SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

HENRI COHEN

Tests de primalité d'après Adleman, Rumely, Pomerance et Lenstra

Séminaire de théorie des nombres de Grenoble, tome 9 (1980-1981), exp. n° 3, p. 1-32

<http://www.numdam.org/item?id=STNG_1980-1981__9__A3_0>

Séminaire de Théorie des Nombres
2, 11 et 18 juin 1981
Grenoble

TESTS DE PRIMALITE
D'APRES ADLEMAN, RUMELY, POMERANCE ET LENSTRA

par Henri COHEN

1. - HISTORIQUE

La méthode la plus ancienne et la plus simple pour tester si un nombre n est premier ou non consiste à essayer de factoriser n. En utilisant le fait qu'un nombre non premier n possède un diviseur r tel que $1 < r \leq \sqrt{n}$, on obtient ainsi une méthode praticable sur un ordinateur jusqu'à $n = 10^{16}$ environ. Toutefois c'est une méthode qui nécessite $O(\sqrt{n})$ opérations (ou au mieux $O(\sqrt{n}/\mathrm{Log}\, n)$ opérations si l'on dispose d'une table de nombres premiers jusqu'à $\sqrt{n}$), ce qui est beaucoup quand n est très grand.

De remarquables améliorations ont été apportées aux tecniques de factorisation. C'est ainsi que l'on dispose maintenant d'une méthode relativement simple (programmable sur une calculatrice de poche pour des n jusqu'à 10^{18}) en $O(n^{1/4})$ opérations [7], et des méthodes plus sophistiquées, plus rapides [3], [9]. Grâce à ces méthodes, il devient possible de factoriser un nombre de l'ordre de 10^{40}, mais guère plus en général.

Toutefois, si l'on ne s'intéresse qu'à la primalité d'un nombre (et non à ses facteurs éventuels s'il n'est pas premier) il existe des tests beaucoup plus efficaces. Tous ces tests sont basés sur le théorème de Fermat (ou sur des théo-

rèmes analogues) qui affirme que si n est premier et si $(a,n) = 1$ alors, $a^{n-1} \equiv 1 \pmod{n}$. Or le calcul de $a^b \pmod{c}$ peut se faire très rapidement, en $O(\text{Log } b)$ opérations, en utilisant un algorithme très simple utilisant l'écriture en binaire de b .

Le théorème de Fermat fournit donc un test très rapide pour déterminer si un nombre est composé. Malheureusement, sa réciproque directe est fausse (voir ci-dessous) donc on ne peut pas l'utiliser tel quel comme test de primalité. Malgré tout, les nombres n non premiers tels que $a^{n-1} \equiv 1 \pmod{n}$ sont relativement rares ; il est donc raisonnable d'utiliser la méthodologie suivante pour tester la primalité d'un nombre $n > 10^{10}$:

M1 | 1°) Diviser n par les nombres premiers $\leq B$, où B est une borne raisonnable donnée (par exemple $B = 10^5$) . Si l'un des restes est nul, n est composé. Sinon :

2°) Calculer $a^{n-1} \pmod{n}$ pour $a = 2$ et $a = 13$ (par exemple). Si on ne trouve pas toujours 1 , n est composé. Sinon, il est raisonnable de penser que n est premier.

Ce test est en $O(\text{Log } n)$ opérations mais n'est pas un algorithme à proprement parler car on ne peut pas montrer grâce à lui que n est premier puisque la réciproque du théorème de Fermat est fausse. On sait d'ailleurs qu'il existe des nombres n (appelés nombres de Carmichael) tels que $(a,n) = 1 \Rightarrow a^{n-1} \equiv 1 \pmod{n}$, sans être premiers. Le plus petit tel nombre est $561 = 3.11.17$, mais il en est d'autres tel que $252601 = 41.61.101$ dont la factorisation est moins évidente.

L'étape suivante consiste donc à trouver une réciproque valable au théorème de Fermat. Une telle réciproque a été trouvée par Lehmer et améliorée par la suite. Elle est basée sur la proposition suivante de démonstration immédiate :

PROPOSITION 1.1. - Supposons que $n-1 = F \cdot R$ avec $(F,R) = 1$ où F est complètement factorisé et $R = 1$ ou bien a tous ses facteurs premiers $> B$. Alors :

1°) Si pour tout $p|F$ premier il existe a_p tel que $a_p^{n-1} \equiv 1 \pmod n$ et $(a_p^{(n-1)/p}-1, n) = 1$ alors tout diviseur (premier ou non) r de n vérifie $r \equiv 1 \pmod F$.

2°) Si de plus il existe a tel que $a^{n-1} \equiv 1 \pmod n$ et $(a^F-1, n) = 1$, alors pour tout diviseur r de n il existe un diviseur premier f de R tel que $r \equiv 1 \pmod{F.f}$. En particulier, si $R \neq 1$ on a $r > FB$.

Remarques.

a) Si n est premier, il suffit de prendre pour a_p (et pour a si $R \neq 1$) une racine primitive modulo n .

b) Si $BF \geq \sqrt{n}$, la proposition 1.1 implique que n ne possède pas de diviseur premier inférieur à $\sqrt{n}$, donc que n est premier.

Ceci nous conduit donc à utiliser la méthodologie suivante (à n'utiliser qu'après avoir obtenu un résultat positif à M1).

M2 | 1°) Divisons $n-1$ par les nombres premiers $\leq B$, et écrivons $n-1 = F.R$ où $(F, R) = 1$, F est complètement factorisé, et $R = 1$ ou bien tous ses facteurs premiers sont supérieurs à B . Si $BF < n$ on ne pourra probablement rien conclure, donc augmenter la borne B jusqu'à ce que $BF \geq \sqrt{n}$.

2°) Pour tout p premier divisant F , trouver a_p tel que $a_p^{n-1} \equiv 1 \pmod n$ et $(a_p^{(n-1)/p} - 1, n) = 1$. Si pour un certain p on n'arrive pas à trouver un tel a_p après un nombre d'essais raisonnablement grand, il est probable que n n'est pas premier. Sinon :

3°) Trouver a tel que $a^{n-1} \equiv 1 \pmod n$ et $(a^F-1, n) = 1$ (même remarque que ci-dessus en cas d'échec). Si on a pu trouver les a_p et a , et si $BF \geq \sqrt{n}$ alors n est premier.

Ce test fait intervenir des calculs de PGCD qui sont aussi en $O(\text{Log } n)$ par l'algorithme d'Euclide. Il n'échoue que quand on ne peut pas trouver a ou a_p , ce qui est extrêmement rare si n est effectivement premier car dans ce

cas on peut presque toujours prendre a ou a_p assez petits.

On possède donc ici un véritable test de primalité (alors que le théorème de Fermat est un test de non primalité). Son défaut majeur est qu'il nécessite une factorisation (au moins partielle) de $n-1$; ceci est faisable pour certains nombres n , mais bien sûr en toute généralité ce test possède le handicap fondamental de tous les tests utilisant la factorisation.

Il existe des tests tout à fait analogues à celui-ci mais utilisant la factorisation de $n+1$, n^2+1 , n^2-n+1 , n^2+n+1 à la place de celle de $n-1$ (ces nombres sont des diviseurs de n^t-1 pour $t = 1,2,3,4,6$). Chacun de ces tests fournit des renseignements sur les diviseurs possibles r de n , et on peut donc utiliser ces tests en conjonction pour montrer la primalité de n . Je renvoie aux excellents articles [2] , [8] pour plus de détails sur ces sujets.

L'idée suivante consiste à chercher des critères plus sévères que le théorème de Fermat (c'est-à-dire possédant moins d'exceptions). Donnons d'abord une définition :

DEFINITION 1.2. - Soit $n > 1$ un entier, et écrivons $n-1 = 2^{t_0} n_1$ avec $2 \nmid n_1$. On dit que n est un nombre pseudo-premier fort (p.p.f.) à base a si :

- ou bien $a^{n_1} \equiv 1 \pmod{n}$
- ou bien il existe t avec $0 \leq t < t_0$ tel que $a^{2^t n_1} \equiv -1 \pmod{n}$.

Il est clair qu'un nombre premier n est p.p.f. à base a pour tout a tel que $(a,n) = 1$. D'autre part, il existe des nombres p.p.f. qui ne sont pas premiers. Par exemple $2047 = 23.89$ est p.p.f. à base 2 . Toutefois ces nombres sont beaucoup plus rares que les nombres non premiers n vérifiant simplement $a^{n-1} \equiv 1 \pmod{n}$. De plus on peut montrer que les "nombres de Carmichael forts", c'est-à-dire p.p.f. à base a dès que $(a,n) = 1$ et non premiers, n'existent pas. On peut ainsi obtenir des tests de primalité efficaces pour des petites machines. Par exemple, on a montré que le seul $n < 2,5 \cdot 10^{10}$ qui est non premier tout en étant un p.p.f. à base $2,3,5$ et 7 est $n = 3215031751$ [8] . Ceci fournit donc

un test de primalité très rapide pour $n < 2,5.10^{10}$.

L'utilité de la notion de p.p.f. réside surtout dans le théorème suivant démontré par Rabin [6] :

THEOREME 1.3. - Soit n un nombre non premier. Le nombre de a tels que $2 \leq a \leq n-1$ et tels que n soit p.p.f. à base a est au plus $\frac{n-1}{4}$.

On en déduit ainsi un nouveau type de test appelé test probabiliste et utilisant la méthodologie suivante :

M3 (Miller, Rabin [6]) 1°) Choisir un entier k (par exemple $k = 50$). A l'aide d'un générateur de nombres aléatoires, choisir au hasard k entiers $a_1,\ldots,a_k \in [2,n-1]$.

2°) Si pour un $i \in [1,k]$, n n'est pas un p.p.f. à base a_i , n est composé. Sinon nous dirons que n est premier avec une probabilité d'erreur inférieure à 4^{-k} .

