Un problème d'arithmétique

Daniel PERRIN

0. Le problème.

Il s'agit de déterminer les entiers $n > 1$ qui sont tels que n divise $2^n + 1$ ou encore tels que 2^n soit congru à -1 modulo n. On appellera "convenables" (faute de mieux) ces entiers. Ils sont évidemment impairs. Le plus petit nombre convenable est 3 puisqu'on a $2^3 = 8 \equiv -1 \pmod 3$.

Notations et rappels.

On note $v_p(n)$ l'exposant du nombre premier p dans la décomposition de n en produit de facteurs premiers.
On rappelle d'abord que, si m divise n avec n impair, $2^m + 1$ divise $2^n + 1$ (c'est clair en termes de congruences).
On rappelle ensuite le calcul de la fonction d'Euler $\varphi(n)$ (c'est-à-dire le cardinal de $(\mathbf{Z}/n\mathbf{Z})^*$) : si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ est décomposé en produit de facteurs premiers distincts on a :

$$\varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_r^{\alpha_r - 1}(p_r - 1).$$

On rappelle enfin le théorème de Lagrange : dans un groupe fini l'ordre d'un élément divise l'ordre du groupe.

1. Quelques résultats généraux.

Lemme 1.1.
Soient m et n des entiers avec $m > 2$. On suppose qu'on a $2^n \equiv -1 \pmod m$. Si d est le pgcd de n et de $\varphi(m)$ on a $2^d \equiv -1 \pmod m$. En particulier on a $2^d \geq m - 1$.

Démonstration.
Dans le groupe $(\mathbf{Z}/m\mathbf{Z})^*$ on a $2^{\varphi(m)} \equiv 1$ par le théorème de Lagrange, donc l'ordre ω de 2 est un diviseur de $\varphi(m)$. Par ailleurs, on a $2^n \equiv -1 \pmod m$ par hypothèse donc ω est aussi un diviseur de $2n$, donc du *pgcd* δ de $2n$ et de $\varphi(m)$ et on a $2^\delta \equiv 1 \pmod m$. *A priori* on a $\delta = d$ ou $\delta = 2d$. En effet, il est clair que d divise $2n$ et $\varphi(m)$ donc aussi δ. D'autre part on a une relation de Bézout $d = \lambda n + \mu\varphi(m)$ d'où, en multipliant par 2, $2d = \lambda(2n) + 2\mu\varphi(m)$ et il en résulte que δ divise $2d$.
Si on a $\delta = d$ on a $2^d \equiv 1 \pmod m$ donc, comme d divise n, $2^n \equiv 1 \pmod m$ ce qui est absurde car m est plus grand que 2. On a donc à la fois $2^{2d} \equiv 1 \pmod m$ et, en posant $n = dn'$, $2^{dn'} \equiv -1 \pmod m$. On en déduit que n' est impair et, en écrivant $n' = 2k + 1$, on obtient $2^d \equiv -1 \pmod m$.

Lemme 1.2.
Soit N un entier. On suppose qu'on a $N+1 = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec les p_i premiers distincts et les α_i positifs. Soit p un nombre premier impair. On a $v_{p_i}(N^p+1) = \alpha_i$ si $p \neq p_i$ et $v_p(N^p+1) = \alpha_i + 1$ si $p = p_i$.

Démonstration. On écrit $N = -1 + p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ et on calcule N^p par la formule du binôme. On a $N^p = -1 + p\, p_1^{\alpha_1} \cdots p_r^{\alpha_r} + k\, p_i^{2\alpha_i}$, d'où le résultat.

Le théorème suivant résume l'essentiel des propriétés des nombres convenables :

Théorème 1.3.
Soit n un entier convenable. On écrit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec les p_i premiers tels que $p_1 < \cdots < p_r$ et les α_i positifs et on pose, pour $i \geq 1$, $m_i = p_1^{\alpha_1} \cdots p_i^{\alpha_i}$.
1) On a $p_1 = 3$.
2) On a, pour tout $i < r$, $2^{m_i} \equiv -1 \pmod{p_{i+1}}$ (ou encore p_{i+1} divise $2^{m_i}+1$).
3) Pour tout $i \geq 1$ le nombre m_i est convenable.
4) Soit $m = p_1^{\beta_1} \cdots p_r^{\beta_r}$ avec $\beta_i \geq \alpha_i$ pour tout i. Alors, m est convenable.
5) Soient $q_1, \cdots, q_s$ des diviseurs premiers de 2^n+1. Alors $nq_1 \cdots q_s$ est convenable (donc aussi $nq_1^{\gamma_1} \cdots q_r^{\gamma_r}$ avec les $\gamma_i \geq 0$).
6) Les nombres $p_1^{\alpha_1} \cdots p_{r-1}^{\alpha_{r-1}} p_r^{\beta_r}$, avec $\beta_r > 0$ sont convenables.

