Exercices sur les nombres premiers

Exercice 1. — *Déterminer les nombres premiers p tels que $p+2$ et $p+4$ soient premiers.*

Exercice 2. — *Déterminer les nombres premiers p tels que p divise 2^p+1.*

Exercice 3. — *Soit p un nombre premier impair. Montrer qu'il existe une infinité d'entiers n tels que p divise $n2^n+1$.*

Exercice 4. — *Pour tout $n \geq 2$, construire un intervalle $[N, N+n]$ ne contenant aucun nombre premier.*

Exercice 5. — *En utilisant l'écriture de $\zeta(s)$ en produit Eulérien, montrer que la série $\sum_{p\in\mathcal{P}} p^{-1}$ diverge ; en particulier $\mathcal{P}$ est infini.*

Exercice 6. — *Soit $p \geq 3$ premier et soit $M_p = 2^p - 1$ le nombre de Mersenne associé.*

(a) Montrer que si q est un diviseur de M_p alors $q \equiv 1 \mod 2p$ et $q \equiv \pm 1 \mod 8$.

(b) Montrer que 3 est un résidu quadratique modulo $p \neq 2, 3$ si et seulement si $p \equiv \pm 1 \mod 12$.

(c) Montrer que pour $p > 3$ premier non congru à ± 1 modulo 12, on a le petit théorème de Fermat suivant dans $\mathbb{Z}[\sqrt{3}]$:

$$(x + y\sqrt{3})^p \equiv x - y\sqrt{3} \mod p.$$

(d) Montrer que M_p est premier si et seulement si

$$(2 + \sqrt{3})^{2^{p-1}} \equiv -1 \mod M_p.$$

(e) Soit $(L_i)_{i\geq 0}$ la suite de Lucas-Lehmer définie par

$$L_0 = 4 \text{ et } L_{i+1} = L_i^2 - 2 \mod M_p.$$

Montrer que M_p est premier si et seulement si $L_{p-2} \equiv 0 \mod M_p$.

Exercice 7. — *Soient $n \geq 2$ et $a \in \mathbb{Z}$ tels que $a \wedge n = 1$. Montrer que n est premier si et seulement si*

$$(X + a)^n \equiv X^n + a \mod n.$$

1 Le seul nombre premier vérifiant la condition de l'énoncé est 3. En effet, soit p un nombre premier tel que $p+2$ et $p+4$ soient premiers. Si l'on a $p \equiv 1 \mod 3$, (resp. $p \equiv 2 \mod 3$), alors $p+2$ (resp. $p+4$) est divisible par 3. Les entiers $p+2$ et $p+4$ étant distincts de 3, on a donc $p \equiv 0 \mod 3$, puis $p = 3$. Par ailleurs, 5 et 7 sont premiers.

2 Il n'y a que $p = 3$. En effet, soit p un nombre premier divisant $2^p + 1$. D'après le petit théorème de Fermat, p divise $2^p - 2$, d'où $p = 3$.

3 Les entiers n de la forme $(p-1)(1+kp)$, où k est un entier naturel, conviennent. En effet, pour un tel entier n, on a $n \equiv -1 \mod p$. Par ailleurs, $p-1$ divise n et l'on a $2^{p-1} \equiv 1 \mod p$, donc on a $2^n \equiv 1 \mod p$. Il en résulte que $n2^n + 1 \equiv 0 \mod p$, d'où le résultat.

4 Pour $N = n! + 2$, l'intervalle $[N, N + (n-2)]$ ne contient aucun nombre premier.

5 Si la série $\sum_{p \in \mathcal{P}} \frac{1}{p}$ converge alors la série des $\log(1 - 1/p)$ converge aussi et donc le produit $\prod (1 - 1/p)^{-1}$ converge. On en déduit alors que la série $\sum_n 1/n$ converge, ce qui est faux.

6 (a) Si q est un diviseur de M_p alors l'ordre de la classe de 2 dans $\mathbb{Z}/q\mathbb{Z}$ est égale à p qui doit diviser $q-1$ et donc $q \equiv 1 \mod p$. Comme q est impair, on a aussi $q \equiv 1 \mod 2p$ et donc 2 est un carré modulo q soit $q \equiv \pm 1 \mod 8$.