Ce type de résultat est satisfaisant dans beaucoup de cas, et notamment, pour les applications à la cryptographie. Il faut aussi penser au fait que la probabilité d'erreur peut être rendue aussi petite que l'on veut en augmentant k , et même avec $k = 50$ est déjà très nettement inférieure à la probabilité d'une erreur due à l'ordinateur lui-même.

En utilisant une idée un peu analogue, on est conduit à un autre type de test :

DEFINITION 1.4. - Soit p_k le k^e nombre premier. On dit que x est un pseudo-carré d'ordre k si pour tout $i \leq k$ on a $(\frac{p_i}{x}) = 1$. On note $F(p_k)$ le plus petit pseudo-carré d'ordre k qui ne soit pas un carré. Par exemple on a $F(2) = 7$, $F(3) = 23$, ... , $F(109) = 2570169839$. On a alors le test suivant ([8]) :

M4 (Miller, Selfridge, Weinberger) 1°) Vérifier que n n'est pas une puissance ≥ 2 d'un nombre premier (cette vérification est très rapide).

2°) Diviser n par les nombres premiers inférieurs ou égaux à B .

3°) Trouver p_k tel que $N/B < F(p_k)$.

4°) Pour tout $i = 1,\ldots,k$ vérifier que $p_i^{(n-1)/2} \equiv \pm 1 \pmod n$ et que pour au moins un i_0 on a $p_{i_0}^{(n-1)/2} \equiv -1 \pmod n$. Si l'une des vérifications ne marche pas, n est composé. Sinon n est premier.

Ce test semble être idéal puisqu'enfin le résultat est sans ambiguité possible. Malheureusement la difficulté majeure réside dans l'évaluation de $F(p_k)$ au 3°) . On ne peut le faire de façon efficace qu'en admettant l'hypothèse de Riemann généralisée (GRH) . Dans ce cas Weinberger a montré qu'il existe des constantes c_1, c_2, c_3 (explicites et de taille raisonnable) telles que si $p_k > (c_1 \operatorname{Log} N + c_2 \operatorname{Log}\operatorname{Log} N + c_3)^2$ alors $N < F(p_k)$. Le test M_4 est donc un test conditionnel : si l'on accepte l'hypothèse de Riemann généralisée, le test est en $O((\operatorname{Log} n)^4)$ opérations et dès que cette hypothèse sera démontrée, tous les nombres déclarés premiers par ce test seront vraiment premiers.

Remarque. - La démonstration de la validité du test M4 , bien que simple, est relativement subtile ; c'est un excellent exercice de théorie élémentaire des nombres.

2. - LE TEST d'ADLEMAN [1], [4]

Avant de décrire en détail le nouveau test dû à Adleman (1980) précisons à l'avance ses caractéristiques. Tout d'abord, quand cet algorithme déclare qu'un nombre est composé ou premier, il l'est effectivement, sans pour cela devoir faire appel à des hypothèses non démontrées telles que GRH .

D'autre part, la version la plus simple et la plus rapide de ce test est une version probabiliste mais dans un sens tout à fait différent du test M3 : si n est premier, il est pratiquement certain que l'algorithme le démontrera rigoureusement. Le seul aspect probabiliste là dedans est qu'il peut arriver pour de très rares n premiers que l'algorithme échoue à déterminer si n est premier ou composé. Comme, dans le cas où n est composé, il est pratiquement certain que le test probabiliste de Miller-Rabin M3 le démontrera rigoureusement, le test d'Adleman est à utiliser <u>après</u> s'être assuré grâce au test M3 que n n'a que très peu de chances d'être composé.

Il existe en fait une version déterministe du test qui n'a pas d'intérêt pratique à cause de ce qui vient d'être dit, mais qui a un intérêt théorique certain.

Enfin le temps d'exécution du test est $O((\text{Log } n)^{c \text{ Log Log Log } n})$ où c est une constante effective. Ce n'est donc pas un test polynomial en Log n comme M4 , mais c'est à peine plus lent, et surtout ne dépend pas de GRH .

La présentation du test d'Adleman a été notablement simplifiée par Lenstra [4] , qui y a également apporté des améliorations. C'est sa présentation que je suis ici, en y incorporant ses améliorations dès le départ.

Introduisons quelques notations. n est un nombre fixé à tester. p et q sont deux nombres premiers tels que $p^k \mid (q-1)$ et $(pq, n) = 1$. ζ_{p^k} (resp. ζ_q) est une racine primitive p^k-ième (resp. q-ième) de l'unité ; $\langle \zeta_{p^k} \rangle$ est le groupe cyclique de toutes les racines p^k-ièmes de l'unité.

$G = \text{Gal}(\mathbb{Q}(\zeta_{p^k})/\mathbb{Q}) = \{\sigma_x / 1 \le x \le p^k - 1 \ , \ p \nmid x\}$ où σ_x est l'automorphisme de $\mathbb{Q}(\zeta_{p^k})$ qui à ζ_{p^k} associe $\zeta_{p^k}^x$. $\mathfrak{p} = \{\gamma \in \mathbb{Z}[G] / \zeta_p^\gamma = 1\}$ (il s'agit bien de ζ_p et non de ζ_{p^k} ici). C'est un idéal premier engendré par tous les $\sigma_x - x$ pour $x \in \mathbb{Z} - p\mathbb{Z}$ et par p .

Enfin soit χ un caractère d'ordre p^k exactement, et de conducteur q . Notons pour la suite les relations suivantes :

si $p \ge 3$, $\chi(-1) = 1$

si $p = 2$, $\chi(-1) = (-1)^{(q-1)/2^k}$.

La somme de Gauss

$$\tau(\chi) = \sum_{x \in \mathbb{F}_q^*} \chi(x)\, \zeta_q^x \in \mathbb{Z}[\zeta_{p^k}, \zeta_q]$$

vérifie $\tau(\chi)\,\tau(\bar{\chi}) = \chi(-1)q$ donc puisque $(q, n) = 1$, $\tau(\chi)$ est inversible modulo n.

Soit β un élément quelconque de $\mathbb{Z}[G]$ tel que

$$\boxed{\beta \notin p} \ .$$

Nous utiliserons intensivement la condition suivante, analogue à un test utilisant le théorème de Fermat :

(*β) $\quad$ Il existe $\eta(\chi) \in \langle \zeta_{p^k} \rangle$ tel que
$\tau(\chi)^{\beta(n-\sigma_n)} \equiv \eta(\chi)^{-\beta n} \pmod{n}$

On remarque tout d'abord que :

LEMME 2.1. - Si n est premier, (*β) est vérifiée avec $\eta(\chi) = \chi(n)$.

En effet dans ce cas,

$$\tau^n(\chi) \equiv \sum_x \chi^n(x)\, \zeta_q^{nx} \equiv \sum_x \chi^n(n^{-1}x)\, \zeta_q^x \equiv \chi(n)^{-n}\, \tau(\chi^n) \pmod{n}$$

d'où le lemme puisque $\tau(\chi^n) = \tau(\chi)^{\sigma_n}$.

Dans le cas particulier $p = 2$, $k = 1$ et $\beta = 1$ on sait que $\tau(\chi)^2 = \chi(-1)q = (-1)^{(q-1)/2} q = q^*$ donc le test équivaut à

$(q^*)^{(n-1)/2} \equiv \eta(\chi) \pmod{n}$ où $\eta(\chi) = \pm 1$.

L'idée de base du test d'Adleman est que si la condition (*β) est vérifiée pour "assez" de caractères χ (avec des p et q différents) alors on a suffisamment de renseignements pour décider si n est premier. Nous allons progressivement nous acheminer vers ce but, en étudiant les déductions que l'on peut faire à partir de (*β).

LEMME 2.2. - Si (*β) est vérifiée, alors pour tout i :

$$\tau(\chi)^{\beta(n^i-\sigma_{n^i})} \equiv \eta(\chi)^{-\beta i n^i} \pmod{n}$$

Démonstration. - L'assertion pour $i = 1$ n'est autre que (*β) . Supposons-la vraie pour i . On a : $n^{i+1} - \sigma_{n^{i+1}} = n^i(n - \sigma_{n^i}) + \sigma_n(n^i - \sigma_{n^i})$ donc d'après (*β) et l'hypothèse de récurrence :

$$\tau(\chi)^{\beta(n^{i+1}-\sigma_{n^{i+1}})} = \left(\tau(\chi)^{\beta(n-\sigma_n)}\right)^{n^i} \cdot \left(\tau(\chi)^{\beta(n^i-\sigma_{n^i})}\right)^{\sigma_n}$$

$$\equiv \eta(\chi)^{-\beta n^{i+1}} \cdot \eta(\chi)^{-\beta i n^i \sigma_n} \pmod{n} .$$

Or $\eta(\chi) \in \langle \zeta_{p^k} \rangle$ donc $\eta(\chi)^{\sigma_n} = \eta(\chi)^n$, d'où le lemme 2.2 par récurrence.

LEMME 2.3. - 1) Si (*β) est vérifiée, alors

$$\tau(\chi)^{\beta(n^{(p-1)p^{k-1}}-1)} \equiv \eta(\chi)^{\beta p^{k-1}} \pmod{n} .$$

2) Si r est premier et $(r, pq) = 1$ (en particulier si $r \mid n$) :

$$\tau(\chi)^{(r^{(p-1)p^{k-1}}-1)} \equiv \chi(r)^{p^{k-1}} \pmod{r} .$$

Démonstration. - 1) On applique le lemme 2.2 à $i = (p-1)p^{k-1}$. Comme $n^{(p-1)p^{k-1}} \equiv 1 \pmod{p^k}$ on a $\sigma_{n^{(p-1)p^{k-1}}} = \sigma_1$ et $\eta(\chi)^{n^{(p-1)p^{k-1}}} = \eta(\chi)$, d'où 1).

Pour 2), on remarque que d'après le lemme 2.1 r satisfait à la condition $(*_1)$ avec $\eta(\chi) = \chi(r)$, donc 2) résulte immédiatement de 1) .

