Feuille d'exercices 5

Avertissement : tous les exercices ne seront pas traités durant les séances ; pour en suivre l'avancement veuillez consulter mon site personnel dans la rubrique *Forum*.

Exercice 1. — *Un entier $n \geq 1$ est dit de Carmichael s'il n'est pas premier et si pour tout entier a premier avec n, $a^{n-1} \equiv 1 \mod n$. On note $\lambda(n)$ l'ordre maximal d'un élément de $(\mathbb{Z}/n\mathbb{Z})^\times$.*

1. *Montrer que n est de Carmichael si et seulement si $\lambda(n)$ divise $n-1$.*
2. *Soit $n \geq 2$ un entier. Montrez que les conditions suivantes sont équivalentes*
   (i) n est sans facteurs carrés et $p|n \Rightarrow p-1|n-1$, pour p premier ;
   (ii) $\forall a \in \mathbb{Z}$, on a $a^n \equiv a \mod n$;
   (iii) $\forall a \in \mathbb{Z}$ premier à n, on a $a^{n-1} \equiv 1 \mod n$.
3. *Montrer qu'un nombre pair n'est pas de Carmichael et qu'un nombre de Carmichael est divisible par au moins trois nombres premiers distincts.*
4. *Montrez que $n = 561 = 3.11.17$ est un nombre de Carmichael.*
5. *Soit $m \geq 1$ tel que $6m+1$, $12m+1$ et $18m+1$ sont premiers. Montrer alors que $N(m) = (6m+1)(12m+1)(18m+1)$ est un nombre de Carmichael.*

Remarque : en 1992, Alford, Granville et Pomerance ont prouvé qu'il existait une infinité de nombres de Carmichael ; en fait si on note $C(x)$ le cardinal de l'ensemble des nombres de Carmichael inférieur à x, on a montré $C(x) > x^{1/8}$. Sur ce sujet Erdos a formulé une conjecture précise. Pour $k \geq 4$ et $m \geq 1$, on pose

$$M_k(m) = (6m+1)(12m+1)\prod_{i=1}^{k-2}(9 \times 2^i m + 1).$$

Si tous les facteurs de $M_k(m)$ sont premiers alors $M_k(m)$ est un nombre de Carmichael avec k facteurs ; cette formule n'a jusqu'à présent que donné des nombres avec au plus une quinzaine de facteurs. On ne sait pas encore s'il existe un nombre infini de nombres de Carmichael avec k facteurs ni s'il existe des nombres de Carmichael avec k facteurs pour k arbitrairement grand. Récemment Zhang a construit des nombres de Carmichael avec 1300 facteurs et 8300 chiffres.

Exercice 2. — *Montrez que si $a^n - 1$ est premier alors $a = 2$ et n est premier ; $M_p = 2^p - 1$ est appelé un nombre de Mersenne pour p premier. On veut montrer le test de primalité de Lucas-Lehmer : M_q est premier ($q \geq 3$ premier) si et seulement si $(2+\sqrt{3})^{2^{q-1}} \equiv -1 \mod M_q$.*

(i) Montrez que l'anneau $A = \mathbb{Z}[\sqrt{3}]$ est euclidien et caractérisez les unités.

(ii) Remarquez que pour q impair, $M_q \equiv 7 \mod 12$ et en déduire qu'il existe un premier $p \not\equiv \pm 1 \mod 12$ divisant M_q et remarquer que p reste irréductible dans $\mathbb{Z}[\sqrt{3}]$. Montrez que si M_q vérifie la congruence ci-dessus, alors $p = M_q$.

(iii) En utilisant la loi de réciprocité quadratique, montrez que 3 est un résidu quadratique modulo $p \neq 2, 3$ si et seulement si $p \equiv \pm 1 \mod 12$. En supposant M_q est premier, montrez le petit théorème de Fermat suivant dans $\mathbb{Z}[\sqrt{3}]$: $(x+y\sqrt{3})^p \equiv x - y\sqrt{3} \mod p$. En remarquant que 2 est un carré modulo p, on définit dans $\mathbb{Z}[\sqrt{3}]/(p)$: $\tau = \frac{1+\sqrt{3}}{\sqrt{2}}$ et $\bar{\tau} = \frac{1-\sqrt{3}}{\sqrt{2}}$. A partir des relations $\tau^2 = 2+\sqrt{3}$ et $\tau\bar{\tau} = -1$, en déduire la congruence de l'énoncé.

