NOM : NT

Prénom : Félix

Rouge entourez l'épreuve Bleu

entourez le Jury A B C D E F

Sujet choisi : 121 : Nombres premiers. Applications.

Autre sujet : 102 : Groupe des nombres complexes de module 1. Racines de l'unité. Applications.

I - Nombres premiers

1) Arithmétique des entiers

Déf 1 : $p \in \mathbb{N}$ est premier s'il a exactement 2 diviseurs positifs (1 et p). $\mathcal{P}$ est l'ensemble des nombres premiers.

Ex 2 : $2, 3, 5, 7, 11, 13, 17 \in \mathcal{P}$.

Prop 3 : $\forall n \in \mathbb{Z} \setminus \{-1, 0, 1\}$, n admet un diviseur premier

Cor 4 : Si $n \geq 2$ est non premier, alors $n = pq$ avec p premier et $q \geq 2$. n est dit composé.

Prop 5 : Soit $p \in \mathcal{P}$, $n \in \mathbb{N}^*$. Alors : soit $p \mid n$, soit $p \wedge n = 1$.

Lemme 6 : (Euclide) Soit $n_1, \dots, n_r \in \mathbb{N}^*$ et $p \in \mathcal{P}$. Alors $p \mid \prod_{k=1}^{r} n_k$ si $\exists k \in [\![1, r]\!]$, $p \mid n_k$.

App 7 : $\forall p \in \mathcal{P}$, $\sqrt{p} \notin \mathbb{Q}$.

Th 8 : Tout $n \geq 2$ s'écrit $n = q_1^{\alpha_1} \cdots q_r^{\alpha_r}$, avec $q_1 < \dots < q_r \in \mathcal{P}$, $\alpha_1, \dots, \alpha_r \in \mathbb{N}^*$, et ce de façon unique.

Déf 9 : Si $p \in \mathcal{P}$, la valuation p-adique de $n \geq 1$ est $v_p(n) := \max \{k \in \mathbb{N} / p^k \mid n\}$.

Prop 10 : $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$.

Prop 11 : Si $n, m \in \mathbb{N}^*$, alors : $n \mid m \Leftrightarrow \forall p \in \mathcal{P}, v_p(n) \leq v_p(m)$.

De plus, $n \wedge m = \prod_{p \in \mathcal{P}} p^{\min(v_p(n), v_p(m))}$

$n \vee m = \prod_{p \in \mathcal{P}} p^{\max(v_p(n), v_p(m))}$.

Prop 12 : (Legendre) $\forall p \in \mathcal{P}$, $\forall n \in \mathbb{N}^*$, $v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$

2) Critères de primalité

Prop 13 : Si $n \geq 2$ est composé, alors il admet un diviseur premier $p \in [\![2, \sqrt{n}]\!]$.

Algo 14 : (Crible d'Ératosthène) Pour obtenir la liste des nb. premiers entre 2 et n : cf annexe.

Prop 15 : Soit $n \geq 2$, s'équivalent :
- $n \in \mathcal{P}$
- $\forall k \in [\![1, n-1]\!]$, $n \wedge k = 1$
- $\mathbb{Z}/n\mathbb{Z}$ est un corps
- $\mathbb{Z}/n\mathbb{Z}$ est intègre
- $\varphi(n) = n - 1$ (φ est l'indicatrice d'Euler)

Th 16 : (Fermat) Soit $p \in \mathcal{P}$ et $a \in \mathbb{Z}$, alors : $a^p \equiv a [p]$, et si $a \wedge p = 1$, alors $a^{p-1} \equiv 1 [p]$.

Th 17 : (Wilson) $n \geq 2$ est premier ssi $(n-1)! \equiv -1 [n]$

Ex 18 : $561 = 3 \times 11 \times 17 \notin \mathcal{P}$, mais $\forall a \in \mathbb{Z}$, $a \wedge 561 = 1$ $\Rightarrow a^{560} \equiv 1 [561]$.

Déf 19 : Un nombre de Carmichaël est $n \geq 3$ non premier tq $\forall a \in \mathbb{Z}$, $a \wedge n = 1 \Rightarrow a^{n-1} \equiv 1 [n]$.

Prop 20 : Un nombre de Carmichaël est impair et sans facteur carré.

Th 21 : (Korselt) Soit $n \geq 3$, s'équivalent :
- n est de Carmichaël
- $n \notin \mathcal{P}$ et $\forall x \in \mathbb{Z}/n\mathbb{Z}$, $x^n = x$
- $\exists r \geq 3$, $\exists p_1 < \dots < p_r \in \mathcal{P}_{\geq 3}$, $n = \prod_{j=1}^{r} p_j$ et $\forall j \in [\![1, r]\!]$, $(p_j - 1) \mid (n - 1)$.

