fermat : $2^m + 1 \in \mathbb{P} \Rightarrow \exists n \in \mathbb{N}, m = 2^n$
n=0,1,2,3,4 Ok.Récip fausse : $641 | 2^{2^5} + 1$
On ne sait même pas s'il y en a d'autre premier.

II- Propriétés

Prop : On a équivalence entre :
$(i) \quad p \in \mathbb{P}$.
$(ii) \quad \mathbb{Z}/p\mathbb{Z}$ est un corps.
$(iii) \quad \mathbb{Z}/p\mathbb{Z}$ est intègre.

Appli : La caractéristique d'un anneau unitaire intègre est 0 ou $p \in \mathbb{P}$ Gd p. 30

Exo :$(p_1, \dots, p_n) \in \mathbb{P}^n$ 2 à 2distincts $\sqrt{p_1 \dots p_n} \notin \mathbb{Q}$

Th de Fermat : Si $p \in \mathbb{P}$, $\varphi(p) = p - 1$ et donc $\forall a \in \mathbb{Z}, \qquad p \not| a \Rightarrow \ a^{p-1} \equiv 1 \pmod p$

Récip. fausse : nbr de Carmichael $561 = 3.11.17$

Appli : Gd p. 31 + Per p. 74
Si $p \in \mathbb{P}$ alors $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ (cyclique)

Th (Wilson) : $p \in \mathbb{P} \Longleftrightarrow (p-1)! \equiv -1 \pmod p$
Gd p. 9, X-ENS p. 128

Exo :
1) $2 < p \in \mathbb{P}$. Mq -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ ssi $p \equiv 1 \pmod 4$.
2) En déduire qu'il existe une infinité de nbr premier $p \equiv 1 \pmod 4$. Gd p. 37

Exo : Soit la suite croissante $(p_n)_{n \geq 1} = \mathbb{P}$.
1) Montrer que $\sum_{n \geq 1} \frac{1}{p_n}$ diverge.
2) Déduire que $Card\{p \in \mathbb{P}; p \leqslant n\} = \pi(n) = o(n)$
X-ENS (analyse) p. 153

Théorèmes admis :
th. des nbres premiers : $\pi(x) \sim \frac{x}{\ln x}$
th. Dirichlet : $a \wedge b = 1 \Longrightarrow \ (\exists \infty p \in \mathbb{P})\ p = an + b$
th. Tchebychev : $(\forall n \geqslant 2)(\exists p \in \mathbb{P}) \quad n < p < 2n$

III- Applications

Th : Soit $p \in \mathbb{P}$, p est somme de 2 carrés ssi $p = 2$ ou $p \equiv 1 \pmod 4$. Per p. 57
(Nécessite : si A principal alors p irred $\Leftrightarrow (p)$ premier que l'on peut trouver dans X-ENS p. 93)

Cryptographie (RSA) : $p, q \in \mathbb{P}$ distincts. $n = pq$.
Si $cd \equiv 1 \pmod{\varphi(n)}$ alors $\forall t \in \mathbb{Z}\ t^{cd} \equiv t \pmod n$
Gd p. 34

Critère d'Eisenstein : $P \in \mathbb{Z}[X], P(X) = \sum_{k=0}^{n} a_k X^k$.
Si $(\exists p \in \mathbb{P}) \quad p | a_k \ k = 0, 1, ..., n-1;\ p \not| a_n;\ p^2 \not| a_0$ alors P est irreductible sur $\mathbb{Q}[X]$
Gd p. 58

Th. Cauchy (groupes finis) : Soit G un groupe fini et $p \in \mathbb{P}$. Si $p | Card(G)$ alors G contient un élément d'ordre p.
Gd p. 27

Prop : Le centre d'un p-groupe est non trivial.
Appli : Les groupes d'ordre p^2, $p \in \mathbb{P}$ sont abéliens.
Gd p. 27

José Gregorio : http://agregorio.net