I. Arithmétique dans $\mathbb{Z}$

Def 1 On dit qu'un nombre $p \in \mathbb{Z}$ est premier lorsque ses seuls diviseurs positifs sont 1 et lui même. ($p \neq 1$).

Notation : On note $\mathcal{P}$ l'ensemble des nombres premiers positifs

Def 2 Deux entiers $a, b \in \mathbb{Z}$ sont dit premiers entre eux si $a \wedge b = 1$ (ou $a \wedge b = PGCD(a,b)$).

Proposition 3 (identité de Bézout). Soient a et b deux entiers, $\exists (u,v) \in \mathbb{Z}^2$ tels que $au + bv = a \wedge b$
(Un tel couple est appelé couple de coef. de Bézout pour a et b).

Théorème de Bézout 4 Deux entiers a et b sont premiers entre eux si, et seulement si $\exists (u,v) \in \mathbb{Z}^2$)
$au + bv = 1$

Ex : $\forall m \in \mathbb{Z}$, $(m+1)\times 1 - m \times 1 = 1$ i.e : deux entiers consécutifs sont toujours premiers entre eux.

Théorème de Gauss 5 Soient a, b, c trois entiers si a et premier avec b et $a \mid bc$, alors $a \mid c$.

App : $\forall 1 \leq k \leq p-1$, $p \mid \binom{p}{k}$

Lemme d'Euclide 6 Un nombre premier p divise un produit d'entiers ab ssi p divise a ou p divise b.

Proposition 7 Tout entier ≥ 2 admet un diviseur premier

Proposition 8 Si un entier n ne possède aucun diviseur premier p tel que $p^2 \leq |n|$, alors il est premier.

Théorème 9 (Decomposition en facteurs premiers)
Soit n un entier ≥ 2. Alors n admet une décompo' en produit de facteurs premiers
$n = q_1 \cdots q_k$ ou $q_1, \ldots, q_k$ sont premiers.
ou encore : $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ ou $p_1, \ldots, p_r$ sont des nombres premiers distincts, et $\alpha_1, \ldots, \alpha_r$ des entiers naturels non nuls.
De plus, cette décomposition est unique à l'ordre près des facteurs.

Rq : Cela équivaut à dire que l'anneau $\mathbb{Z}$ est factoriel.

Ex : $280 = 2\times2\times2\times5\times7 = 2^3 \times 5 \times 7$.

Proposition 10 : Soient a et b deux entiers naturels non nuls : si $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, $b = p_1^{\beta_1} \cdots p_r^{\beta_r}$.
Alors $a \mid b \iff \forall i \in [\![1, r]\!]$ $\alpha_i \leq \beta_i$

Rq : Le PGCD : $a \wedge b = \prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i)}$
Le PPCM : $a \vee b = \prod_{i=1}^{r} p_i^{\max(\alpha_i, \beta_i)}$

II. Distribution des nombres premiers

A. Test de primalité et fonction indicatrice d'Euler.

Théorème 11 : (Petit Théorème de Fermat).

- Soit p un nombre premier ; alors
$\forall a \in \mathbb{Z}$, $a^p \equiv a \,[p]$

Rq : La réciproque est fausse : $341 = 11 \times 31$ non premier. et pourtant : $2^{341} \equiv 2 \,[341]$

- Soit p un nombre premier. pour tout entiers a premier avec p, on a $a^{p-1} \equiv 1 \,[p]$

Ex : Si p est un nombre premier, alors :
$\sum_{k=1}^{p-1} k^{p-1} \equiv -1 \,[p]$

Théorème 12 (Th. de Wilson) Un entier $p \geq 2$ est un nombre premier ssi $(p-1)! + 1 \equiv 0 \,[p]$

Indicatrice d'Euler

Def 13 Soit un entier $m \geq 2$ notons $(\mathbb{Z}/m\mathbb{Z})^\times$ le groupe des éléments inversibles de l'anneau $\mathbb{Z}/m\mathbb{Z}$.
On appelle indicatrice d'Euler de m l'entier $\varphi(m) = \text{Card}((\mathbb{Z}/m\mathbb{Z})^\times)$

Théorème 14 (d'Euler) Soit $m \geq 2$ un entier. Si k est premier avec m, alors $k^{\varphi(m)} \equiv 1 [m]$.

Proposition 15 Soit $m \geq 2$ un entier $/ m = p_1^{d_1} \dots p_r^{d_r}$
Alors $\varphi(m) = \prod_{i=1}^{r} \varphi(p_i^{d_i})$.

- Pour tout nombre p premier et tout entier naturel $d \geq 1$ on a : $\varphi(p^d) = (p-1)p^{d-1}$

Conséquence Si $m = p_1^{d_1} \dots p_r^{d_r}$, sa décomposition en facteurs premiers. Alors :
$\varphi(m) = p_1^{d_1-1} \dots p_r^{d_r-1}(p_1-1)\dots(p_r-1) = m\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_r}\right)$

Proposition 16 : $\forall m \geq 1 \quad m = \sum_{d/m} \varphi(d)$.

B. Répartition des nombres premiers

Crible d'Enatostène : Pour trouver tous les nombres premiers entre 1 et m, comme 2 est premier, on le garde et on retire de $\{2, \dots, m\}$ tous les multiples de 2, le plus petit entier restant sera premier, on retire tous ses multiples, ainsi de suite : ...

Proposition 17 : Il existe une infinité de nombres premiers.

Théorème 18 (De Dirichlet fort) (admis)
Soient a et b deux nombres premiers entres eux. Alors il existe une infinité de nombres premiers congrus à a modulo b.