Nous introduisons maintenant la condition (£) suivante sur le nombre premier p :

(£) Pour tout $r \mid n$, r premier, on a $r^{p-1} \in (n^{p-1})^{\mathbb{Z}_p}$ dans $1 + p\mathbb{Z}_p$, ou en d'autres termes il existe $\ell_p(r) \in \mathbb{Z}_p$ tel que $r^{p-1} = (n^{p-1})^{\ell_p(r)}$.

Cette condition est évidemment vérifiée si n est premier.

LEMME 2.4. - 1°) Si $p \geq 3$, la condition $r^{p-1} \in (n^{p-1})^{\mathbb{Z}_p}$ équivaut à $v_p(r^{p-1}-1) \geq v_p(n^{p-1}-1)$.

2°) Si $p = 2$, la condition $r \in n^{\mathbb{Z}_2}$ équivaut à

$\sup(v_2(r-1), v_2(r-n)) \geq v_2(n^2-1)$.

Démonstration. - Il est facile de voir que $r^{p-1} \in (n^{p-1})^{\mathbb{Z}_p}$ implique $v_p(r^{p-1}-1) \geq v_p(n^{p-1}-1)$ et de même que $r \in n^{\mathbb{Z}_2}$ implique $r \in n^{2\mathbb{Z}_2}$ ou $r \in n^{1+2\mathbb{Z}_2}$ donc $v_2(r-1)$ ou $v_2(n-r) \geq v_2(n^2-1)$.

La réciproque se montre aisément par récurrence en prenant comme hypothèse de récurrence :

Si $p \geq 3$, pour $\ell \geq 0$: il existe $a_0, \ldots, a_{\ell-1} \in [0, p-1]$ tels que

$$r^{p-1} \in (n^{p-1})^{a_0 + pa_1 + \ldots + p^{\ell-1}a_{\ell-1}} (1 + p^{\ell+u}\mathbb{Z}_p) \quad \text{où} \quad u = v_p(n^{p-1} - 1) .$$

Si $p = 2$, pour $\ell \geq 1$: il existe $a_0, \ldots, a_{\ell-1} \in \{0, 1\}$ tels que

$$r \in n^{a_0 + 2a_1 + \ldots + 2^{\ell-1}a_{\ell-1}} (1 + 2^{\ell+u-1}\mathbb{Z}_2) \quad \text{où} \quad u = v_2(n^2-1) .$$

COROLLAIRE 2.5. - Si $p \geq 3$ et $n^{p-1} \not\equiv 1 \pmod{p^2}$ la condition $(\mathfrak{L})$ est vérifiée pour p .

Evident, puisque $v_p(n^{p-1}-1) = 1$ dans ce cas.

Ce corollaire est utile mais bien sûr est loin d'être suffisant pour vérifier la condition $(\mathfrak{L})$ pour p . Nous allons voir qu'avec certaines hypothèses supplémentaires, $(\mathfrak{L})$ est conséquence de $(*\beta)$.

LEMME 2.6. - Soient a, b deux entiers positifs. Supposons que pour un $x \in \mathbb{Z}[\zeta_{p^k}, \zeta_q]$ on ait

$x^a \equiv \eta_a \pmod{r}$ et $x^b \equiv \eta_b \pmod{r}$

où r est premier à p et où η_a (resp. η_b) est une racine primitive

p^{ℓ_a}-ième (resp. p^{ℓ_b}-ième) de l'unité, avec ℓ_a et $\ell_b \leq k$. Supposons $\ell_a \geq \ell_b$ et $\ell_a \geq 1$. On a alors :

$v_p(b) - v_p(a) = \ell_a - \ell_b$ si $\ell_b > 0$

$v_p(b) - v_p(a) \geq \ell_a$ si $\ell_b = 0$.

Démonstration. - Ecrivons $a = p^{v_p(a)} a'$, $b = p^{v_p(b)} b'$ avec $p \nmid a'b'$. On a tout d'abord $v_p(b) - v_p(a) \geq 0$. En effet, sinon en calculant $x^{p^{v_p(a)} a'b'} \pmod r$ de deux façons différentes, on aurait $\eta_a^{b'} = \eta_b^{a'p^{v_p(a)-v_p(b)}}$ donc $\ell_a < \ell_b$ contrairement à l'hypothèse. On calcule donc $x^{p^{v_p(b)} a'b'} \pmod r$ de deux façons différentes et on en déduit $\eta_b^{a'} = \eta_a^{b'p^{v_p(b)-v_p(a)}}$ (on a égalité et pas seulement une congruence mod r car la différence des deux membres divise p et p est premier à r). Le lemme résulte aussitôt de cette égalité.

PROPOSITION 2.7. - Supposons qu'il existe un caractère χ d'ordre p^k et un $\beta \notin \mathfrak{p}$ pour lesquels (*β) est vérifiée avec $\eta(\chi)$ une racine primitive p^k-ième de l'unité. Alors si l'une au moins des conditions supplémentaires suivantes est vraie, p satisfait la condition (£) :

a) si $p \geq 3$;

b) si $p = 2$, $k = 1$ et $n \equiv 1 \pmod 4$;

c) si $p = 2$, $k \geq 2$ et de plus si $\tau(\chi^{2^{k-1}})^{n-1} \equiv -1 \pmod n$ (ou encore $q^{(n-1)/2} \equiv -1 \pmod n$).

Démonstration. - a) $p \geq 3$. D'après le lemme 2.3, si r est un diviseur premier de n on a

$$x^{n^{(p-1)p^{k-1}}-1} \equiv \eta(\chi)^{\beta p^{k-1}} \pmod r$$

et

$$x^{r^{(p-1)p^{k-1}}-1} \equiv \chi(r)^{\beta p^{k-1}} \pmod r, \text{ où } x = \tau(\chi)^\beta .$$

Puisque $\beta \notin \mathfrak{p}$, $\eta(\chi)^{\beta p^{k-1}}$ est une racine primitive p-ième de 1. On déduit donc

du lemme 2.6 que

$$v_p(r^{(p-1)p^{k-1}}-1) - v_p(n^{(p-1)p^{k-1}}-1) \geq 0 .$$

Or puisque $p \geq 3$, $v_p(r^{(p-1)p^{k-1}}-1) = k-1+v_p(r^{p-1}-1)$, et de même pour n . On a donc $v_p(r^{p-1}-1) \geq v_p(n^{p-1}-1)$ et on conclut grâce au lemme 2.4.

b) $p = 2$, $k = 1$ et $n \equiv 1 \pmod 4$. On a ici d'après le lemme 2.3 (avec $x = \tau(\chi)^\beta$)

$$x^{n-1} \equiv -1 \pmod r$$
$$x^{r-1} \equiv \chi(r) \pmod r$$

d'où

$$x^{n-r} \equiv -\chi(r) \pmod r .$$

Il en résulte que soit x^{r-1} , soit x^{n-r} est congru à 1 (mod r) donc d'après le lemme 2.6 soit $v_p(r-1)$ soit $v_p(r-n)$ est supérieur ou égal à $1+v_p(n-1) = v_p(n^2-1)$ puisque $n \equiv 1 \pmod 4$. On conclut grâce au lemme 2.4.

c) $p = 2$, $k \geq 2$ et $\tau(\chi^{2^{k-1}})^{n-1} \equiv -1 \pmod n$. Si $n \equiv 1 \pmod 4$ on peut appliquer b) au caractère $\chi^{2^{k-1}}$ qui est d'ordre 2 et vérifie la condition (*1) . On peut donc supposer que $n \equiv 3 \pmod 4$. Notons que d'après le lemme 2.3 on a $x^{n2^{k-1}-1} \equiv -1 \pmod n$, $x^{r2^{k-1}-1} \equiv \chi^{2^{k-1}}(r) \pmod r$ où $x = \tau(\chi)^\beta$, $y^{n-1} \equiv -1 \pmod n$, $y^{r-1} \equiv \chi^{2^{k-1}}(r) \pmod r$ où $y = \tau(\chi^{2^{k-1}})$. Comme $v_2(n^{2^{k-1}}-1) = v_2(n^2-1) + k - 2$ on déduit du lemme 2.6 que :

• Si $\chi^{2^{k-1}}(r) = -1$, $v_2(n^2-1) = v_2(r^2-1)$, $v_2(n-1) = v_2(r-1)$ donc par soustraction $v_2(n+1) = v_2(r+1)$ donc $v_2(n-r) = v_2((n+1) - (r+1)) \geq 1+v_2(n+1) = v_2(n^2-1)$ puisque $v_2(n-1) = 1$, et on conclut par le lemme 2.4.

• Si $\chi^{2^{k-1}}(r) = 1$, $v_2(r^2-1) \geq 1 + v_2(n^2-1)$, $v_2(r-1) \geq 1+v_2(n-1) = 2$ donc $r \equiv 1 \bmod 4$ donc $v_2(r+1) = 1$ donc $v_2(r-1) \geq v_2(n^2-1)$ et on conclut à nouveau par le lemme 2.4.

L'utilité de la condition £ provient de la proposition suivante :

PROPOSITION 2.8. - Supposons que p vérifie la condition (£) .

1°) Si χ vérifie (*β) pour un certain $\beta \notin p$. Alors pour tout $r \mid n$ (premier ou non) on a

$\chi(r) = \chi(n)^{\ell_p(r)}$ et $\eta(\chi) = \chi(n)$.

2°) Si ψ est un caractère d'ordre une puissance de p et de conducteur également une puissance de p alors on a aussi

$\psi(r) = \psi(n)^{\ell_p(r)}$.

Remarque. - L'expression $\chi(n)^{\ell_p(r)}$ a bien un sens puisque χ est d'ordre une puissance de p , et de même $\psi(n)^{\ell_p(r)}$.