(iv) Montrez le test de primalité suivant sur M_q pour $q \geq 3$ premier : soit $(L_i)_{i \geq 0}$ la suite de Lucas-Lehmer définie par $L_0 = 4$ et $L_{i+1} = L_i^2 - 2 \mod M_q$, alors M_q est premier si et seulement si $L_{q-2} \equiv 0 \mod M_q$.

Exercice 3. — *Soient p et q deux nombres premiers impairs distincts. Posons*

$$n = pq \quad et \quad d = \mathrm{pgcd}(p-1, q-1).$$

1. *Soit a un entier compris entre 1 et n. Montrer que n est pseudo-premier en base a si et seulement si on a $a^d \equiv 1 \mod n$.*
2. *En déduire que si l'on a $2^d \leq n$, alors 2 est un témoin de Fermat pour n.*

3. *Quel est le nombre d'entiers a tels que n soit pseudo-premier en base a ?*

Exercice 4. — *Soient p un nombre premier et h un entier naturel non nul $< p$. Posons $n = hp + 1$ et supposons $2^h \not\equiv 1 \mod n$. Montrer l'équivalence*

$$n \text{ est premier} \iff 2^{n-1} \equiv 1 \mod n.$$

Exercice 5. — *Soit n un entier impair vérifiant les deux conditions suivantes :*

1. *on a $a^{\frac{n-1}{2}} \equiv \pm 1 \mod n$ pour tout entier a premier avec n.*
2. *Il existe un entier b tel que l'on ait $b^{\frac{n-1}{2}} \equiv -1 \mod n$. Montrer que n est premier.*

Exercice 6. — *(Test de Pocklington, 1914)*

1. *Démontrer l'énoncé suivant :*

   Théorème : soit n un entier > 1. Supposons qu'il existe un nombre premier q divisant $n-1$ vérifiant l'inégalité $q > \sqrt{n} - 1$, et qu'il existe un entier $a \geq 1$ tels que l'on ait

   $$a^{n-1} \equiv 1 \mod n \quad \text{et} \quad \operatorname{pgcd}\left(a^{\frac{n-1}{q}} - 1, n\right) = 1.$$

   Alors, n est premier.
2. *Soit n un nombre premier tel que $n-1$ soit divisible par un nombre premier q tel que $q > \sqrt{n} - 1$. Quelle est la « probabilité » pour qu'un entier a, choisi au hasard entre 1 et $n-1$, vérifie la condition du théorème ? Que peut-on en conclure ?*
3. *Montrer en utilisant le critère précédent que 4127 est premier.*

Exercice 7. — *(Critère de Lehmer-Pocklington) Cet exercice fournit une version plus générale du test de Pocklington.*

Théorème : soit n un entier > 1. Posons $n - 1 = uv$ où u et v sont deux entiers. Supposons que pour chaque facteur premier q de u, il existe un entier a_q tel que, si q^r est la plus grande puissance de q qui divise u, on ait

$$a_q^{q^r} \equiv 1 \mod n \quad \text{et} \quad \operatorname{pgcd}\left(a_q^{q^{r-1}} - 1, n\right) = 1.$$

Alors, tout facteur premier de n est congru à 1 modulo u. De plus, si l'on a $v \leq u + 1$, alors n est premier.

1. *Montrer le lemme suivant :*

   Lemme Soit n un entier > 1. On écrit $n - 1 = q^r m$, avec q premier et $r \geq 1$. Supposons qu'il existe un entier a tel que l'on ait

   $$a^{q^r} \equiv 1 \mod n \quad \text{et} \quad \operatorname{pgcd}\left(a^{q^{r-1}} - 1, n\right) = 1.$$

   Alors, tout facteur premier de n est congru à 1 modulo q^r.
2. *En déduire le théorème.*
3. *Montrer avec le critère précédent que 12289 est premier.*
4. *En déduire le critère de primalité de Proth (1878) :*

   Proposition Soient h et n deux entiers naturels tels que h soit impair et que $2^n > h$. Posons $N = 2^n h + 1$. S'il existe un entier $a > 1$ tel que l'on ait

   $$a^{\frac{N-1}{2}} \equiv -1 \mod N,$$

   alors N est premier.

1. Solutions

1 (1) Si n est de Carmichael, de manière évidente, on a $\lambda(n)$ qui divise $n-1$. Réciproquement soit a_0 un élément d'ordre $\lambda(n)$ et $a \in (\mathbb{Z}/n\mathbb{Z})^\times$; l'élément $a_0 a$ est d'ordre le ppcm de $\lambda(n)$ et l'ordre de a de sorte que par maximalité de $\lambda(n)$ on a $a^{\lambda(n)}1$ et donc $a^{n-1}=1$, d'où le résultat.