Démonstration.
1) On a $2^n \equiv -1 \pmod{p_1}$. Comme p_1 est premier on a $\varphi(p_1) = p_1 - 1$ et comme p_1 est le plus petit diviseur premier de n, $p_1 - 1$ et n sont premiers entre eux. On a donc $2^1 \geq p_1 - 1$ par le lemme 1.1, donc $p_1 = 3$.

2) Soit $d = pgcd\,(n, p_{i+1} - 1)$. Il est clair que d divise m_i. Comme on a $2^n \equiv -1 \pmod{p_{i+1}}$, le lemme 1.1 montre qu'on a aussi $2^d \equiv -1 \pmod{p_{i+1}}$ donc $2^{m_i} \equiv \pm 1 \pmod{p_{i+1}}$. Mais on ne peut avoir $2^{m_i} \equiv 1$ (sinon on aurait $2^n \equiv 1 \pmod{p_{i+1}}$), d'où le résultat.

3) On a $2^n \equiv -1 \pmod{m_i}$ donc, par le lemme 1.1, $2^d \equiv -1 \pmod{m_i}$ avec $d = pgcd\,(n, \varphi(m_i))$. Comme les facteurs premiers $p_k > p_i$ ne divisent pas $\varphi(m_i)$, on voit que d divise m_i. Précisément on a $m_i = db$ avec b impair (car m_i l'est) d'où encore $2^{m_i} \equiv -1 \pmod{m_i}$ ce qui montre que m_i est convenable.

4) Par récurrence on se ramène à montrer qu'on a, pour chaque i, $(2^n)^{p_i} \equiv -1 \pmod{p_i^{\alpha_i+1}}$. Mais on sait qu'on a $2^n \equiv -1 \pmod{p_i^{\alpha_i}}$, donc $2^n = -1 + kp_i^{\alpha_i}$. On conclut par le lemme 1.2.

5) Par récurrence sur s il suffit de montrer que si n est convenable et si p premier divise $2^n + 1$, np est encore convenable. Si p divise n cela résulte du point 4). Sinon, il s'agit de montrer qu'on a $2^{np} \equiv -1 \pmod{np}$ et il suffit de montrer cette congruence modulo n et modulo p. Pour n c'est évident (car p est impair) et pour p on a $2^p \equiv 2 \pmod{p}$ par le petit théorème de Fermat d'où la conclusion puisque p divise $2^n + 1$.

6) Cela résulte de 3), 2) et 5).

2. Construction de nombres convenables.

a) Augmenter le nombre de facteurs premiers.

Le théorème 1.3 indique une méthode récursive de construction de nombres convenables : à partir d'un nombre convenable n on peut :
• augmenter l'exposant de ses facteurs premiers (1.3.4),
• multiplier n par un diviseur premier de $2^n + 1$ (1.3.5).
Pour obtenir des nombres convenables avec beaucoup de facteurs premiers il faut donc montrer que $2^n + 1$ contient d'autres facteurs que ceux de n. C'est l'objet du résultat suivant :

Proposition 2.1.
Soit n un nombre convenable différent de 3. Alors 2^n+1 a d'autres facteurs premiers que ceux de n.

Démonstration. On raisonne par l'absurde en supposant qu'il existe un nombre convenable $n > 3$ qui n'a pas d'autres facteurs premiers que ceux de n. On pose $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} = mp_r$. On a $m > 1$ (sinon $n = p_r = 3$ en vertu de 1.3.1) et le nombre m est convenable en vertu de 1.3.3 si $\alpha_r = 1$ ou de 1.3.6 sinon. Comme $2^m + 1$ divise $2^n + 1$, on voit que $2^m + 1$ n'a pas d'autres facteurs premiers que les p_i. Inversement, $2^m + 1$ est multiple de tous les p_i. En effet, comme m est convenable $2^m + 1$ est multiple de m, donc de tous les p_i, sauf peut-être de p_r dans le cas $\alpha_r = 1$. Mais, dans ce cas, $2^m + 1$ est multiple de p_r en vertu de 1.3.2.
On pose donc $2^m + 1 = p_1^{\beta_1} \cdots p_r^{\beta_r}$ avec $\beta_i > 0$. Comme $2^n + 1 = 2^{mp_r} + 1$ n'a pas non plus d'autres facteurs premiers que les p_i il résulte de 1.2 qu'on a $2^{mp_r} + 1 \leq p_r(2^m + 1)$ (car seule la valuation p_r-adique augmente de 1). On conclut alors grâce au lemme suivant :