Prop 22 : (Test probabiliste) Soit $n \geq 2$ non premier et non de Carmichaël. Alors $|\{a \in [\![1, n-1]\!] / a \wedge n = 1 \text{ et } \bar{a}^{n-1} \neq \bar{1}\}| \geq \frac{\varphi(n)}{2}$.

3) Répartition des nombres premiers

Th 23 : (Euclide) $\mathcal{P}$ est infini.

Prop 24 : $\forall \alpha > 1$, $\zeta(\alpha) = \sum_{n=1}^{+\infty} \frac{1}{n^\alpha} = \prod_{n=1}^{+\infty} \frac{1}{1 - \frac{1}{p_n^\alpha}}$

où $\mathcal{P} = \{p_1 < p_2 < \dots\}$

Cor 25 : $\sum_{n=1}^{+\infty} \frac{1}{p_n} = +\infty$.

Déf 26 : $\pi(n) := |[1,n] \cap \mathcal{P}|$

Th 27 : (Hadamard, De La Vallée-Poussin, "Th des nb premiers") [admis] $\pi(n) \underset{n\to+\infty}{\sim} \frac{n}{\ln(n)}$.

Cor 28 : $p_n \underset{n\to+\infty}{\sim} n\ln(n)$

Prop 29 : (Version faible) $\ln(2)\frac{n}{\ln(n)} \underset{n\to+\infty}{\leq} \pi(n) \underset{n\to+\infty}{\leq} 2\ln(2)\frac{n}{\ln(n)}$

où $\underset{n\to+\infty}{\leq}$ est la clôture transitive de $(\leq$ ou $\underset{n\to+\infty}{\sim})$. (DV1)

Th 30 : (Progression arithmétique de Dirichlet) Soit $a, N \geq 1$ tq $a \wedge N = 1$. Alors il existe une infinité de $p \in \mathcal{P}$ tq $p \equiv a\ [N]$. [admis].

Conjecture 31 :
- Il existe une infinité de nombres premiers jumeaux
- (Goldbach) Tout nombre pair composé est somme de 2 nombres premiers.

II - Applications

1) Théorie des groupes finis

Th 32 : (Cauchy) Soit G un groupe fini, $p \in \mathcal{P}$ tq $p \mid |G|$. Alors G admet un élément d'ordre p.

App 33 : Les seuls groupes d'ordre ≤ 5 sont $\mathbb{Z}/6\mathbb{Z}$ et S_3.

Prop 34 : Soit $p \in \mathcal{P}$ minimal tq $p \mid |G|$, et H un sg de G d'indice p. Alors H est distingué dans G (DV2)

Déf 35 : Un p-groupe est un groupe de cardinal p^α, $\alpha \geq 1$.

Prop 36 : Soit G un p-groupe et X fini, avec $G \curvearrowright X$. Alors $|X^G| \equiv |X|\ [p]$.

Cor 37 : Si G est un p-groupe, alors $Z(G) \neq \{1\}$.

Déf 38 : Soit G un groupe, le sous-groupe de Frattini de G est $\Phi(G) = \bigcap_{H \text{ sg maximal de } G} H$.

Ex 38.5 : Si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ alors $\Phi(\mathbb{Z}/n\mathbb{Z}) = \overline{p_1 \cdots p_r}^{\mathbb{Z}/n\mathbb{Z}}$

Lemme 39 : Si $g \in G$, alors : $g \in \Phi(G)$ ssi $\forall (g_1, \dots, g_k)$ génératrice de G, $(g_1, \dots, g_k)$ est encore génératrice. On dit que g est inutile.

Th 40 : (Frattini) Si G est un p-groupe, alors $G/\Phi(G)$ est un $\mathbb{Z}/p\mathbb{Z}$-ev. De plus, toute famille génératrice minimale (pour l'inclusion) a pour cardinal $\dim_{\mathbb{Z}/p\mathbb{Z}}(G/\Phi(G))$ (DV2)

C-Ex 41 : dans $\mathbb{Z}/6\mathbb{Z}$, $\{1\}$ et $\{2,3\}$ sont minimales.

2) Arithmétique des polynômes

Lemme 41 : (Gauss) Si $P, Q \in \mathbb{Z}[X]$, alors $c(PQ) = c(P)c(Q)$ (où c est le contenu)

Cor 41.5 : avec $P = AB \in \mathbb{Z}[X]$, alors $A, B \in \mathbb{Q}[X]$ unitaires

Th 42 : (Gauss) $\mathbb{Z}[X]$ est factoriel, et ses irréductibles sont :
- les constantes $p \in \mathcal{P}$
- les $P \in \mathbb{Z}[X]$ de degré ≥ 1 primitifs et irréductibles dans $\mathbb{Q}[X]$

Prop 43 : (Eisenstein) Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ et $p \in \mathcal{P}$.
Si : $-p \nmid a_n$ $-\forall k \in [\![0, n-1]\!], p \mid a_k$ $-p^2 \nmid a_0$
Alors P est irréductible dans $\mathbb{Q}[X]$ (donc dans $\mathbb{Z}[X]$ s'il est de plus primitif).