Démonstration. - 1°) D'après le lemme 2.2 on a

$$x^{n^{(p-1)p^k}-1} \equiv 1 \pmod{n} \quad \text{avec} \quad x = \tau(\chi)^\beta .$$

Ecrivons $n^{(p-1)p^k}-1 = p^\gamma n_1$ avec $p \nmid n_1$. Par définition de $\ell_p(r)$ on peut trouver $\ell \in \mathbb{N}$ avec $\ell \equiv \ell_p(r) \pmod{p^k}$ tel que $v_p(n^{(p-1)\ell} - r^{p-1}) \geq \sup(\gamma, k+1)$. Or d'après le lemme 2.2 on a :

$$x^{n^{(p-1)\ell}} \equiv \eta(\chi)^{-\beta(p-1)\ell n^{(p-1)\ell}} \tau(\chi^{n^{(p-1)\ell}})^\beta \pmod{n}$$

$$\equiv \eta(\chi)^{-\beta(p-1)\ell r^{p-1}} \tau(\chi^{r^{p-1}})^\beta \pmod{n}$$

puisque $\eta(\chi)$ et χ sont d'ordre p^k . D'autre part, si r est premier :

$$x^{r^{p-1}} \equiv \chi(r)^{-\beta(p-1)r^{p-1}} \tau(\chi^{r^{p-1}})^\beta \pmod{r} .$$

Il en résulte que

$$x^{(n^{(p-1)\ell} - r^{p-1})} \equiv \zeta^{\beta(p-1)r^{p-1}} \pmod{r} \quad \text{avec} \quad \zeta = \chi(r)\eta(\chi)^{-\ell}$$

(noter que $\tau(\chi^{r^{p-1}})^\beta$ est inversible modulo r puisque $(r,q) = 1$). Si on avait $\zeta \neq 1$, comme $\beta(p-1)r^{p-1} \notin p$ on aurait $\zeta^{\beta(p-1)r^{p-1}} \neq 1$ donc d'après le lemme 2.6 :

$$v_p(n^{(p-1)\ell} - r^{p-1}) < v_p(n^{(p-1)p^k} - 1) = \gamma \quad \text{contrairement à l'hypothèse.}$$

On a donc $\zeta = 1$, ou encore :

$$\chi(r) = \eta(\chi)^{\ell} = \eta(\chi)^{\ell_p(r)} \quad \text{pour} \quad r \quad \text{premier,} \quad r \mid n \ .$$

Or $\ell_p(rr') = \ell_p(r) + \ell_p(r')$ donc par multiplicativité des deux membres on voit que $\chi(r) = \eta(\chi)^{\ell_p(r)}$ pour tout $r \mid n$, et en particulier pour $r = n$. Comme $\ell_p(n) = 1$, on a $\chi(n) = \eta(\chi)$ d'où 1°) .

2°) Si ψ est d'ordre p^{k_1} et de conducteur p^{k_2} , et si $\ell \in \mathbb{N}$ est tel que $\ell \equiv \ell_p(r) \pmod{p^{\sup(k_1, k_2)}}$ il est clair que $r^{p-1} \equiv (n^{p-1})^{\ell} \pmod{p^{k_2}}$ donc $\psi(r^{p-1}) = \psi((n^{p-1})^{\ell}) = \psi(n^{p-1})^{\ell}$ et comme $p-1$ est premier à l'ordre de ψ :

$$\psi(r) = \psi(n)^{\ell} = \psi(n)^{\ell_p(r)} \quad \text{puisque} \quad \ell \equiv \ell_p(r) \pmod{p^{k_1}}$$

d'où la proposition 2.8.

De tout ce qui précède, on peut déduire le théorème central du test d'Adleman :

THEOREME 2.9. - Soit t un entier pair tel que

$$e(t) = 2 \prod_{\substack{q \text{ premier} \\ (q-1) \mid t}} q^{v_q(t)+1}$$

soit tel que $(n, te(t)) = 1$.

Pour tout couple (p,q) de nombres premiers avec $(q-1) \mid t$ et $p^k \| (q-1)$ choisissons un caractère χ_{pq} d'ordre p^k et de conducteur q (par exemple $\chi(g_q^a) = \zeta_{p^k}^a$ si g_q est une racine primitive mod q). Supposons que :

1°) Pour tout (p,q) comme ci-dessus, χ_{pq} vérifie (*β) pour un certain $\beta \notin \mathfrak{p}$ (pouvant dépendre de p et q) .

2°) Pour tout $p \mid t$, on a soit $p \geq 3$ et $n^{p-1} \not\equiv 1 \pmod{p^2}$ soit il existe q tel que

a) $\eta(\chi_{pq})$ soit une racine primitive p^k-ième de 1 , où $k = v_p(q-1)$ et

b) soit $p \geq 3$

soit $p = 2$, $k = 1$ et $n \equiv 1 \pmod 4$

soit $p = 2$, $k \geq 2$ et $q^{(n-1)/2} \equiv -1 \pmod n$.

Alors pour tout diviseur r de n il existe $i \in [0, t-1]$ tel que $r \equiv n^i \pmod{e(t)}$.

Démonstration. - D'après le 2°), le corollaire 2.5 et la proposition 2.7, tous les $p \mid t$ satisfont à la condition (£) . Il résulte de la proposition 2.8 1°) que si on définit $\ell(r)$ modulo t par $\ell(r) \equiv \ell_p(r) \pmod{p^{v_p(t)}}$ pour tout $p \mid t$, alors pour tous p, q comme ci-dessus on a $\chi_{pq}(r) = \chi_{pq}(n^{\ell(r)})$. Or $\chi_q = \prod_{p \mid q} \chi_{pq}$ est un caractère d'ordre $q-1$: en effet soit ϵ le caractère trivial modulo q . Si on a $\chi_q^a = \epsilon$ on en déduit $\prod_{p \mid q} \chi_{pq}^a = \epsilon$ donc élevant à la puissance $(q-1)/p_0^k$ où $p_0^k \| (q-1)$:

$$\chi_{p_0 q}^{a((q-1)/p_0^k)} = \epsilon \quad \text{puisque si } p \neq p_0 \text{ , } \chi_{pq}^{(q-1)/p_0^k} = \epsilon .$$

Il en résulte que $p_0^k \mid a$. Ceci étant vrai pour tout p_0 on a $(q-1) \mid a$ d'où notre assertion. χ_q engendre donc tous les caractères modulo q , et donc pour tout tel caractère χ_1 on a $\chi_1(r) = \chi_1(n^{\ell(r)})$.

Soit maintenant χ un caractère modulo $q^{v_q(t)+1+\delta}$ où $\delta = 0$ si $q > 2$, $\delta = 1$ si $q = 2$. On sait que l'on peut écrire $\chi = \chi_1 \chi_2$, où χ_1 est un caractère modulo q (donc d'ordre divisant $q-1$) et χ_2 un caractère modulo $q^{v_q(t)+1+\delta}$ et d'ordre $q^{v_q(t)+1+\delta-(1+\delta)} = q^{v_q(t)}$.

Si $q \nmid t$, on a $\chi = \chi_1$ donc $\chi(r) = \chi(n^{\ell(r)})$;

Si $q \mid t$, q vérifie la condition (£) donc d'après la proposition 2.8 2°), on a

$$\chi_2(r) = \chi_2(n)^{\ell_q(r)} = \chi_2(n^{\ell(r)})$$

puisque χ_2 est d'ordre $q^{v_q(t)}$ et que $\ell_q(r) \equiv \ell(r) \pmod{q^{v_q(t)}}$. Il en résulte que pour tout χ modulo $q^{v_q(t)+1+\delta}$ on a

$$\chi(r) = \chi(n^{\ell(r)})$$

et on en déduit donc que $r \equiv n^{\ell(r)} \pmod{q^{v_q(t)+1+\delta}}$. Il en résulte que $r \equiv n^{\ell(r)} \pmod{\prod_{(q-1)|t} q^{v_q(t)+1+\delta} = e(t)}$. Enfin, remarquons que pour tout q premier tel que $(q-1)|t$ on a $n^{(q-1)q^{v_q(t)}} \equiv 1 \pmod{q^{v_q(t)+1+\delta}}$. Comme $(q-1)q^{v_q(t)} | t$ on a donc $n^t \equiv 1 \pmod{e(t)}$. Si $i \in [0,t-1]$ est tel que $i \equiv \ell(r) \pmod{t}$ on a donc $r \equiv n^i \pmod{e(t)}$, d'où le théorème.

Pour la suite, notons $R(n^i, e(t))$ l'unique entier congru à n^i mod $e(t)$ et appartenant à $[0, e(t)-1]$. On a alors :

COROLLAIRE 2.10. - Conservons les notations et hypothèses du théorème 2.9. Si de plus $e(t) > \sqrt{n}$ et si pour tout $i \in [0,t-1]$ on a soit $R(n^i, e(t)) = 1$ soit $R(n^i, e(t)) \nmid n$, alors n est premier.

Démonstration. - En effet, sinon il existerait un diviseur r de n tel que $1 < r \leq \sqrt{n} < e(t)$ donc d'après le théorème 2.9, il existerait $i < t$ tel que $r \equiv n^i \pmod{e(t)}$, donc $r = R(n^i, e(t))$ donc $R(n^i, e(t)) \neq 1$ et $R(n^i, e(t)) | n$ contrairement à l'hypothèse.

La méthodologie à utiliser est claire :

M5 (Adleman, Rumely, Pomerance, Lenstra [1], [4])

1°) (Cette partie ne dépend que de la taille de n et non de sa valeur donc peut être faite une fois pour toutes pour des n de taille comparable).

a) Choisir t tel que $e(t) > \sqrt{n}$. Pour $n < 4.10^{313}$, on peut pour cela utiliser la table 1 ; toutefois le choix du plus petit t possible n'est pas toujours le meilleur.

b) Pour tout $q | e(t)$ choisir g_q une racine primitive modulo q. Pour tout $p | (q-1)$, soit $k = v_p(q-1)$ et soit χ_{pq} le caractère de conducteur q et d'ordre p^k défini par $\chi_{pq}(g_q^x) = \zeta_{p^k}^x$.

2°) Vérifier que $(n, te(t)) = 1$.