(2) (i) implique (ii) : Supposons $n = p_1.\cdots.p_s$ les p_i étant distincts deux à deux. Le théorème chinois donne alors $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s\mathbb{Z}$ et la congruence $a^n \equiv a \mod n$ est équivalente à $a^n \equiv a \mod p_i$ pour tout i· Pour i fixé, si p_i divise a le résultat est clair, sinon la congruence est équivalente à $a^{n-1} \equiv 1 \mod p_i$. Par hypothèse $p_i - 1$ divise $n-1$, le petit théorème de Fermat donne alors $a^{p_i-1} \equiv 1 \mod p_i$ soit $a^{n-1} \equiv 1 \mod p_i$.

(ii) implique (iii) : si a et n sont premiers entre eux l'implication est évidente car a est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

(iii) implique (i) : Commençons par montrer que n est sans facteur carré : supposons par l'absurde que $n = p^r q$ avec $r > 1$, p premier et q non divisible par p. Pour a non divisible par p, on a $a^{n-1} \equiv 1 \mod p^r$. On choisit alors un élément a de $(\mathbb{Z}/p^r\mathbb{Z})^\times$ d'ordre p (c'est possible car $r > 1$). On en déduit alors que p divise $p^r q - 1$ ce qui n'est pas. Montrons ensuite la deuxième propriété : soit p premier divisant n et soit a tel que sa classe modulo p engendre $(\mathbb{Z}/p\mathbb{Z})^\times$. La congruence $a^n \equiv a \mod n$ implique $a^n \equiv a \mod p$ soit $a^{n-1} \equiv 1 \mod p$ et donc $p-1$ divise $n-1$ car $p-1$ est l'ordre de a.

(3) Si n est de Carmichael divisible par un nombre premier impair, on en déduit que $p-1$ divise $n-1$ et donc $n-1$ est pair. En utilisant la même propriété si $n = pq$ alors $pq - 1 \equiv q - 1 \mod p-1$ et donc $p-1$ divise $q-1$ qui divise $p-1$ soit $p = q$ ce qui n'est pas.

(4) Il suffit de remarquer que 560 est multiple de $2, 10, 15$ et par suite $x^{560} \equiv 1$ dans $(\mathbb{Z}/3\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$, dans $(\mathbb{Z}/11\mathbb{Z})^\times \simeq \mathbb{Z}/10\mathbb{Z}$ et dans $(\mathbb{Z}/17\mathbb{Z})^\times \simeq \mathbb{Z}/16\mathbb{Z}$ et donc dans $(\mathbb{Z}/561\mathbb{Z})^\times$ d'après le lemme chinois.

(6) Il suffit de vérifier le critère de la question 2) ce qui est immédiat.

2 La factorisation $a^{pq} - 1 = (a^p - 1)(a^{p(q-1)} + \cdots + a^p + 1)$ donne l'implication M_n irréductible alors $a = 2$ et n premier.

(i) On considère le sthasme $v : x + y\sqrt{3} \mapsto |x^2 - 3y^2|$, soit la valeur absolue de la norme N. Soient alors $\alpha, \beta \in\in \mathbb{Z}[\sqrt{3}]$; $\alpha/\beta = r + s\sqrt{3}$ avec $r, s \in \mathbb{Q}$ que l'on approxime par des entiers x, y avec une erreur inférieure à $1/2$: $|x-r| \leq 1/2$ et $|y-s| \leq 1/2$. On obtient alors $-3/4 \leq (r-x)^2 - 3(s-y)^2 \leq 1/4$ soit $v(\alpha/\beta - (x+y\sqrt{3})) \leq 3/4$ et donc $v(\alpha - \beta(x+y\sqrt{3})) < v(\beta)$.

Si $z \in \mathbb{Z}[\sqrt{3}]$ est inversible alors $N(zz^{-1}) = N(z)N(z^{-1})$ et donc $N(z) \in \mathbb{Z}^\times = \{\pm 1\}$. Réciproquement si $N(x + y\sqrt{3}) = \epsilon = \pm 1$ alors $\epsilon(x - y\sqrt{3})$ est son inverse. En particulier $2 + \sqrt{3}$ est inversible d'inverse $2 - \sqrt{3}$.