(b) D'après la loi de réciprocité quadratique, $(\frac{3}{p})(\frac{p}{3}) = (-1)^{(p-1)/2}$ et donc 3 est résidu quadratique modulo p si et seulement si $(\frac{p}{3}) = (-1)^{(p-1)/2}$. Le seul carré modulo 3 autre que 0 est 1, soit $p \equiv 1 \mod 3$ et $p \equiv 1 \mod 4$ ou bien $p \equiv 2 \mod 3$ et $p \equiv 3 \mod 4$, soit en définitive $p \equiv \pm 1 \mod 12$.

(c) Par hypothèse 3 n'est pas un carré modulo p et par conséquent $\sqrt{3}^p = 3^{(p-1)/2}\sqrt{3} \equiv -\sqrt{3} \mod p$ et donc $(x + y\sqrt{3})^p \equiv x - y\sqrt{3} \mod p$.

(d) Supposons alors M_q premier : en remarquant que 2 est un carré modulo M_q, on définit dans $\mathbb{Z}[\sqrt{3}]/(M_q)$: $\tau = \frac{1+\sqrt{3}}{\sqrt{2}}$ et $\bar{\tau} = \frac{1-\sqrt{3}}{\sqrt{2}}$. À partir des relations $\tau^2 = 2 + \sqrt{3}$ et $\tau\bar{\tau} = -1$: $\tau^p = \bar{\tau}$ soit $\tau^{p+1} = -1$ ce qui donne la congruence de l'énoncé $(\tau^2)^{(p+1)/2} \equiv -1 \mod p$ car $\tau^2 = 2 + \sqrt{3}$.

(e) Soit $\alpha = 2 + \sqrt{3}$ et $\bar{\alpha} = 2 - \sqrt{3}$, en remarquant que $\alpha\bar{\alpha} = 1$, on montre aisément par récurrence que $L_i = \alpha^{2^i} + \bar{\alpha}^{2^i}$; la congruence $L_i \equiv 0 \mod n$ est ainsi équivalente à $\alpha^{2^{i+1}} \equiv -1 \mod n$, d'où le résultat.

7 On a déjà vu que pour p premier et pour tout $1 \leq k < p$, le coefficient binomial $\binom{p}{k}$ est divisible par p. Il reste donc à étudier la réciproque. Supposons donc que pour tout $1 \leq i \leq n-1$, on ait $\binom{n}{i} \equiv 0 \mod n$. Regardons alors les congruences modulo n des $\binom{n-1}{i}$. Pour $i = 1$, on a $\binom{n-1}{1} = n - 1 \equiv -1 \mod n$. De la formule de Pascal

$$\binom{n-1}{i} + \binom{n-1}{i+1} = \binom{n}{i+1}$$

et de l'hypothèse $\binom{n}{i} \equiv 0 \mod n$ pour tout $1 \leq i \leq n-1$, on en déduit par une récurrence simple que pour tout $1 \leq i \leq n-1$

$$\binom{n-1}{i} \equiv (-1)^i \mod n.$$

Soit alors d un diviseur strict de n. Rappelons la relation $d\binom{n}{d} = n\binom{n-1}{d-1}$ que l'on interprète combinatoirement comme le nombre de choisir d personnes parmi n et de nommer un chef parmi eux : pour ce faire on peut soit commencer par choisir le groupe puis le chef, ou

inversement choisir le chef puis le reste du groupe. D'après ce qui précède on doit donc avoir

$$\binom{n}{d} \equiv 0 \mod n \quad \text{et} \quad \frac{n}{d}\binom{d-1}{n-1} = \frac{n}{d}(-1)^{d-1},$$

soit $\frac{n}{d}(-1)^{d-1} \equiv 0 \mod n$ ce qui n'est possible que pour $d = 1$, i.e. n ne possède qu'un unique diviseur strict et est donc premier.