

Solutions des exercices de la pl. 18

Exercice 1. a) (Résultat cité à propos du crible d'Eratosthène). Si $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ et $n \notin \mathbb{P}$, montrer qu'il a toujours un facteur premier inférieur ou égal à $\sqrt{n}$.

b) Montrer que si le plus petit facteur premier p d'un nombre n est strictement plus grand que $\sqrt[3]{n}$ alors ou bien n est premier ou bien n est le produit de deux nombres premiers.

Solution 1 a) Soit p_1 le plus petit facteur premier dans la déc. de n . Comme n n'est pas premier $n = p_1 q$ avec $q \geq p_1$, donc $n \geq p_1^2$ i.e. $p_1 \leq \sqrt{n}$.

b) (M1) Par contraposée. La négation de la conclusion est qu'il existe trois nombres p, q, r tous différents de 1 tel que $n = pqr$. SRdG on prend pour p le plus petit diviseur premier de n . Alors $q \geq p$ et $r \geq p$ et donc $n \geq p^3$ ce qui donne la négation de l'hyp.

(M2) Si p est le plus petit facteur premier de n , il vérifie $p > \sqrt[3]{n}$, on considère $m = n/p \in \mathbb{N}$.

On veut montrer que ou bien $m = 1$ ou bien m est premier.

Or $m = \frac{n}{p} < \frac{n}{\sqrt[3]{n}} = n^{2/3}$. Si m n'est pas premier et différent de 1, par le a), il admet un facteur premier $p_1 \leq m^{1/2}$ donc par l'inég. précédente $p_1 < (n^{2/3})^{1/2} = n^{1/3}$. Donc p_1 est un facteur premier de n inférieur strictement à $n^{1/3}$ *contradiction*.

Exercice 2. a) En adaptant la preuve d'Euclide, et en considérant $A = 4(\prod_{i=1}^n p_i) - 1$ montrer qu'il y a une infinité de nombres premiers congrus à -1 modulo 4.

Remarque – Il est aussi vrai, mais cela demande un argument supplémentaire, qu'il y a une infinité de nombres premiers congrus à 1 modulo 4.

b) Adapter encore cette preuve pour montrer qu'il y a une infinité de nombres premiers congrus à -1 modulo 6.

Solution 2 a) *Par l'absurde* Supposons que l'ensemble des nombres premiers congrus à -1 modulo 4 est fini : on le note $\{p_1, \dots, p_k\}$ et on prend $N = 4p_1 \dots p_k - 1$.

Avec la forme de N on voit que N est premier avec tous les nombres p_i .

Mais comme $N \equiv -1 [4]$ il admet nécessairement un diviseur premier congru à -1 mod. 4.

(Par l'absurde sinon, si tous les diviseurs premiers de N étaient congrus à 1 mod. 4 (ou 2) le résultat du produit serait 1 ou 2 ou 4 mod. 4 et donc N serait congru à 1 ou 2 ou 4 modulo 4.)

b) *Par l'absurde* Supposons que l'ensemble des nombres premiers congrus à -1 modulo 6 est fini : on le note $\{p_1, \dots, p_k\}$ et on prend $N = 6p_1 \dots p_k - 1$.

Avec la forme de N on voit que N est premier avec tous les nombres p_i .

Or à part 2, les nombres premiers sont impairs donc congrus à 1, 3, -1 modulo 6. En outre un nombre congru à 3 modulo 6 est divisible par 3.

Donc à part 2 et 3 tous les nombres premiers sont congrus à 1 ou à -1 modulo 6.

Mais comme $N \equiv -1 [6]$, on sait que N n'est divisible ni par 2 ni par 3.

Donc tous les diviseurs premiers de N sont congrus à 1 ou -1 modulo 6.

Sous-par-l'absurde si tous les diviseurs premiers de N étaient congrus à 1 modulo 6 on aurait par produit $N \equiv 1 [6]$, ce qui n'est pas vrai.

Donc N admet au moins un diviseur premier congru à -1 modulo 6, mais ceci est une *contradiction* avec le fait que $N \wedge p_i = 1$ pour chaque p_i premier congru à -1 modulo 6.

Exercice 3 (Nombres premiers et divisibilité des binomiaux).

a) Soit $n \in \mathbb{N}^*$. Montrer que $\binom{2n+1}{n} \leq 4^n$.

b) Pour tout $n \in \mathbb{N}$, on note $\mathbb{P}_n = \{p \in \mathbb{P}, p \leq n\}$.

i) Soit $n = 2k + 1$ un entier impair. Justifier que pour tout nombre premier p tel que $k + 2 \leq p \leq 2k + 1$, p divise $\binom{2k+1}{k}$.

ii) En déduire que si on note N le produit des nombres premiers p tels que $k + 2 \leq p \leq 2k + 1$, on a $N \leq \binom{2k+1}{k}$.

c) Déduire de ce qui précède que $\prod_{p \in \mathbb{P}_n} p < 4^n$.

Solution 3 a) Ah cela nous change des exercices sur $\binom{2n}{n}$ qui est l'unique binomial maximal de la ligne $2n$ du triangle.

Ici on a $\binom{2n+1}{n}$ qui est le binomial maximal, mais il a un frère, qui est $\binom{2n+1}{n+1}$, on va regarder les deux ensembles.