3°) Pour tout couple p,q vérifier que χ_{pq} satisfait à (*β) pour un $\beta \not\equiv p$ (par exemple avec $\beta = 1$, mais d'autres choix sont utiles, voir plus loin). Si ce n'est pas le cas, n est composé.

4°) Vérifier que pour tout $p|t$ premier au moins l'une des conditions suivantes est satisfaite :

a) $p \geq 3$ et $n^{p-1} \not\equiv 1 \pmod{p^2}$;

b) $p \geq 3$ et $\eta(\chi_{pq})$ est une racine primitive p^k-ième de l'unité pour un $q|e(t)$ au moins, où $k = v_p(q-1)$;

c) $p = 2$, $n \equiv 1 \pmod 4$ et $\eta(\chi_{2q}) = -1$ pour un $q|e(t)$ au moins tel que $v_2(q-1) = 1$ (soit $q \equiv 3 \pmod 4$) ;

d) $p = 2$ et il existe un $q|e(t)$, $q \equiv 1 \pmod 4$ tel que $\eta(\chi_{2q})$ soit une racine primitive 2^k-ième de 1 (où $k = v_2(q-1)$) et de plus $q^{(n-1)/2} \equiv -1 \pmod n$.

Si ces vérifications marchent pour tout $p|t$, aller à 6°). Sinon :

5°) Pour tout $p|t$ où la vérification du 4°) n'a pas marché : choisir un certain nombre de $q \nmid e(t)$ tels que $q \equiv 1 \pmod p$, $(q,n) = 1$, trouver g_q une racine primitive mod q ; soit χ_{pq} le caractère défini par $\chi_{pq}(g_q^x) = \zeta_{p^k}^x$ avec $k = v_p(q-1)$. Vérifier que χ_{pq} satisfait à (*β) (sinon n est composé) et que l'une des conditions du 4°) est satisfaite pour au moins un q. Si ce n'est pas le cas après un nombre raisonnable de q essayés, le test échoue (ceci est très rare si n est effectivement premier). Sinon :

6°) Pour $0 < i < t$ calculer $R(n^i, e(t))$, reste de la division euclidienne de n^i par $e(t)$. S'il existe un tel i tel que $R(n^i, e(t)) \neq 1, n$ et divise n, n est évidemment composé. Sinon n est premier.

Remarque. - L'étape 5°) a été mise pour que la probabilité que le test échoue quand n est premier soit aussi faible que l'on veut. En effet, il n'est pas difficile de montrer que si n est premier pour tout p il existera

$q \equiv 1 \pmod p$ tel que les conditions du 4°) soient satisfaites.

Il est clair que le temps d'exécution du test M5 dépend essentiellement de la taille de t. Le temps en $O((\text{Log } n)^{c \text{ Log Log Log } n})$ annoncé au début de ce paragraphe résulte du théorème suivant dû à Odlyzko et Pomerance :

THEOREME 2.11 (Odlyzko-Pomerance [1]) Il existe t sans facteur carré vérifiant $t < (\text{Log } n)^{c \text{ Log Log Log } n}$ (où c est une constante effective) et tel que $e(t) > \sqrt{n}$.

Toutefois la borne donnée par ce théorème n'a qu'un intérêt théorique. Dans la pratique, il est rare que l'on ait a tester la primalité de nombres généraux $n > 4.10^{313}$, et pour $n < 4.10^{313}$ la table 1 suffit. Le plus grand t nécessaire est alors 166320 ce qui n'est pas tellement grand.

3. - CONSIDERATIONS PRATIQUES - SOMMES DE JACOBI

Etant maintenant en possession de cinq méthodologies différentes, en nature et en efficacité, posons nous la question de savoir quel doit être la marche à suivre si l'on veut déterminer la primalité d'un nombre n avec certitude. Pour fixer les idées, nous prendrons pour n un nombre de l'ordre de 10^{100}, sans propriété particulière.

Tout d'abord on exécute M1 : à la fin, soit n aura été éliminé (c'est-à-dire que n est composé), soit on peut commencer à penser que n est premier. Ensuite on exécute M3 ; à la sortie, soit n aura été éliminé, soit la probabilité que n ne soit pas premier est ridiculement faible. Il reste à prouver que n est effectivement premier. Pour cela : si GRH a été démontrée au moment où l'on exécute le test, utiliser M4 qui donnera une réponse sans ambiguité assez rapidement. Sinon, exécuter le test d'Adleman M5. D'après la table 1, si $n < 10^{104}$, $t = 5040$ suffit.

Regardons maintenant en pratique ce qui prend du temps dans le test M5. Il semble apparemment que c'est la 6° étape qui prenne le plus de temps car pour $n < 10^{104}$ il y a 5039 restes à calculer. Toutefois la 3° étape est plus longue qu'il n'y parait. Pour $n < 10^{104}$ il y a 67 couples (p,q) et pour chacun d'eux on doit tester la condition $(*\beta)$, ce qui oblige à travailler dans l'anneau $\mathbb{Z}[\zeta_{p^k}, \zeta_q]$. Or certains q sont assez grands (le plus grand est 2521) donc le travail dans $\mathbb{Z}[\zeta_{p^k}, \zeta_q]$ devient très long pour de tels q. Il s'avère donc que la vérification de $(*\beta)$ n'est pas si facile que cela en pratique. Heureusement, en utilisant les sommes de Jacobi à la place des sommes de Gauss, on peut se ramener à travailler dans $\mathbb{Z}[\zeta_{p^k}]$ ce qui est tout à fait raisonnable puisque pour $n < 10^{104}$ on a $p^k \leq 16$ et même pour $n < 4.10^{313}$ on a $p^k \leq 27$. C'est ce que nous allons maintenant expliquer.

Rappelons que si χ et χ' sont deux caractères modulo q, on pose

$$j(\chi,\chi') = \sum_{x \in \mathbb{F}_q^* - \{1\}} \chi(x)\chi'(1-x) .$$

Si $\chi\chi'$ n'est pas le caractère trivial on a $j(\chi,\chi') = \frac{\tau(\chi)\tau(\chi')}{\tau(\chi\chi')}$. D'autre part, si χ et χ' sont des caractères d'ordre p^k on a $j(\chi,\chi') \in \mathbb{Z}[\zeta_{p^k}]$. Il résulte de ce qui précède que si $a,b \in \mathbb{Z}$ sont tels que $p \nmid ab(a+b)$ on a

$$j(\chi^a,\chi^b) = \tau(\chi)^{\sigma_a + \sigma_b - \sigma_{a+b}} .$$

Pour $p = 2$, il est impossible que $2 \nmid ab(a+b)$ et nous traiterons donc ce cas séparément. Nous supposerons donc pour l'instant :

1er cas : $p \geq 3$

Posons $\Theta = \sum_{\substack{1 \leq x \leq p^k \\ p \nmid x}} x\sigma_x^{-1}$. On vérifie aisément que l'on a pour tout t tel que $p \nmid t$:

$$\Theta(\sigma_t - t) = -p^k \sum_{p \nmid x} [tx/p^k]\,\sigma_x^{-1} .$$

En particulier :

$$\Theta(n-\sigma_n) = p^k \sum_x [\,nx/p^k]\,\sigma_x^{-1}$$

$$\Theta(\sigma_a+\sigma_b-\sigma_{a+b}) = \Theta(\sigma_a - a + \sigma_b - b - (\sigma_{a+b}-(a+b))) = p^k K \ ,$$

où $K = -\sum_x \left([\frac{xa}{p^k}] + [\frac{xb}{p^k}] - [\frac{x(a+b)}{p^k}] \right) \sigma_x^{-1}$. Il est sous-entendu que les sommations sur x portent sur les $x \in [1, p^k]$ tels que $p \nmid x$.

Si on pose $\alpha = \sum_x [\,nx/p^k]\,\sigma_x^{-1}$ et $\beta = K$ on a donc

$$\beta(n-\sigma_n) = \frac{1}{p^k}\,\Theta(n-\sigma_n)(\sigma_a+\sigma_b-\sigma_{a+b}) = \alpha(\sigma_a+\sigma_b-\sigma_{a+b})$$

et en particulier on a la relation :

$$\tau(\chi)^{\beta(n-\sigma_n)} = j(\chi^a, \chi^b)\alpha \ .$$

Il en résulte que l'on peut avantageusement remplacer la condition (*β) qui nécessite de travailler dans $\mathbb{Z}[\zeta_{p^k}, \zeta_q]$ par une condition sur $j(\chi^a, \chi^b)$ qui nécessite de travailler seulement dans $\mathbb{Z}[\zeta_{p^k}]$, à condition de choisir a et b pour que $\beta \notin \mathfrak{p}$. Or on a :

LEMME 3.1. - <u>Une condition nécessaire et suffisante pour que</u> $K \notin \mathfrak{p}$ <u>est que</u> $a^p+b^p \not\equiv (a+b)^p \pmod{p^2}$.

<u>Démonstration.</u> - Posons $K_1 = -\sum_x \left([\frac{xa}{p^k}] + [\frac{xb}{p^k}] - [\frac{x(a+b)}{p^k}] \right) x^{-1}$ où x^{-1} est un inverse de x modulo p^k . Il est clair que $\zeta_p^K = \zeta_p^{K_1}$ donc une CNS pour que $K \notin \mathfrak{p}$ est que $p \nmid K_1$. Or on vérifie aisément en calculant de deux façons le produit des ax pour $x \in [1, p^k]$, $p \nmid x$ que

$$\sum_x x^{-1} [\frac{xa}{p^k}] \equiv a \cdot \frac{a^{(p-1)p^{k-1}}-1}{p^k} \pmod{p^k} \ .$$

Or $\frac{a^{(p-1)p^{k-1}}-1}{p^k} \equiv \frac{a^{p-1}-1}{p} \pmod{p}$. On a donc

$$K \notin \mathfrak{p} \Leftrightarrow \frac{a^p-a+b^p-b-((a+b)^p-(a+b))}{p} \not\equiv 0 \pmod{p} \ ,$$

ce qui n'est autre que la condition du lemme 3.1.