(ii) On a $M_3 \equiv 7 \mod 12$; par récurrence supposons $M_n \equiv 7 \mod 12$ alors $M_{n+2} = (M_n + 1)^4 - 1 \equiv 8^4 - 1 \mod 12$; or $8^4 - 1 \equiv 3 \mod 12$, d'où le résultat. Remarquons que 2 et 3 ne divise pas M_q pour q impair, de sorte que si p divise M_q alors $p \equiv \pm 1, \pm 5 \mod 12$; tous les diviseurs p de M_q ne peuvent pas être congrus à $\pm 1 \mod 12$ car sinon il en serait de même de M_q. Soit donc p premier divisant M_q avec $p \not\equiv \pm 1 \mod 12$ et montrons que p reste irréductible dans $\mathbb{Z}[\sqrt{3}]$. On raisonne par l'absurde : $p = \alpha\beta$ soit $p^2 = N(\alpha)N(\beta)$ et $p = \pm N(\alpha)$ car β n'est pas inversible. On en déduit alors $p = \pm(x^2 - 3y^2)$; or comme $x^2 - 3y^2$ est un nombre premier distinct de $\pm 2, \pm 3$, on a alors $x^2 - 3y^2 \equiv 1 \mod 3$ et $x^2 - 3y^2 \equiv 1 \mod 4$ soit $p \equiv \pm 1 \mod 12$ ce qui n'est pas.

Supposons que $(2 + \sqrt{3})^{2^{q-1}} \equiv -1 \mod M_q$, on va alors montrer que $p = M_q$. Comme $\mathbb{Z}[\sqrt{3}]$ est principal, et p est irréductible, alors le quotient $(\mathbb{Z}[\sqrt{3}]/(p))^\times$ est un corps de cardinal p^2. La congruence $(2 + \sqrt{3})^{2^{q-1}} \equiv -1 \mod M_q$ montre alors que l'ordre de $2 + \sqrt{3}$ est d'ordre 2^q dans $(\mathbb{Z}[\sqrt{3}]/(p))^\times$; donc 2^q divise $p^2 - 1$. On écrit $M_q = pa$, soit $p^2 \equiv 1 \mod M_q$ et $ap \equiv -1 \mod 2^q$ soit $ap \equiv -p^2 \mod 2^q$. Comme p est inversible modulo 2^q, on obtient $a + p \equiv 0 \mod 2^q$, or $ap < 2^q \leq a + p$ soit $(a-1)p \leq a - 1$ soit $a = 1$ et $p = M_q$.

(iii) La loi de réciprocité quadratique donne $(\frac{3}{p})(\frac{p}{3}) = (-1)^{(p-1)/2}$; 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 $p \equiv \pm 1 \mod 12$.

Comme $p = M_q$ premier est congru à 7 modulo 12, on en déduit que 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 $(x + y\sqrt{3})^p \equiv x - y\sqrt{3} \mod p$. On considère les éléments $\tau, \bar{\tau}$ de l'énoncé ; $\tau^p = \bar{\tau}$ soit $\tau^{p+1} = -1$ ce qui donne la congruence de l'énoncé $(\tau^2)^{(p+1)/2} \equiv -1 \mod p$ car $\tau^2 = 2 + \sqrt{3}$.

(iv) En posant $\alpha = 2 + \sqrt{3}$ 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.

3 1) Supposons que l'on ait $a^{n-1} \equiv 1 \mod n$. On a l'égalité

$$n-1 = (p-1)q + (q-1). \tag{1}$$

Puisque l'on a $a^{q-1} \equiv 1 \mod q$, on obtient

$$a^{n-1} = \left(a^q\right)^{p-1} a^{q-1} \equiv a^{p-1} \mod q.$$

De même, on a la congruence

$$a^{n-1} \equiv a^{q-1} \mod p.$$

On en déduit que l'on a

$$a^{p-1} \equiv 1 \mod q \quad \text{et} \quad a^{q-1} \equiv 1 \mod p.$$

Les congruences $a^{p-1} \equiv 1 \mod p$ et $a^{q-1} \equiv 1 \mod q$ entraînent alors

$$a^{p-1} \equiv 1 \mod n \quad \text{et} \quad a^{q-1} \equiv 1 \mod n.$$

Il en résulte que n divise le pgcd de $a^{p-1}-1$ et $a^{q-1}-1$, qui n'est autre que $a^d - 1$, autrement dit, on a $a^d \equiv 1 \mod n$.
Inversement, si $a^d \equiv 1 \mod n$, on a $a^{p-1} \equiv 1 \mod n$ et $a^{q-1} \equiv 1 \mod n$, et l'égalité (1) implique $a^{n-1} \equiv 1 \mod n$. 2) C'est une conséquence directe de la question précédente. 3) Il s'agit de compter les entiers a tels que $1 < a < n$ et $a^d \equiv 1 \mod n$. Cette congruence est équivalente à la condition