Ex 44 : Soit $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \in \mathbb{N}$, avec l'un des $\alpha_i = 1$.
Alors $X^n - a$ est irréductible sur $\mathbb{Z}$.
Ainsi $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} / \alpha \text{ algébrique sur } \mathbb{Q}\}$ est de degré infini sur $\mathbb{Q}$.

Prop 45 : (réduction) Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ et $p \in \mathcal{P}$, on note $\overline{P} = \sum_{k=0}^{n} \overline{a_k} X^k \in \mathbb{Z}/p\mathbb{Z}[X]$.
Si : $\overline{a_n} \neq \overline{0}$ et $\overline{P}$ est irréd sur $\mathbb{Z}/p\mathbb{Z}$,
Alors P est irréd sur $\mathbb{Q}$ (donc sur $\mathbb{Z}$ si P primitif).

Ex 46 : $X^3 + 462X + 2433X - 67691$ est irréd sur $\mathbb{Z}$.

Déf 47 : Le n^e polynôme cyclotomique est $\Phi_n = \prod_{\zeta \in \mu_n^*} (X - \zeta)$
où $\mu_n^* \subset \mathbb{C}$ est l'ensemble des racines n^e primitives de l'unité.

Prop 48 : • $X^n - 1 = \prod_{d \mid n} \Phi_d$
• $\forall n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$

Ex 49 : $\Phi_1 = X - 1$, $\Phi_2 = X + 1$, $\Phi_3 = X^2 + X + 1$, $\Phi_4 = X^2 + 1$, ...

App 50 : (Dirichlet, version faible) Soit $N \geq 1$, il existe une infinité de nb premiers p tq $p \equiv 1 [N]$.
DV3

Th 51 : $\forall n \geq 1$, Φ_n est irréductible (sur $\mathbb{Q}$ et sur $\mathbb{C}$)

Déf (Prop 52) : Si $2^n + 1$ est premier, alors $n = 2^m$ avec $m \in \mathbb{N}$.
On appelle $F_n := 2^{2^n} + 1$ le n^e nombre de Fermat

Rq 53 : F_0, F_1, F_2, F_3, F_4 sont premiers et on conjecture que ce sont les seuls.

App 54 : (Gauss-Wantzel) Le polygone régulier à n côtés est constructible à la règle et au compas ssi $n = 2^k p_1 \dots p_\ell$ où $p_1, \dots p_\ell$ sont des nb premiers de Fermat 2 à 2 distincts, et $k \in \mathbb{N}$.
DV4?

3) Corps finis

Dans cette partie, $p \in \mathcal{P}$ et $q = p^r$ avec $r \geq 1$

Lemme 55 : $\forall k \in [\![1, p-1]\!]$, $p \mid \binom{p}{k}$.
Si K est un corps de carac p, alors $F : \begin{matrix} K \to K \\ x \mapsto x^p \end{matrix}$ est un morphisme de corps, dit de Frobenius.

Th 56 : Il existe un unique corps à q éléments, c'est $D_{/\mathbb{Z}}(X^q - X)$. On le note $\mathbb{F}_q$.

Prop 57 : Si K est un corps, tout sg fini de $K^\times$ est cyclique. En particulier $\mathbb{F}_q^\times$ l'est.

Th 58 : (Chevalley-Warning) Soit $P_1, \dots P_n \in \mathbb{F}_q[X_1, \dots X_m]$ tq $\sum_{i=1}^{n} \deg(P_i) < m$. Notons $V := \{x \in K^m / \forall i, P_i(x) = 0\}$ alors $|V| \equiv 0 [p]$.

App 59 : (Erdös-Ginzburg-Ziv) Parmi $2n-1$ entiers, on peut en trouver n dont la somme est divisible par n.
DV5!

Annexe : Crible d'Ératosthène
- on se donne la liste $[\![2, n]\!]$
- on garde 2 et on supprime tous les multiples de 2
- on garde (bien sûr) le suivant qui reste dans la liste, et on supprime tous ses multiples
- on continue jusqu'à avoir gardé un nb $\geq \sqrt{n}$

2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	18	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	~~29~~	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	~~37~~	~~38~~	~~39~~	~~40~~
41	~~42~~	~~43~~	~~44~~	~~45~~	~~46~~	~~47~~	~~48~~	~~49~~	~~50~~

Ici pour $n = 50$, on s'arrête après avoir gardé 11 ($\sqrt{50} > 7$)