Remarque. - L'étude générale des α, β possibles tels que $\beta(n-\sigma_n) = \alpha(\sigma_a + \sigma_b - \sigma_{a+b})$ et $\beta \notin \mathfrak{p}$ nécessite de travailler dans le complété de $\mathbb{Z}[G]_{\mathfrak{p}}$. On peut montrer que ce complété est isomorphe à $\mathbb{Z}_p[C]$ où C est le groupe cyclique engendré par une racine primitive p^{k-1}-ième de l'unité, en envoyant σ_t sur $\omega(t^{p^{k-1}})\sigma_{t^{1-p^{k-1}}}$, où $\omega(t) \in \mathbb{Z}_p$ est le caractère de Teichmüller. Toutefois, le choix de α, β fait ici est tout à fait satisfaisant.

COROLLAIRE 3.2. - 1°) Soit $\beta \notin \mathfrak{p}$ comme ci-dessus. Si la condition (*1) est vérifiée alors

(**) $j(\chi^a, \chi^b)^\alpha \equiv \eta(\chi)^{-\beta n} \pmod{n}$.

Réciproquement, cette dernière congruence équivaut à (*β) .

2°) Si $p < 10^9$ et $p \neq 1093, 3511$ on peut prendre $\beta = \sum_{\substack{p^k/2 < x \leq p^k \\ p \nmid x}} \sigma_x^{-1}$,

et (**) équivaut à

$$j(\chi, \chi)^\alpha \equiv \eta(\chi)^{-\beta_1 n} \pmod{n} \quad \text{où} \quad \beta_1 = 2 \cdot \frac{2^{(p-1)p^{k-1}} - 1}{p^k}$$

(avec toujours $\alpha = \sum_x [nx/p^k]\, \sigma_x^{-1}$) .

Démonstration. - Vu ce qui a été dit plus haut, le 1°) est clair. Pour le 2°) on utilise le fait que les seuls $p < 10^9$ tels que $2^{p-1} \equiv 1 \pmod{p^2}$ sont $p = 1093$ et 3511 . On voit donc que si $p < 10^9$ est différent de ces deux nombres on peut prendre $a = b = 1$, d'où la valeur de β . La dernière assertion résulte de ce que $\sum_x [2x/p^k]\, x^{-1} \equiv 2 \cdot \frac{2^{(p-1)p^{k-1}} - 1}{p^k} \pmod{p^k}$ comme il a été dit plus haut.

Remarque. - Même pour n de l'ordre de 10^{300} il suffit d'utiliser des $p \leq 17$. La restriction du 2°) n'en est donc pas du tout une dans la pratique.

Nous avons donc achevé pour $p \geq 3$ la transformation de (*β) au lieu de tester (*1) ou (*β) , on teste la condition (**) (et dans la pratique avec $a = b = 1$).

2ème cas : $p = 2$ et $k \geq 3$

Nous considérons ici trois nombres impairs a, b, c et la somme de Jacobi pour trois caractères :

$$j_3(\chi^a, \chi^b, \chi^c) = \sum_{x+y+z = 1} \chi^a(x)\chi^b(y)\chi^c(z) \in \mathbb{Z}[\zeta_{2^k}] .$$

On sait que

$$j_3(\chi^a, \chi^b, \chi^c) = \frac{\tau(\chi^a)\tau(\chi^b)\tau(\chi^c)}{\tau(\chi^{a+b+c})} = \tau(\chi)^{\sigma_a+\sigma_b+\sigma_c-\sigma_{a+b+c}} .$$

D'autre part, puisque $(a+b)+(b+c)+(a+c) \equiv 2 \pmod 4$, au moins l'un des trois nombres $a+b$, $a+c$ ou $b+c$ n'est pas divisible par 4. Supposons sans perte de généralité que ce soit $a+b$. Le caractère χ^{a+b} est donc non trivial, et on calcule efficacement $j_3(\chi^a, \chi^b, \chi^c)$ grâce à :

$$j_3(\chi^a, \chi^b, \chi^c) = j(\chi^a, \chi^b)\, j(\chi^{a+b}, \chi^c) .$$

Nous allons poser

$$\Theta = \sum_{\substack{1 \leq x \leq 2^k \\ x \equiv 1 \text{ ou } 3 \pmod 8}} x\sigma_x^{-1} .$$

La raison de ce choix apparaîtra au fur et à mesure.

Une première remarque toutefois est que l'on ne peut pas sommer sur tous les x impairs car l'on voit facilement que dans ce cas le K obtenu plus loin appartiendrait à $\mathfrak{p}$, ce qui est interdit. Ceci résulte essentiellement du fait que $(\mathbb{Z}/2^k\mathbb{Z})^*$ n'est pas un groupe cyclique. Il est donc raisonnable de le remplacer par l'un de ses trois sous-groupes cycliques d'indice 2. Soit G_3 l'ensemble des $x \in \mathbb{Z}$ tels que $x \equiv 1$ ou $3 \pmod 8$. Si $t \in G_3$ on voit que

$$\Theta(\sigma_t - t) = -2^k \sum_{\substack{1 \leq x \leq 2^k \\ x \in G_3}} [xt/2^k]\, \sigma_x^{-1} .$$

Il en résulte que si a, b, c, $a+b+c \in G_3$ on a

$$\Theta(\sigma_a + \sigma_b + \sigma_c - \sigma_{a+b+c}) = 2^k K$$

avec $K = -\sum_{\substack{1\le x\le 2^k \\ x\in G_3}} \left([\frac{xa}{2^k}] + [\frac{xb}{2^k}] + [\frac{xc}{2^k}] - [\frac{x(a+b+c)}{2^k}]\right)\sigma_x^{-1}$. Ceci explique pourquoi on n'a pas choisi G_5 à la place de G_3 où $G_5 = \{x \in \mathbb{Z} \mid x \equiv 1 \text{ ou } 5 \pmod 8\}$ $= \{x \in \mathbb{Z} \mid x \equiv 1 \pmod 4\}$. En effet $a,b,c \in G_5 \Rightarrow a+b+c \equiv 3 \pmod 4$ donc $a+b+c \notin G_5$. On vérifie aisément que si $a \in G_3$ on a :

$$\sum_{\substack{1\le x\le 2^k \\ x\in G_3}} x^{-1}[\frac{xa}{2^k}] \equiv a.\frac{a^{2k-2}-1}{2^k} \pmod{2^k} \equiv \frac{a^2-1}{8} \pmod 2 .$$

La condition à satisfaire pour que $K \notin \mathfrak{p}$ est donc $\frac{a^2+b^2+c^2-3-(a+b+c)^2+1}{8} \not\equiv 0 \pmod 2$, soit encore $ab+ac+bc+1 \not\equiv 0 \pmod 8$. Or si $a,b,c,a+b+c \in G_3$ on vérifie que l'on doit avoir $a \equiv b \equiv c \pmod 8$ donc $ab+ac+bc+1 \equiv 4 \pmod 8$. On a donc toujours $K \notin \mathfrak{p}$.

Examinons maintenant l'expression $\Theta(n-\sigma_n)$: si $n \in G_3$ on peut écrire

$$\Theta(n-\sigma_n) = 2^k \sum_{\substack{1\le x\le 2^k \\ x\in G_3}} [\frac{xn}{2^k}]\,\sigma_x^{-1}$$

et l'on peut poursuivre comme pour le cas $p \ge 3$. Par contre, si $n \equiv 5$ ou $7 \pmod 8$ l'expression $\Theta(n-\sigma_n)$ n'a pas de forme particulière, et en tous cas n'a aucune raison d'être divisible par 2^k . Toutefois, on remarque que si $n \notin G_3$ alors $-n \in G_3$ (et ceci explique pourquoi on n'a pas choisi G_7 à la place de G_3 , où $G_7 = \{x \in \mathbb{Z} \mid x \equiv 1 \text{ ou } 7 \pmod 8\}$) . Donc :

$$\Theta(\sigma_{-n}+n) = -2^k \sum_{\substack{1\le x\le 2^k \\ x\in G_3}} [\frac{-xn}{2^k}]\,\sigma_x^{-1} = 2^k \sum_{\substack{1\le x\le 2^k \\ x\in G_3}} ([\frac{xn}{2^k}]+1)\,\sigma_x^{-1}$$

et on pourra poursuivre si l'on trouve une condition du type (*β) faisant intervenir l'expression $\sigma_{-n}+n$ à la place de $n-\sigma_n$. Le résultat est le suivant :

PROPOSITION 3.3. - 1°) Soient a,b,c tels que $a \equiv b \equiv c \equiv 1$ ou $3 \pmod 8$ et posons

$$\alpha_1 = \sum_{\substack{1\le x\le 2^k \\ x\equiv 1,3 \pmod 8}} ([\frac{xn}{2^k}]+\delta_n)\sigma_x^{-1}$$

$$\beta = - \sum_{\substack{1 \le x \le 2^k \\ x \equiv 1,3 \pmod 8}} \left([\frac{xa}{2^k}] + [\frac{xb}{2^k}] + [\frac{xc}{2^k}] - [\frac{x(a+b+c)}{2^k}] \right) \sigma_x^{-1}$$

où $\delta_n = 0$ si $n \equiv 1$ ou $3 \pmod 8$, $\delta_n = 1$ si $n \equiv 5$ ou $7 \pmod 8$.
Si la condition (*1) est vérifiée, alors

(***) $j_3(\chi^a, \chi^b, \chi^c)^{\alpha_1} \equiv \eta(\chi)^{-\beta n} (-q)^{\delta_n \beta} \pmod n$.

Réciproquement, cette dernière condition équivaut à (*β) .

