121

NOM : Prénom : Jury :

Algèbre ← Entourez l'épreuve → Analyse

Sujet choisi : Nombres Premiers. Applications

Autre sujet :

[DEK] (p≥11) + [ARN] (p≥123)

I Nombres premiers. (entre eux)

DEF 1 On dit que $a,b \in \mathbb{Z}$ sont premiers entre eux si $\text{pgcd}(a,b)=1$.

TH 2 [Bézout] Soient $a,b \in \mathbb{Z}$.
$\text{pgcd}(a,b)=1 \iff \exists u,v \in \mathbb{Z},\ au+bv=1$.

LEM 3 [Euclide] Soient $a,b,c \in \mathbb{Z}$.
Si $a \mid bc$ et $\text{pgcd}(a,b)=1$ alors $a \mid c$.

DEF 4 On dit que $p>1$ est premier si ses seuls diviseurs sont 1 et p.
On note $\mathcal{P}$ l'ensemble des nombres premiers.

LEM 5 [Gauss] Si p est premier et $p \mid ab$ alors $p \mid a$ ou $p \mid b$.

COR 6 Si p premier et $p \mid a_1 \cdots a_n$ alors il existe $k \in [\![1;n]\!]$ tel que $p \mid a_k$.

TH 7 [Th fondamental de l'arithmétique]
Tout nombre naturel $n>1$ peut s'écrire comme un produit de nombres premiers.
Cette écriture est unique à l'ordre près des facteurs.

APP 8 Soient $a=\prod_{i=1}^{n} p_i^{\alpha_i}$ et $b=\prod_{i=1}^{n} p_i^{\beta_i}$.

Alors $\begin{cases} \text{pgcd}(a,b)=\prod_{i=1}^{n} p_i^{\min(\alpha_i,\beta_i)} \\ \text{ppcm}(a,b)=\prod_{i=1}^{n} p_i^{\max(\alpha_i,\beta_i)} \end{cases}$.

DEF/PROP 10 [indicatrice d'Euler]
On définit $\varphi : \mathbb{N}^* \to \mathbb{N}^*$, $n \mapsto |\{k \in [\![1;n-1]\!] / \text{pgcd}(k,n)=1\}|$
On a $\varphi(n)=|(\mathbb{Z}/n\mathbb{Z})^\times|$.

TH 11 [Euler] Soit $n>1$. Soit $k \in \mathbb{N}$.
Si $\text{pgcd}(k,n)=1$ alors $k^{\varphi(n)} \equiv 1 \ [n]$.

TH 12 [petit théorème de Fermat]
Soit p premier et $a \in \mathbb{N}$ tel que $p \nmid a$.
Alors $a^{p-1} \equiv 1 \ [p]$.

APP 9 $\forall p \in \mathcal{P}, \forall k \in [\![1;p-1]\!],\ p \mid \binom{p}{k}$. [ARN] ↑144 (ex 13)

II Où sont les nombres premiers ?

1 Nombres (premiers) historiques

[DEK] ↑34

DEF/PROP 13 [nombres de Mersenne]
$M_n=2^n-1 \in \mathcal{P} \Rightarrow n \in \mathcal{P}$. [ARN] ↑150

DEF/PROP 14 [nombres de Fermat] [OX] ↑116
$2^m+1 \in \mathcal{P} \Rightarrow 2^m+1=2^{2^n}+1=F_n$.

PROP 15 $n \neq m \Rightarrow \text{pgcd}(F_n,F_m)=1$. [Wikipédia]

PROP 16 Soit p un diviseur premier de F_n. [OX]
Alors $p \equiv 1 \ [2^{n+1}]$. ↑116

2 Tests de primalité

PROP 17 [Crible d'Eratosthène] [DEK]
$n \geq 2$ qui n'est divisible par aucun premier dans $[\![2;\lfloor\sqrt{n}\rfloor]\!]$ est premier. ↑25

121

NOM : Prénom : Jury :

Algèbre ← Entourez l'épreuve → Analyse

Sujet choisi :

Autre sujet :

TH18 $n \in \mathcal{P} \iff \mathbb{Z}/n\mathbb{Z}$ intègre $\iff \mathbb{Z}/n\mathbb{Z}$ corps

[OX] ↑113 **TH19** [Wilson] Soit $p > 1$. $p \in \mathcal{P} \iff (p-1)! \equiv -1 \ [p]$.

3 Répartition des nombres premiers

[DEK] ($p \geq 26$) **TH20** [Euclide] Il existe une infinité de nombres premiers.

DEF21 On note $\pi(x) = |\mathcal{P} \cap [0;x]|$.

PROP22 $\forall x \geq 2$, $\pi(x) \geqslant \ln(\ln(x))$.

ADMIS **TH23** [Th des nombres premiers] $\pi(x) \underset{+\infty}{\sim} \frac{x}{\ln(x)}$.

PROP24 La série $\sum_{p \in \mathcal{P}} \frac{1}{p}$ diverge.

PROP25 Pour tout $n \geq 1$, il existe $N \in \mathbb{N}$ tel que $[\![N; N+n-1]\!] \cap \mathcal{P} = \varnothing$.

[OX] **TH26** [Th faible de Dirichlet] Pour tout $n \in \mathbb{N}^*$, il existe une infinité de nombres premiers congrus à 1 mod n.

ADMIS **TH27** [Th de Dirichlet]. Soient a et b deux entiers premiers entre eux. Il existe une infinité de nombres premiers congrus à a mod b.

III Applications

[PER] ↑76 **TH28** [Critère d'Eisenstein] Soit $n \geq 2$. Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$. Soit $p \in \mathcal{P}$. On suppose
- $p \nmid a_n$
- $\forall i \in [\![0; n-1]\!]$, $p \mid a_i$
- $p^2 \nmid a_0$.

Alors P est irréductible dans $\mathbb{Q}[X]$. DEV1

TH29 Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$. ↑77 Soit $p \in \mathcal{P}$ tel que $p \nmid a_n$. Si $\overline{P} \in (\mathbb{Z}/p\mathbb{Z})[X]$ est irréductible alors P est irréductible dans $\mathbb{Q}[X]$.

EX30 $X^n - 2$ est irréductible dans $\mathbb{Q}[X]$ pour tout $n \geqslant 1$.

TH31 $p \in \mathcal{P}$ est la somme de deux carrés d'entiers $\iff p = 2$ ou $p \equiv 1 \ [4]$. ↑57

TH32 Soit $n = \prod_{i=1}^{r} p_i^{\alpha_i} \geqslant 2$. ↑58 n est la somme de deux carrés d'entiers $\iff \alpha_i$ est pair pour tout $p_i \equiv 3 \ [4]$. DEV2

[DEK] : DE KONINCK, MERCIER, Introduction à la théorie des Nombres (+)
[ARN] : ARNAUDIES, FRAYSSE, Algèbre (-)
[OX] : Cours X-ENS Algèbre 1 (+)
[PER] : PERRIN, Cours d'algèbre (+)