121 : Nombres premiers. Applications

I- Arithmétique dans $\mathbb{Z}$

1) Divisibilité, PGCD, PPCM

Définition 1 : soient $a, b \in \mathbb{Z}$, on dit que <u>a divise b</u> ($a|b$) si il existe $n \in \mathbb{Z}$ tel que $b = an$.

Proposition 2 : soit $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$, il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$ avec $0 \leq r \leq b-1$; q est le quotient, r le reste.
Cette opération s'appelle la division euclidienne.
Ici $b | a \iff r = 0$.

Déf 3 : soient $a_1, \dots, a_n$ des entiers, alors il existe un unique $d \in \mathbb{N}$ tel que $a_1\mathbb{Z} + \dots + a_n\mathbb{Z} = d\mathbb{Z}$, c'est le <u>pgcd</u> des a_i.
Si $pgcd(a_i) = 1$, on dit qu'ils sont <u>premiers</u> entre eux.

Thm (de Bézout) 4 : $a_1, \dots, a_n$ sont premiers entre eux si et seulement si il existe $u_1, \dots, u_n$ des entiers tels que $u_1a_1 + \dots + u_na_n = 1$.

Remarque : Si $n = 2$, on peut calculer ces u_1, u_2 avec l'algorithme d'Euclide.

Exemple 5 : $4 \times 7 - 3 \times 9 = 1$ donc 7 et 9 sont premiers entre eux.

Théorème (de Gauss) 5 : si $a | bc$ et $a \wedge b = 1$ alors $a | c$ (en notant $pgcd(a,b) = a \wedge b$).

Corollaire 6 : si $a_1, \dots, a_n$ sont premiers entre eux deux à deux, alors $a_1 \dots a_n | b \iff \forall i, a_i | b$.

Définition 7 : il existe un unique d pour $a_1, \dots, a_n$ entiers tel que $a_1\mathbb{Z} \cap \dots \cap a_n\mathbb{Z} = d\mathbb{Z}$.
On l'appelle le ppcm des $(a_i)_i$.

2) Nombres premiers et localisation

Déf 8 : $p \in \mathbb{N}$ ($p \geq 2$) est premier si ses seuls diviseurs sont $p, -p, 1$ et -1.

Thm 9 : tout entier $n \geq 2$ s'écrit de manière unique sous la forme $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ avec, p_i premiers et $\alpha_i > 0$.

Thm 10 : il existe une infinité de nombres premiers.

Proposition 11 : si $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ et $b = p_1^{\beta_1} \dots p_k^{\beta_k}$ (avec les $\alpha_i, \beta_i \geq 0$) alors $pgcd(a,b) = \prod p_i^{\min(\alpha_i, \beta_i)}$ et $ppcm = \prod p_i^{\max(\alpha_i, \beta_i)}$

Thm (de la progression arithmétique) 12 : Soient a, b entiers premiers entre eux, alors il existe une infinité de nombres premiers de la forme $ak + b$. (admis)

Application du théorème fondamental de l'arithmétique :

Thm d'Erdös - Ginzburg - Ziv 13 pour n entier ≥ 1, et $a_1, \dots, a_{2n-1}$ des entiers, il existe n parmi ceux-ci dont la somme est divisible par n.

DVP1

3) L'anneau $\mathbb{Z}/n\mathbb{Z}$

Déf 14 : soit $n \neq 0$ entier, on dit que $x \equiv y\ [n]$ si $x - y \in n\mathbb{Z}$.
Cette relation définit l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$.
$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$.

Prop 15 : $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.
Les inversibles sont les $m \in \mathbb{Z}/n\mathbb{Z}$ tels que $m \wedge n = 1$.

Thm (Fermat) 16 : $\forall a \in \mathbb{Z}$, $p \nmid a$, alors $a^{p-1} \equiv 1\ [p]$.

Prop 17 : il existe un unique sous-groupe d'ordre $d | n$ de $\mathbb{Z}/n\mathbb{Z}$.

Thm (chinois) 18 : soient $n \wedge m = 1$ alors $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/(nm)\mathbb{Z}$

II - Nombres premiers en théorie des groupes

1) p-groupes

Déf 19 : un p-groupe est un groupe dont l'ordre de tout élément est une puissance de p.

Ex 20 : Q_8, D_4, $\mathbb{Z}/8\mathbb{Z}$.