Théorème 19 : (Dirichlet faible)
Soit m un entier. Alors il existe une infinité de nombres premiers congrus à 1 modulo m.

DEY 1

Théorème 20 (Th. des nombres premiers) (Admis)
Le nombre $\pi(x)$ de nombres premiers inférieurs ou égaux à x est équivalent quand $x \to +\infty$, au quotient de x et de son log népérien.

$$\pi(x) \underset{+\infty}{\sim} \frac{x}{\ln(x)}$$

III. Théorie des groupes, corps finis

Th 21 Premier théorème de Sylow Soient G un gpe fini et p un nombre premier divisant l'ordre de G. Si $o(G) = sp^m$, avec $p \nmid s$, alors pour tt entier n / $1 \leq n \leq m$, $\exists$ un sous groupe de G d'ordre p^n.

Corollaire 22 : G gpe fini, si p premier divisant $o(G)$. Alors G a au moins un élément d'ordre p.

Corollaire 23 : G fini d'ordre sp^m ou $p \nmid s$, Alors G contient au moins un sous gpe d'ordre p^m.

Def 24 : • Si G fini, on dit que G est un p gpe si :
• $o(G) = p^m$, p premier, $m \in \mathbb{N}$
• Si $p \mid o(G)$, p premier, H ss-gpe de G est apellé p-ss-gpe de G si $o(H) = p^n$, $n > 0$ de $\mathbb{N}$.
• G finis, $o(G) = sp^m$ / $p \nmid s$, H ss gpe d'ordre p^m → p-sous-gpe de Sylow.

Th 25 : (Second Théorème de Sylow). Soient G un gpe fini et p premier divisant $o(G)$, alors
① tout p-sous-gpe de G est contenu dans un p-ss-gpe de Sylow de G.
② Les p-sous-groupes de Sylow de G sont conjugués.
③ Le nombre de p-sous-groupes de Sylow de G est congru à 1 modulo p et divise $o(G)$.

Proposition 26 : Si G gpe fini d'ordre pq, p et q sont deux nombres premiers, alors G n'est pas simple.

Proposition 27 : Soient p et q deux nombres premiers distincts tel que $p \not\equiv 1 [q]$, $q \not\equiv 1 [p]$ alors tout groupe d'ordre pq est cyclique.

B. Corps finis

Def 27 : Soit $\mathbb{K}$ un corps, $\varphi : \mathbb{Z} \to \mathbb{K}$ morphisme $m \mapsto m 1_{\mathbb{K}}$ d'anneaux
Le nombre générateur de $\ker(\varphi)$ est appelé caractéristique de $\mathbb{K}$.

Rq : Si φ inj. alors $\mathrm{car}(\mathbb{K}) = 0$
Sinon $\mathrm{car}(\mathbb{K}) = p$, $p \in \mathcal{P}$.

Prop 28) $\forall p \in \mathcal{P}$, le corps $\mathbb{Z}/p\mathbb{Z}$ est de cardinal p et de caractéristique p.

Prop 29 : Si V est un $\mathbb{K}$ esp. vectoriel, alors $\dim_{\mathbb{K}} V = m$ où $m < +\infty \iff V \simeq \mathbb{K}^m$.

Théorème 30 : Si $\mathbb{K}$ est un corps fini de caractéristique p, il existe alors un entier $m \geq 1$ tel que $|\mathbb{K}| = p^m$

Notation : On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ $|$ p premier.

Théorème 31 : Soit $m \in \mathbb{N}^*$, un corps $\mathbb{K}$, fini de $\mathrm{car}(\mathbb{K}) = p$ est de cardinal p^m ssi $\mathbb{K}$ est [corps de décomposition (*)] sur $\mathbb{F}_p$ du polynôme $X^{p^m} - X$.

(*) $\mathbb{K}$ est une extension de $\mathbb{F}_p$ tq pour $f(X) \in \mathbb{F}_p[X]$.
- f est scindé sur $\mathbb{K}$.
- ($\mathbb{F}_p \subseteq \mathbb{K}' \subseteq \mathbb{K}$ et $f(X)$ scindé sur $\mathbb{K}'$) $\Rightarrow \mathbb{K} = \mathbb{K}'$.

Théorème 32 : (Th. des deux carrés de Fermat)
Un entier est somme de deux carrés ssi la valuation p-adique de chacun des facteurs premiers p congrus à 3 modulo 4 est paire

DEV 2

Rq : Cela revient à donner une condition nécessaire quant à l'existence de solutions de l'eq.
$m = x^2 + y^2$

IV. Nombres premiers et cryptographie.

Principe de la cryptographie : Le principe général est le suivant : on appelle $\mathcal{M}$ l'ens. des messages ($= [\![0, N-1]\!]$ ou $\mathbb{Z}/N\mathbb{Z}$ en pratique). Deux personne A et B souhaitent s'envoyer un message sans que C ne puisse déchiffrer. A et B choisissent une bij. f_A et f_B. A veut envoyer un message à B, $m \in \mathcal{M}$. A envoie $m' = f_B \circ f_A^{-1}(m)$ (A connait f_B et f_A^{-1}) pour calculer m, B calcule $f_A \circ f_B^{-1}(m') = m$. (B connait f_A et f_B^{-1})

Système RSA :

Procédé : On choisit deux très gd nombres premiers distincts p et q on calcule $N = pq$. On choisit aussi un entier d premier avec $\varphi(N) = (p-1)(q-1)$. La clef publique est (N, d)
- p et q sont secrets, pour $a < N$, on pose $f(a) = a^d \bmod N$.

Pour décoder, on calcule l'inverse de d modulo $\varphi(N)$, on note e cet inverse.
et on aura $f^{-1}(b) = b^e \bmod N$.