$$a^d \equiv 1 \mod p \quad \text{et} \quad a^d \equiv 1 \mod q.$$

Puisque d divise $p-1$ et que $\mathbb{F}_p^*$ est cyclique d'ordre $p-1$, l'équation $x^d = 1$ possède d solutions dans $\mathbb{F}_p^*$. La même assertion vaut en remplaçant p par q. Compte tenu du théorème chinois, il y a donc $d^2 - 1$ bases a en lesquelles n est pseudo-premier.

4 Supposons $2^{n-1} \equiv 1 \mod n$. Soit d l'ordre multiplicatif de 2 modulo n. L'entier d divise $n-1 = hp$. La condition $2^h \not\equiv 1 \mod n$ entraîne que d ne divise pas h. D'après le théorème de Gauss, on en déduit que p divise d : si p ne divise pas d, d et p sont premiers entre eux. Puisque d divise $\varphi(n)$ (théorème d'Euler), p divise $\varphi(n)$. Soit $n = p_1^{n_1} \cdots p_r^{n_r}$ la décomposition de n en facteurs premiers. On a

$$\varphi(n) = p_1^{n_1-1} \cdots p_r^{n_r-1}(p_1-1)\cdots(p_r-1).$$

Par hypothèse, p divise $n-1$, donc il ne divise pas n, ainsi il existe i tel que $p_i \equiv 1 \mod p$. Posons $n = p_i m$. Vérifions que l'on a $m = 1$, ce qui prouvera que n est premier. On a $m \equiv 1 \mod p$ car tel est le cas de p_i et n. Posons $p_i = up + 1$ et $m = vp + 1$ où $u, v \in \mathbb{N}$. On a l'égalité $hp + 1 = (up+1)(vp+1)$, d'où $h = uvp + u + v$. L'inégalité $h < p$ entraîne alors $v = 0$ et l'assertion.
Inversement, si n est premier, on a $n \geq 3$ puis $2^{n-1} \equiv 1 \mod n$.

5 Pour tout entier a premier à n, on a $a^{n-1} \equiv 1 \mod n$. Ainsi n est sans facteurs carrés (exercice 13 de la première feuille d'exercices). Il suffit donc de prouver que n ne peut pas s'écrire sous la forme mm' avec m et $m' > 1$ et $\text{pgcd}(m, m') = 1$. Supposons qu'il existe deux tels entiers m et m'. D'après le théorème chinois, il existe un entier c tel que l'on ait

$$c \equiv b \mod m \quad \text{et} \quad c \equiv 1 \mod m'.$$

On a donc

$$c^{\frac{n-1}{2}} \equiv b^{\frac{n-1}{2}} \equiv -1 \mod m \quad \text{et} \quad c^{\frac{n-1}{2}} \equiv 1 \mod m'.$$

L'entier c est premier avec n car tel est le cas de b, et $c^{\frac{n-1}{2}}$ ne peut être congru à 1 ni à -1 modulo n, sinon m ou m' diviserait 2, ce qui n'est pas, vu que m et m' sont impairs > 1. On obtient ainsi une contradiction à la première condition de l'énoncé, d'où le résultat. [Inversement, on notera que si n est premier, les deux conditions de l'énoncé sont satisfaites].

6 1) Supposons que n ne soit pas premier. Il existe alors un nombre premier $p \leq \sqrt{n}$ qui divise n. On a $q > p-1$, donc q est premier avec $p-1$. Par suite, il existe un entier $u \geq 1$ tel que l'on ait $uq \equiv 1 \mod p-1$. D'après la congruence $a^{n-1} \equiv 1 \mod n$, p ne divise pas a, et l'on obtient ainsi

$$a^{\frac{n-1}{q}} \equiv a^{uq\frac{(n-1)}{q}} = a^{u(n-1)} \equiv 1 \mod p,$$

ce qui contredit le fait que les entiers $a^{\frac{n-1}{q}} - 1$ et n soient premiers entre eux, d'où le théorème. 2) Puisque n est

premier, le groupe $\big(\mathbb{Z}/n\mathbb{Z}\big)^*$ est cyclique d'ordre $\varphi(n) = n-1$. Pour tout a non divisible par n, on a $a^{n-1} \equiv 1 \mod n$. De plus, la condition