Prop 21 : Soit p premier, G un p-groupe et X un G-ensemble fini, alors $|X^G| \equiv x\ [p]$.

Thm (de Cauchy) 22 : Soit G fini d'ordre divisible par p premier, alors il existe dans G un élément d'ordre p.

Proposition 23 : soit G un p-groupe fini non trivial, alors $Z(G)$ n'est pas trivial. En particulier, G n'est pas simple.

Corollaire 24 : un groupe d'ordre p^2 est toujours abélien.

2) Théorèmes de Sylow

Définition 25 : soit p premier, G fini, un p-sous-groupe de G maximal pour l'inclusion est appelé un p-Sylow de G. On note $Syl_p(G)$ l'ensemble de tels sous-groupes.

Prop 26 : Si $N \triangleleft G$ est distingué dans G, un p-groupe, alors il est contenu dans l'intersection des p-Sylows de G.

Déf 27 : un p-sous-groupe de G est dit p-clos s'il contient tous les éléments dont l'ordre est une puissance de p.

Corollaire 28 : un p-Sylow est distingué ssi il est p-clos.

Thm (de Sylow) 29 : si $|G| = p^e m$ avec p premier et $e \geq 1$ et $m \wedge p = 1$

→ Les p-Sylow sont les sous-groupes d'ordre p^e de G

→ Les p-Sylow sont tous conjugués.

→ si n_p est le nombre de p-Sylow de G, alors $n_p | m$ et $n_p \equiv 1 [p]$.

Applications : • Prop 30 : un groupe d'ordre $2p$ avec p premier impair est soit isomorphe à $\mathbb{Z}/2p\mathbb{Z}$, soit à D_p.

• un groupe d'ordre 42 n'est pas simple.

• classifications des sous-groupes finis de $SO_3(\mathbb{R})$.

III – Corps finis

1) Existence, unicité, propriétés des corps finis

Prop 31 : Le cardinal d'un corps fini est p^n ~~avec~~ p sa caractéristique et n un certain entier.

Prop 32 : Si K est un corps fini, $K^\times$ est cyclique.

Thm 33 : Il existe un unique corps fini à p^n éléments (unicité à isomorphisme près), c'est le corps de décomposition de $X^{p^n} - X$ sur $\mathbb{Z}/p\mathbb{Z}$.

Thm 34 : Les sous-corps de $\mathbb{F}_{p^n}$ sont les $\mathbb{F}_{p^d}$ avec $d | n$.

exemple :

$$\begin{tikzcd} & \mathbb{F}_{64} & \\ \mathbb{F}_4 \arrow[ur] & & \mathbb{F}_8 \arrow[ul] \\ & \mathbb{F}_2 \arrow[ul] \arrow[ur] & \end{tikzcd}$$

Déf 35 : $\phi : K \to K$, $a \mapsto a^p$ avec K un corps fini est appelé le morphisme de Frobenius.

Prop 36 : Si $K = \mathbb{Z}/p\mathbb{Z}$, $\phi = id$

Si $K = \mathbb{F}_{p^n}$, ϕ est un automorphisme.

Corollaire 37 : tout corps fini est parfait.

2) Carrés dans les corps finis

Déf 38 : on pose $\mathbb{F}_q^2 = \{x^2, x \in \mathbb{F}_q\}$ l'ensemble des carrés de $\mathbb{F}_q$ avec $q = p^n$.

On pose de même $(\mathbb{F}_q^\times)^2$

Prop 39 : si $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$

sinon $|\mathbb{F}_q^{\times 2}| = \frac{q-1}{2}$ et $|\mathbb{F}_q^2| = \frac{q+1}{2}$

Déf 40 : on définit le symbole de Legendre $\left(\frac{x}{p}\right)$ pour $x \in \mathbb{F}_p^\times$ par $\left(\frac{x}{p}\right) = 1$ si et seulement si $x \in \mathbb{F}_p^{\times 2}$ et $\left(\frac{x}{p}\right) = -1$ si $x \notin \mathbb{F}_p^{\times 2}$

Prop 41 : $x \mapsto \frac{x}{p}$ est un morphisme de groupe non constant.