2°) On peut toujours prendre $a = b = c = 1$. Dans ce cas (***) équivaut à l'une quelconque des deux conditions suivantes :

(i) $j_3(\chi, \chi, \chi)^{\alpha_1} = (j(\chi, \chi)\, j(\chi^2, \chi))^{\alpha_1} \equiv \eta(\chi)^{-\beta_1 \eta} (-q)^{\delta_n \beta_2} \pmod n$

(ii) $j_3(\chi, \chi, \chi)^{\alpha} j^{2\delta_n}(\chi^{2^{k-3}}, \chi^{3.2^{k-3}}) \equiv (-1)^{\delta_n} \eta(\chi)^{-\beta_1 n} \pmod n$

où $\beta_1 = 3 \cdot \frac{3^{2k-2}-1}{2^k}$, $\beta_2 = 2^{k-2} - 1$ et $\alpha = \sum_{\substack{1 \le x \le 2^k \\ x \equiv 1,3 \pmod 8}} [\frac{xn}{2^k}]\, \sigma_x^{-1}$

Démonstration. - Si $n \equiv 1$ ou $3 \pmod 8$, on a vu ci-dessus que $\beta(n - \sigma_n) = \alpha_1(\sigma_a + \sigma_b + \sigma_c - \sigma_{a+b+c})$ donc 1°) est clair dans ce cas. Si $n \equiv 5$ ou $7 \pmod 8$ on a

$$\beta(\sigma_{-n} + n) = \alpha_1(\sigma_a + \sigma_b + \sigma_c - \sigma_{a+b+c}) .$$

Or si (*1) est vérifiée on a

$$\tau(\chi)^{n+\sigma_{-n}} = \tau(\chi)^n \tau(\chi^{-n}) \equiv \eta(\chi)^{-n} \tau(\chi^n)\, \tau(\chi^{-n})$$

$$\equiv \eta(\chi)^{-n} \chi^n(-1) q \equiv \eta(\chi)^{-n}(-q) \pmod n$$

puisque $\chi(-1) = (-1)^{(q-1)/2^k} = -1$. Appliquant β on en déduit bien (***) et la réciproque est également claire.

La condition (i) du 2°) résulte du fait que

$$\sum_{\substack{1 \le x \le 2^k \\ x \equiv 1,3 \pmod 8}} [\frac{3x}{2^k}]\, x^{-1} \equiv 3 \cdot \frac{3^{2^{k-2}} - 1}{2^k} \pmod{2^k}$$

comme il a déjà été dit, ainsi que de l'identité facile à démontrer :

$$\sum_{\substack{1\le x\le 2^k \\ x\equiv 1,3 \pmod 8}} \left[\frac{3x}{2^k}\right] = 2^{k-2}-1 .$$

Pour obtenir la condition (ii) il nous faut calculer

$$j_3(\chi,\chi,\chi) \sum_{x\in G_3,\ 1\le x\le 2^k} \sigma_x^{-1} = \prod_{\substack{1\le x\le 2^k \\ x\in G_3}} \tau^2(\chi^x) .$$

Pour cela, on utilise l'identité de Hasse-Davenport :

$$\prod_{0\le x<m} \tau(\psi,\chi_1^x) = -\tau(\psi^m)\,\psi^{-m}(m) \prod_{0\le x<m} \tau(\chi_1^x)$$

où χ_1 est un caractère d'ordre exactement m .

Appliquant cette identité à $\psi = \chi^a$, $\chi_1 = \chi^{2^{k-\ell}}$ on montre aisément par récurrence que

$$\prod_{0\le\lambda<2^\ell} \tau^2(\chi^{a+\lambda 2^{k-\ell}}) = q^{2^\ell-1}\,\tau^2(\chi^{2^\ell a})\,\chi^{-\ell\cdot 2^{\ell+1}a}(2) .$$

En particulier avec $\ell = k-3$ et multipliant les identités pour $a = 1$ et $a = 3$ on obtient :

$$\begin{aligned}\prod_{\substack{1\le x\le 2^k \\ x\in G_3}} \tau^2(\chi^x) &= q^{2^{k-2}-2}\,\tau^2(\chi^{2^{k-3}})\,\tau^2(\chi^{3\cdot 2^{k-3}}) \\ &= (q^{2^{k-2}-2})\,\tau^2(\chi^{2^{k-1}})\,j^2(\chi^{2^{k-3}},\chi^{3\cdot 2^{k-3}}) \\ &= q^{2^{k-2}-1}\,j^2(\chi^{2^{k-3}},\chi^{3\cdot 2^{k-3}}) .\end{aligned}$$

La condition (ii) en résulte aisément.

3ème cas : $p = 2$, $k \le 2$

Si $k = 1$, on a vu que (*1) équivaut à la condition

$$(-q)^{(n-1)/2} \equiv \eta(\chi) \pmod n$$

puisque $(-1)^{(q-1)/2} = -1$.

Si $k = 2$, on a $\tau(\chi)\,\tau(\chi^3) = \chi(-1)q = -q$, $\tau(\chi^2)^2 = \chi^2(-1)q = q$ et $j(\chi,\chi) = \tau^2(\chi)/\tau(\chi^2)$. On en déduit aisément :

LEMME 3.4. - Si $n \equiv 1 \pmod 4$ la condition (*1) équivaut à

$$j(\chi,\chi)^{(n-1)/2}\, q^{(n-1)/4} \equiv \eta(\chi)^{-1} \pmod n .$$

Si $n \equiv 3 \pmod 4$ la condition (*1) équivaut à

$$j(\chi,\chi)^{(n+1)/2}\, q^{(n-3)/4} \equiv -\eta(\chi) \pmod n .$$

Nous avons donc achevé pour $p = 2$ la transformation de (*β) en conditions n'utilisant que des calculs dans $\mathbb{Z}[\zeta_{p^k}]$.

4. - L'ALGORITHME DETAILLE

Nous donnons ci-dessous l'algorithme détaillé déduit de M5 et utilisant le §3 pour vérifier les conditions (*β) . Cet algorithme suppose que l'on possède des algorithmes permettant le calcul en multiprécision ainsi que des algorithmes de calcul dans $\mathbb{Z}[\zeta_{p^k}]$ (addition, soustraction, multiplication, action d'un $\sigma_{x^{-1}}$). Pour des raisons pratiques nous supposerons que n est un entier impair positif et inférieur à 4.10^{313} .

1ère étape (Calculs ne dépendant que de la taille de n).

a) Choisir le plus petit t tel que $e^2(t) > n$ en utilisant la table 1 .

b) Pour tout $q \mid e(t)$, $q \geq 3$, q premier faire ce qui suit :

1°) Trouver g_q une racine primitive modulo q et dresser une table de la fonction $f(x)$ définie pour $1 \leq x \leq q-2$ par $1-g^x = g^{f(x)}$ et $1 \leq f(x) \leq q-2$.

2°) Pour tout nombre premier $p \mid (q-1)$ soit $k = v_p(q-1)$ et soit χ_{pq}

le caractère défini par $\chi_{pq}(g_q^x) = \zeta_{p^k}^x$.

3°) Si $p \geq 3$ ou si $p = 2$ et $k = 2$ calculer :

$$j(\chi_{pq}, \chi_{pq}) = \sum_{1 \leq x \leq q-2} \zeta_{p^k}^{x+f(x)} .$$

Si $p = 2$ et $k \geq 3$ calculer $j(\chi_{2q}, \chi_{2q})$ comme ci-dessus, $j(\chi_{2q}^2, \chi_{2q}) = \sum_{1 \leq x \leq q-2} \zeta_{2^k}^{2x+f(x)}$ puis $j_3(\chi_{2q}, \chi_{2q}, \chi_{2q}) = j(\chi_{2q}, \chi_{2q}) j(\chi_{2q}^2, \chi_{2q})$. Enfin calculer $j^2(\chi_{2q}^{2^{k-3}}, \chi_{2q}^{3.2^{k-3}}) = \left(\sum_{1 \leq x \leq q-2} \zeta_8^{3x+f(x)} \right)^2$.

2e étape

Vérifier que $(n, te(t)) = 1$ (sinon il est facile de décider si n est premier ou non puisque $te(t)$ est complètement factorisé).

3e étape

a) Pour tout $p \mid t$ premier, poser $\lambda_p = 1$ si $p \geq 3$ et $n^{p-1} \not\equiv 1 \pmod{p^2}$ $\lambda_p = 0$ sinon .

b) Pour tout couple p, q de nombres premiers tels que $p^k \parallel (q-1) \mid t$, faire l'une des actions suivantes :

b 1) Si $p \geq 3$

calculer $s_1 = j(\chi_{pq}, \chi_{pq})^{\sum_{1 \leq x \leq p^k, p \nmid x} x\sigma_x^{-1}}$ puis $s_2 = s_1^{[n/p^k]}$ puis $s(p,q) = s_2 \cdot j(\chi_{pq}, \chi_{pq})^{\sum_{1 \leq x \leq p^k, p \nmid x} [rx/p^k] \sigma_x^{-1}}$, tout réduit (mod n) , où $r = n \bmod p^k$. S'il n'existe pas de $\eta \in \langle \zeta_{p^k} \rangle$ tel que $s(p,q) \equiv \eta \pmod{n}$, écrire "n est composé" et s'arrêter. Si η existe et est une racine primitive p^k-ième, faire $\lambda_p = 1$.

b2) Si $p = 2$ et $k \geq 3$:

Calculer $s_1 = j_3(\chi_{2q}, \chi_{2q}, \chi_{2q})^{\sum_{1\leq x\leq 2^k,\, x\equiv 1,3 \pmod 8} x\sigma_x^{-1}}$ puis $s_2 = s_1^{[n/2^k]}$

puis $s(p,q) = s_2 \cdot j_3(\chi_{2q}, \chi_{2q}, \chi_{2q})^{\sum_{1\leq x\leq 2^k,\, x\equiv 1,3 \pmod 8} [rx/2^k]\sigma_x^{-1}} j^{2\delta_n}(\chi_{2q}^{2^{k-3}}, \chi_{2q}^{3.2^{k-3}})$ (mod n) où $\delta_n = 0$ si $n \equiv 1$ ou $3 \pmod 8$, $\delta_n = 1$ si $n \equiv 5$ ou $7 \pmod 8$. S'il n'existe pas de $\eta \in \langle \zeta \rangle$ tel que $s(2,q) \equiv \eta \pmod n$, écrire "n est composé" et s'arrêter. Si η existe et est une racine primitive 2^k-ième, et si de plus $q^{(n-1)/2} \equiv -1 \pmod n$, faire $\lambda_2 = 1$.

b3) Si $p = 2$ et $k = 2$:

Calculer $s_1 = j(\chi_{2q}, \chi_{2q})^2 q$ puis $s_2 = s_1^{[n/4]}$ puis $s'(2,q) = s_2$ si $n \equiv 1 \pmod 4$, $s'(2,q) = s_2 \cdot j(\chi_{2q}, \chi_{2q})^2$ si $n \equiv 3 \pmod 4$ (mod n). S'il n'existe pas de $\eta \in \langle \zeta_4 \rangle$ tel que $s'(2,q) \equiv \eta \pmod n$ écrire "n est composé" et s'arrêter. Si η existe et $\eta = \pm i$, et si $q^{(n-1)/2} \equiv -1 \pmod n$, faire $\lambda_2 = 1$.

b4) Si $p = 2$ et $k = 1$:

Calculer $s''(2,q) = (-q)^{(n-1)/2} \pmod n$. Si $s''(2,q)$ n'est pas congru à $\pm 1 \pmod n$ écrire "n est composé" et s'arrêter. Si $s''(2,q) \equiv -1 \pmod n$ et si $n \equiv 1 \pmod 4$, faire $\lambda_2 = 1$.