$$\mathrm{pgcd}\big(a^{\frac{n-1}{q}} - 1, n\big) \neq 1$$

signifie que n divise $a^{\frac{n-1}{q}} - 1$. L'ensemble des éléments $x \in \big(\mathbb{Z}/n\mathbb{Z}\big)^*$ tels que $x^{\frac{n-1}{q}} = 1$ est un sous-groupe de $\big(\mathbb{Z}/n\mathbb{Z}\big)^*$ d'ordre $(n-1)/q$. Il y a donc exactement $(n-1)/q$ éléments a tels que $1 \leq a < n$ et que n divise $a^{\frac{n-1}{q}} - 1$. Le nombre d'entiers a tels que $1 \leq a < n$ vérifiant la condition de l'énoncé est donc

$$(n-1) - \frac{n-1}{q} = (n-1)\left(1 - \frac{1}{q}\right).$$

Il en résulte que la $\ll$ probabilité $\gg$ cherchée est $1 - \frac{1}{q}$. On constate ainsi heuristiquement que le critère de Pocklington est très efficace pour démontrer qu'un entier est premier, si tel est le cas, sous réserve qu'il existe un diviseur premier q de $n-1$ plus grand que $\sqrt{n}-1$. En effet, dans ce cas, on a $q \geq \sqrt{n}$ et la probabilité pour ce test fonctionne est alors plus grande que $1 - \frac{1}{\sqrt{n}}$, qui tend vers 1 quand n tend vers l'infini. Signalons qu'en pratique, dans l'application de ce critère, l'entier $a = 2$ convient très souvent. 3) Posons $n = 4127$. La décomposition de $n-1$ en facteurs premiers est donnée par l'égalité $n - 1 = 2 \times 2063$. L'entier $q = 2063$ est premier, car il n'est pas divisible par un nombre premier < 45. Par ailleurs, on a $q > \sqrt{n} - 1 \simeq 63,2$. On vérifie alors que l'on a $2^{n-1} \equiv 1 \mod n$ et que n n'est pas divisible par 3, d'où l'assertion. Remarquons que l'on peut aussi utiliser l'énoncé de l'exercice 2 pour démontrer que 4127 est premier.

7 1) Soit p un facteur premier de n. Il résulte des hypothèses faites que l'on a

$$a^{q^r} \equiv 1 \mod p \quad \text{et} \quad a^{q^{r-1}} \not\equiv 1 \mod p.$$

Puisque q est premier, on en déduit que q^r est l'ordre de a modulo p, donc q^r divise $p-1$. 2) Soit $u = q_1^{r_1} \cdots q_s^{r_s}$ la décomposition de u en facteurs premiers. Soit p un facteur premier de n. D'après la première question, pour tout $i = 1, \cdots, r$, on a $p \equiv 1 \mod q_i^{r_i}$, par suite, on a $p \equiv 1 \mod u$. En particulier, on a $p > u$. Si l'on a $v \leq u+1$, alors $n = 1 + uv < (u+1)^2 \leq p^2$. Ainsi, tout facteur premier de n est $> \sqrt{n}$, ce qui entraîne que n est premier. 3) Posons $n = 12289$. On a $n - 1 = 2^{12} \times 3$. On vérifie que l'on a

$$3^{2^8} = 3^{256} \equiv -1 \mod n. \tag{1}$$

Le calcul de 3^{2^8} nécessite huit multiplications. On a $3^8 = 6561$ et l'on vérifie les congruences

$$3^{16} \equiv 10643 \mod n, \quad 3^{32} \equiv 5736 \mod n, \quad 3^{64} \equiv 4043 \mod n, \quad 3^{128} \equiv 1479 \mod n,$$

d'où l'on déduit (1). On a donc

$$3^{2^9} \equiv 1 \mod n.$$

On prend alors $u = 2^9$ et $v = 24$ et le théorème entraîne que n est premier. 4) On utilise le théorème avec $u = 2^n$ et $v = h$. D'après l'hypothèse faite, on a

$$v < u \quad \text{et} \quad \big(a^h\big)^{2^n} = a^{N-1} \equiv 1 \mod N.$$

Par ailleurs, on a $\frac{N-1}{2} = 2^{n-1}h$, de sorte que N étant impair, on a

$$\Big(\big(a^h\big)^{2^{n-1}} - 1\Big) \wedge N = 1.$$

Les conditions du théorème sont donc satisfaites avec l'entier a^h, ce qui prouve que N est premier.