Thm 42 : • $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

• $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ pour p impair

• pour $p \neq q$ impairs, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$

application : $\left(\frac{23}{59}\right) = (-1)^{11\times 29}\left(\frac{59}{23}\right) = -\left(\frac{13}{23}\right) = \dots = -1$ donc 23 n'est pas un carré dans $\mathbb{F}_{59}$

$\boxed{\begin{array}{l}\text{Thm (de Frobenius-Zolotarev) 43 : Soit } p>2 \text{ premier et } n\geq 1 \text{ alors} \\ \forall u \in GL_n(\mathbb{F}_p),\ \varepsilon(u) = \left(\frac{\det(u)}{p}\right).\end{array}}$ $\boxed{\text{DVP 2}}$

3) Polynômes irréductibles sur les corps finis

Prop 45 : Notons $A(n,q)$ l'ensemble des polynômes de $\mathbb{F}_q[X]$ irréductibles et unitaires de degré n, et $I(n,q)$ son cardinal ($n\geq 1$).

Alors • $X^{q^n} - X = \prod_{d|n} \prod_{P\in A(d,q)} P$

• $q^n = \sum_{d|n} d\, I(d,q)$

• $I(n,q) = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$ avec μ la fonction de Möbius.

Prop 44 : Il existe des polynômes irréductibles de tout degré sur $\mathbb{F}_q$ et si $\deg(P) = n$ et P est irréductible sur $\mathbb{F}_q$, alors $\mathbb{F}_{q^n} \simeq \mathbb{F}_q[X]/(P)$.

IV – Nombres premiers remarquables

1) Nombres de Fermat et constructibilité à la règle et au compas

Prop 45 : le point $A_\theta(\cos\theta, \sin\theta)$ est constructible si et seulement si $\cos\theta$ est constructible ssi $\sin\theta$ est constructible.

Def 46 : le polygone régulier à n côtés est dit constructible si et seulement si l'angle $2\pi/n$ est constructible.

Prop 46 : un point x est constructible si et seulement si il existe $e\in\mathbb{N}$ tel que $[\mathbb{Q}(x):\mathbb{Q}] = 2^e$. (voir annexe)

Thm 47 : Le polygone régulier à n côtés est constructible à la règle et au compas si et seulement si il existe $\alpha\in\mathbb{N}$ et $p_1,\dots,p_k$ des nombres de Fermat premiers et distincts tels que $n = 2^\alpha p_1\cdots p_k$.

On rappelle qu'un nombre de Fermat est un entier de la forme $2^{2^n}+1$ avec $n\in\mathbb{N}$.

2) Nombres de Carmichael et critère de primalité

Prop 48 : n est composé s'il existe a avec $a^{n-1}\not\equiv 1\ [n]$ et $1<a<n$.

Def 49 : on appelle témoin de Fermat un a premier avec n tel que $a^{n-1}\not\equiv 1\ [n]$

Def 50 : un nombre est de Carmichael si il est composé et n'a pas de témoin de Fermat.

Exemple : $3\times 11\times 17 = 561$ est le premier nombre de Carmichael.

Prop : soit $n>1$ un entier impair, $n-1 = 2^s t$ avec $t\wedge 2 = 1$, si il existe $a\in]\!]1,n[\![$ tel que $a^t\not\equiv 1\ [n]$ et $a^{2^i t}\not\equiv -1\ [n]$ pour tout $i\in\{0,\dots,s-1\}$, alors n est composé.

Un tel a est appelé témoin de Miller.

Prop : si n est composé et impair, alors au moins 3/4 des $n-2$ entiers entre 1 et n sont des témoins de Miller pour n (admis).

Exemple : $2^{560} \equiv 1\,[561]$ car 561 est de Carmichael.

puis comme $560 = 2^4\times 35$,

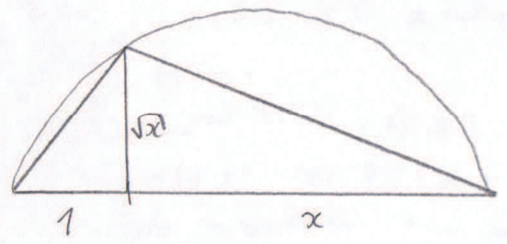
on a $2^{2^3\times 35} \equiv 1\,[561]$

et $2^{2^2\times 35} \equiv 67\,[561]$

donc 2 est un témoin de Miller pour 561.

… sur la constructibilité :

• construire la racine



• construire le produit