L'idée est que $\binom{2n+1}{n} = \binom{2n+1}{n+1}$ et que si l'on somme les deux, $\binom{2n+1}{n+1} + \binom{2n+1}{n}$ reste inférieur à la somme de tous les binomiaux de cette ligne, donc à 2^{2n+1} .

Ainsi $2\binom{2n+1}{n} \leq 2^{2n+1}$, donc $\binom{2n+1}{n} \leq 4^n$.

b) Questions bien guidées

(i) D'abord $\binom{2k+1}{k} = \frac{(2k+1)(2k)\dots(k+2)}{k!}$.

Pour chaque nombre premier $p \in \llbracket k+2, 2k+1 \rrbracket$, p divise $(2k+1)(2k)\dots(k+2)$

En outre $p \nmid (k!) = 1$ puisque p est premier et $p > k$ donc aucun des facteurs de $k!$ ne peut contenir p comme diviseur premier.

Donc en écrivant $(2k+1)(2k)\dots(k+2) = k! \binom{2k+1}{k}$, on a $p \mid (k!) \binom{2k+1}{k}$ et $p \nmid (k!) = 1$ donc $p \mid \binom{2k+1}{k}$.

(ii) Notons $N = p_1 \dots p_r$. Par le (i), $p_i \mid \binom{2k+1}{k}$ pour chaque i et $p_1, \dots, p_r$ sont deux à deux premiers entre eux, donc $N = p_1 \dots p_r \mid \binom{2k+1}{k}$ en particulier $N \leq \binom{2k+1}{k}$.

c) Là on essaie d'utiliser le b), la récurrence s'impose, encore faut-il comprendre la distinction de cas n pair / n impair.

Notons $P_n = \prod_{p \in \mathbb{P}_n} p$. Notons $H(n) : P_n < 4^n$.

- Initialisation : $P_2 = 2$ et on a donc bien $P_2 < 4^2$ donc $H(2)$ est vraie.

- Hérité : supposons $H(k)$ vrai pour tous les $k \leq n-1$.

Si n est pair alors $P_n = P_{n-1}$ donc $H(n)$ est vraie.

Si n est impair, on l'écrit $n = 2k+1$. Alors en notant N , comme à la question précédente, le produit de tous les nombres premiers entre $k+2$ et $2k+1$, on a : $P_n = P_{2k+1} = N \cdot P_{k+1}$.

Or par Hypothèse de récurrence forte, $P_{k+1} < 4^{k+1}$ et par le b) (ii), $N \leq \binom{2k+1}{k} \leq 4^k$.

Donc $P_n = N \cdot P_{k+1} < 4^{k+1} \cdot 4^k = 4^{2k+1} = 4^n$.

La récurrence est établie. $\square$

Exercice 4. a) Montrer que pour tout $(a, b) \in (\mathbb{Z}^*)^2$, $a^2 \mid b^2 \Leftrightarrow a \mid b$.

b) Montrer que si $a \wedge b = 1$ et $ab = c^n$ (avec a, b, c dans $\mathbb{N}$, $n \in \mathbb{N}^*$) alors il existe a_1, b_1 tels que $a = a_1^n$ et $b = b_1^n$.

c) Montrer que si a, b, m, n dans $\mathbb{N}^*$ vérifient $a^m = b^n$ et $m \wedge n = 1$ alors $\exists c \in \mathbb{N}^*$ tel que $a = c^n$ et $b = c^m$.

Solution 4 a) Sens $\Leftarrow$ trivial. La récip. avec les v_p qui permettent en fait de raisonner par équivalence.

Rappel : $m \mid n$ équivaut à : pour tout $p \in \mathbb{P}$, $v_p(m) \leq v_p(n)$.

Donc $a^2 \mid b^2 \Leftrightarrow \forall p \in \mathbb{P}, v_p(a^2) \leq v_p(b^2) \Leftrightarrow \forall p \in \mathbb{P}, 2v_p(a) \leq 2v_p(b) \Leftrightarrow \forall p \in \mathbb{P}, v_p(a) \leq v_p(b) \Leftrightarrow a \mid b$. $\square$

b) Par D.F.P. on sait qu'il existe $a_1 \in \mathbb{Z}$ tel que $a = a_1^n$ si, et seulement si, pour tout $p \in \mathbb{P}$, $n \mid v_p(a)$.

Or par hyp. $ab = c^n$. donc pour tout $p \in \mathbb{P}$, $v_p(ab) = nv_p(c)$ i.e. $n \mid v_p(a) + v_p(b)$ (*).

Mais comme $a \wedge b = 1$, on sait que pour $p \in \mathbb{P}$, $v_p(a)$ ou $v_p(b)$ est nul.

Donc (*) entraîne que $\forall p \in \mathbb{P}$, $n \mid v_p(a)$ et $n \mid v_p(b)$ et la conclusion. $\square$

c) Pour tout p premier : $v_p(a^m) = mv_p(a) = nv_p(b)$. Comme m et n sont premiers entre eux, on a m divise $v_p(b)$ et n divise $v_p(a)$. Mais plus précisément si on écrit $v_p(b) = mk_p$ on a $nmk_p = mv_p(a)$ donc $v_p(a) = nk_p$. On considère maintenant $c = \prod_{p \in \mathbb{P}} p^{k_p}$.

On a $a = c^n$ et $b = c^m$.