4e étape

Pour tout $p \mid t$ tel que $\lambda_p = 0$ faire ce qui suit : choisir un certain nombre de $q \nmid e(t)$ premiers tels que $q \equiv 1 \pmod p$, $(q,n) = 1$ et effectuer les calculs du b) de la 1ère étape uniquement pour le nombre premier p, puis l'action b1), b2), b3) ou b4) de la 3e étape correspondant au couple (p,q). Si au bout d'un nombre raisonnable de q essayés on a toujours $\lambda_p = 0$, écrire "le test a échoué". Sinon (c'est-à-dire maintenant que $\lambda_p = 1$ pour tout $p \mid t$).

5e étape

Pour $i \in [1, t-1]$ calculer $R(n^i, e(t))$, reste de la division euclidienne de n^i par $e(t)$. Si pour tout i , $R(n^i, e(t)) = 1$ ou n (*) ou bien ne divise pas n, écrire "n est premier" et s'arrêter. Sinon écrire "n est composé" et s'arrêter.

Remarques finales.

1°) Lenstra a trouvé un moyen fort ingénieux de remplacer la condition $e(t) > \sqrt{n}$ du corollaire 2.10 par $e(t) > n^{1/3}$, quitte à faire quelques vérifications supplémentaires rapides. Ceci augmente la rapidité d'exécution de l'algorithme dans la pratique mais bien sûr le temps d'exécution $O(\text{Log } n^{C \text{ Log Log Log } n})$ n'est amélioré que d'un facteur constant.

2°) Asymptotiquement (disons $n > 10^{(10^{10})}$) c'est la 5e étape qui prend le plus de temps. Par contre, pour des n de taille raisonnable (disons $n < 10^{313}$) c'est la 3e étape qui est la plus longue. Pour donner une idée, le temps d'exécution de l'algorithme sur un miniordinateur 16 bits pour des nombres n de l'ordre de 10^{100} devrait être inférieur à une heure.

(*) $R(n^i, e(t)) = n$ n'est possible que si $n < e(t)$, ce qui correspondrait à un mauvais choix de t .

BIBLIOGRAPHIE

[1] ADLEMAN, RUMELY, POMERANCE - On distinguishing prime numbers from composite numbers, à paraître.

[2] BRILLHART, LEHMER et SELFRIDGE - New primality criteria and factorizations of $2^m \pm 1$, Math. Comp., 29 (1975), pp. 620-647.

[3] KNUTH - The Art of Computer Programming, vol. II, Seminumerical algorithms, Addison-Wesley 1969, 2nd edition 1981.

[4] LENSTRA - Tests de primalité et théorie de Galois, journées de théorie des nombres, mars 1981, Reims et séminaire Bourbaki, juin 1981.

[5] MILLER - Riemann's hypothesis and tests for primality, Journal of computer and system sciences 13 (1976), pp. 300-317.

[6] RABIN - Probabilistic algorithms for testing primality, J. Number theory 12 (1980), pp. 128-138.

[7] SHANKS - SQUFOF, a fast factoring method, à paraître.

[8] WILLIAMS - Primality testing on a computer, Ars combinatoria, 5 (1978), pp. 127-185.

[9] WUNDERLICH - A running time analysis of Brillhart's continued fraction method, in Proceedings of the Number Theory Conference in Carbondale (1979), Springer Lecture Notes n°751.

Laboratoire de Mathématiques Pures - Institut Fourier
dépendant de l'Université Scientifique et Médicale de Grenoble
associé au C.N.R.S.
B.P. 116
38402 ST MARTIN D'HERES (France)

TABLE 1

Pour t entier, on pose $e(t) = 2 \prod_{\substack{q \text{ premier} \\ (q-1)\mid t}} q^{v_q(t)+1}$.

Dans la première colonne sont indiqués les t tels que $\forall u < t$, $e(u) < e(t)$ ainsi que leur factorisation.

Dans la deuxième colonne sont indiquées les valeurs approchées de $(e(t))^2$, toujours arrondies inférieurement.

t	$(e(t))^2$	t	$(e(t))^2$
$2 = 2$	5,7600000 E 002	$15\,120 = 2^4.3^3.5.7$	5,0831601 E 158
$4 = 2^2$	5,7600000 E 004	$25\,200 = 2^4.3^2.5^2.7$	1,7575997 E 179
$6 = 2.3$	2,5401600 E 005	$30\,240 = 2^5.3^3.5.7$	3,6417363 E 191
$12 = 2^2.3$	4,2928704 E 009	$42\,840 = 2^3.3^2.5.7.17$	2,9544609 E 202
$24 = 2^3.3$	1,7171481 E 010	$45\,360 = 2^4.3^4.5.7$	1,5723798 E 206
$30 = 2.3.5$	2,9537234 E 010	$55\,440 = 2^4.3^2.5.7.11$	2,4216182 E 213
$36 = 2^2.3^2$	1,9094176 E 016	$60\,480 = 2^6.3^3.5.7$	1,6174651 E 232
$60 = 2^2.3.5$	4,6436150 E 019	$75\,600 = 2^4.3^3.5^2.7$	3,8056040 E 233
$72 = 2^3.3^2$	4,0701147 E 020	$85\,680 = 2^4.3^2.5.7.17$	6,2539126 E 258
$108 = 2^2.3^3$	2,0417212 E 021	$100\,800 = 2^6.3^2.5^2.7$	7,8670318 E 268
$120 = 2^3.3.5$	3,1223667 E 023	$110\,880 = 2^5.3^2.5.7.11$	4,4490778 E 274
$144 = 2^4.3^2$	4,7050525 E 023	$128\,520 = 2^3.3^3.5.7.17$	7,2908267 E 290
$180 = 2^2.3^2.5$	6,7665379 E 030	$131\,040 = 2^5.3^2.5.7.13$	6,2430632 E 303
$240 = 2^4.3.5$	2,0964081 E 031	$166\,320 = 2^4.3^3.5.7.11$	4,8871405 E 313
$360 = 2^3.3^2.5$	2,4245991 E 038		
$420 = 2^2.3.5.7$	1,4074436 E 041		
$540 = 2^2.3^3.5$	1,5552318 E 046		
$720 = 2^4.3^2.5$	1,6279155 E 046		
$840 = 2^3.3.5.7$	7,4725932 E 049		
$1\,008 = 2^4.3^2.7$	8,5368948 E 050		
$1\,080 = 2^3.3^3.5$	5,5727372 E 053		
$1\,200 = 2^4.3.5^2$	1,0212596 E 058		
$1\,260 = 2^2.3^2.5.7$	1,3170657 E 062		
$1\,620 = 2^2.3^4.5$	6,4271819 E 063		
$1\,680 = 2^4.3.5.7$	7,2757866 E 066		
$2\,016 = 2^5.3^2.7$	5,9203218 E 067		
$2\,160 = 2^4.3^3.5$	3,2760144 E 073		
$2\,520 = 2^3.3^2.5.7$	2,3683136 E 081		
$3\,360 = 2^5.3.5.7$	1,4010401 E 084		
$3\,780 = 2^2.3^3.5.7$	2,4917603 E 088		
$5\,040 = 2^4.3^2.5.7$	2,3476327 E 104		
$6\,480 = 2^4.3^4.5$	9,5661076 E 104		
$7\,560 = 2^3.3^3.5.7$	2,5615126 E 115		
$8\,400 = 2^4.3.5^2.7$	2,6638720 E 119		
$10\,080 = 2^5.3^2.5.7$	1,8391306 E 128		
$12\,600 = 2^3.3^2.5^2.7$	9,7437932 E 137		

TABLE 2

Dans l'exemple $t = 5\,040$, utilisable pour $n < 2,3.10^{104}$ voici la liste des facteurs premiers $q > 2$ de $e(5\,040)$ suivie de la décomposition en facteurs premiers de $q - 1$:

q	q-1	q	q-1
2 521	$2^3.3^2.5.7$	61	$2^2.3.5$
1 009	$2^4.3^2.7$	43	$2.3.7$
631	$2.3^2.5.7$	41	$2^3.5$
421	$2^2.3.5.7$	37	$2^2.3^2$
337	$2^4.3.7$	31	$2.3.5$
281	$2^3.5.7$	29	$2^2.7$
241	$2^4.3.5$	19	2.3^2
211	$2.3.5.7$	17	2^4
181	$2^2.3^2.5$	13	$2^2.3$
127	$2.3^2.7$	11	2.5
113	$2^4.7$	7	2.3
73	$2^3.3^2$	5	2^2
71	$2.5.7$	3	2