Lemme 2.2.
Soient m et p des entiers ≥ 2. On a $2^{mp} + 1 > p(2^m + 1)$.

Démonstration. En effet, on a

$$2^{mp} + 1 > \underbrace{2^m \times \cdots \times 2^m}_{p \text{ fois}} \geq 4^{p-1} \times 2^m \geq 2p \times 2^m > p\,2^m + p.$$

b) Exemples.

On a vu que les nombres 3^α (pour $\alpha > 0$) sont convenables. On étudie les nombres $F_\alpha = 2^{3^\alpha} + 1$. Bien entendu ces nombres sont impairs. Comme on a $F_1 = 8 + 1 = 9$ la proposition suivante est une conséquence de 1.2, 2.1, 2.2 :

Proposition 2.3.
1) On a $v_3(F_\alpha) = \alpha + 1$.
2) F_α divise F_β pour $\beta \geq \alpha$.
3) Si p est un nombre premier et si $v_p(F_\alpha) = r$, on a $v_p(F_\beta) = r$ pour tout $\beta \geq \alpha$.
4) On a $F_{\alpha+1} > 3F_\alpha$.
5) Le nombre de facteurs premiers de F_α est une fonction strictement croissante de α.

Exemples 2.4. On a $F_1 = 9 = 3^2$, $F_2 = 513 = 3^3 \times 19$, $F_3 = 3^4 \times 19 \times 87211$, $F_4 = 2^{81} + 1 = 3^5 \times 19 \times 87211 \times 163 \times 135433 \times 272010961$.

Proposition 2.5.
Soit α un nombre > 0 et posons $F_\alpha = 3^{\alpha+1} p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Alors tous les nombres de

la forme $3^\beta p_1^{\beta_1} \cdots p_r^{\beta_r}$ *avec* $\beta \geq \alpha$ *et* $\beta_i \geq 0$ *sont convenables (en particulier* F_α *est convenable ainsi que tous ses diviseurs qui contiennent le facteur* 3^α*).*

Démonstration. Comme 3^α est convenable, cela résulte de 1.3.5.

Remarque 2.6. Pour avoir un nombre convenable avec un nombre donné r de facteurs premiers distincts on regarde le nombre F_r qui a au moins r facteurs premiers et on prend pour n un diviseur de F_r avec exactement r facteurs premiers distincts (dont le 3^r, bien entendu). Cela résout le problème des olympiades.

Exemples 2.7. Voici quelques petits exemples de nombres convenables (outre les puissances de 3) : $3^2 \times 19 = 171$, $3^3 \times 87211$, $3^3 \times 19 \times 87211$, $3^4 \times 163$, ... On peut bien entendu fabriquer des nombres convenables à partir d'autres nombres que les F_α. Par exemple, à $n = 9 \times 19 = 171$ on peut ajouter l'un des facteurs premiers de $2^{171} + 1$, i.e. :

$$2^{171} + 1 = 3^3 \times 19^2 \times 571 \times 174763 \times 160465489 \times$$
$$191774583879402681163497666122 11.$$

Ainsi $9 \times 19 \times 571 = 97641$ est convenable. En dessous de 10000 il n'y a que 14 nombres convenables : les 3^α avec $1 \leq \alpha \leq 8$, les $3^\alpha \times 19$ avec $2 \leq \alpha \leq 5$ et enfin $3^2 \times 19^2$ et $3^3 \times 19^2$.

Remarque 2.8. On peut noter que les facteurs premiers des nombres convenables sont congrus à 1 ou 3 modulo 8. En effet, si p est un tel facteur, on $2^n \equiv -1 \pmod{p}$ donc $(-2)^n \equiv 1 \pmod{p}$. Comme n est impair on voit que -2 est un carré modulo p. On en déduit le résultat (cf. par exemple Serre, Cours d'arithmétique). On constate que les facteurs congrus à 1 sont beaucoup plus rares que les autres.