Séminaire Delange-Pisot-Poitou. Théorie des nombres

Henri Cohen

Méthodes de factorisation et nombre de classes des corps quadratiques

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 14, n° 2 (1972-1973), exp. n° G7, p. G1-G10

<http://www.numdam.org/item?id=SDPP_1972-1973__14_2_A14_0>

Séminaire DELANGE-PISOT-POITOU
(Groupe d'étude de théorie des nombres)
14e année, 1972/73, n° G7, 10 p.

11 décembre 1972

MÉTHODES DE FACTORISATION ET NOMBRE DE CLASSES DES CORPS QUADRATIQUES

par Henri COHEN

Mon but est d'exposer une nouvelle méthode de factorisation des nombres entiers découverte récemment par D. SHANKS [2] ; un outil essentiel est la possibilité de calculer rapidement le nombre $h(-D)$ de classes de formes quadratiques positives primitives (f. q. p. p.), de discriminant $-D$, et donc aussi le nombre de classes d'idéaux d'un ordre d'un corps quadratique imaginaire. La structure de groupe s'obtient également très facilement si on le désire.

Rappelons d'abord les méthodes existantes.

1. Méthodes classiques de factorisation.

Nous nous placerons toujours du point de vue d'un individu ayant l'usage d'un ordinateur et qui veut factoriser un nombre N, et nous comparerons les méthodes du point de vue de leur rapidité pour des N d'une certaine taille. En général, on est amené à utiliser plusieurs méthodes simultanément. La meilleure référence semble être D. KNUTH [1].

1.1. La méthode des diviseurs (D). - C'est la méthode la plus naturelle. On choisit une suite d'entiers facile à déterminer $1 < d_1 < d_2 < \dots < d_n < \dots$, contenant tous les nombres premiers, et on divise N successivement par $d_1, d_2, \dots$ jusqu'au plus grand $d_i \leqslant \sqrt{N}$. Si aucun de ces d_i ne divise N, alors N est premier, sinon le plus petit des d_i rencontrés, qui divise N, est le plus petit facteur premier de N, et si on veut la factorisation complète, on recommence à travailler sur N/d_i.

Par exemple, si $d_i = i + 1$, la méthode prend au plus $\sqrt{N}$ divisions. Si $d_i = p_i$ le i-ième nombre premier, la méthode prend au plus $\pi(\sqrt{N}) \sim (2\sqrt{N})/\log N$ opérations. En général, les méthodes intermédiaires entre ces deux exemples sont optimales, car on ne dispose pas d'une table infinie (ou même allant jusqu'à 10^8) de nombres premiers. On choisit un entier k, et on prend $d_i = p_i$ pour $i \leqslant k$, et la suite croissante des entiers non divisibles par $p_1, \dots, p_k$ pour $i > k$. Typiquement, pour des nombres de l'ordre de 10^{12} à 10^{16}, on prend $k = 9$ ou 10 (i. e. $p_k = 23$ ou 29).

De toutes façons, quelle que soit la variante adoptée, la méthode est pratiquement en $O(N^{\frac{1}{2}})$ opérations, le petit facteur logarithmique apporté par la possession d'une très grande table de nombres premiers étant négligeable en pratique par rapport à une méthode intermédiaire convenable.

Si on veut que le temps de calcul soit raisonnable, on ne peut guère dépasser de N de l'ordre de 10^{15} à 10^{16}.

1.2. La méthode de Fermat (F). - De même que toutes les autres méthodes moins "naturelles", on l'utilise quand on n'a pas réussi à trouver de petits diviseurs par la méthode D.

La méthode de Fermat consiste à trouver le plus petit y tel que $N = x^2 - y^2$. Si $y \neq x - 1$, ceci fournit une factorisation de N. Cette méthode revient à chercher les diviseurs de N en descendant, partant de $\sqrt{N}$, et a divers avantages tel que le fait que l'on peut éviter toute division, et utiliser des cribles pour reconnaître les carrés. Elle est encore en $O(N^{\frac{1}{3}})$ et pas moins.

La méthode ci-dessous est en général meilleure, mais est plus complexe.

1.3. La méthode de Legendre (L). - Elle consiste à résoudre la congruence $x^2 \equiv y^2 \pmod N$; si les seules solutions sont $x = \pm y \pmod N$, alors N est premier. Sinon $(N , x - y)$ ou $(N , x + y)$ sont des diviseurs non triviaux de N. C'est une généralisation de la méthode de Fermat. En général, on ne l'utilise qu'après avoir vérifié que N n'est pas premier (voir 1.4).

Pour résoudre la congruence, on cherche les petits résidus quadratiques a de N, i. e. les solutions de $x^2 \equiv a \pmod N$. Si on trouve deux solutions possibles, alors on a une solution de $x^2 \equiv y^2 \pmod N$. Plus généralement, si on a une solution de $x^2 \equiv a \pmod N$ et $y^2 \equiv b \pmod N$, et que ab est un carré, $ab=c^2$, alors $(xy)^2 \equiv c^2 \pmod N$ fournit une solution.

Pour trouver des petits résidus mod N, on emploie la méthode des fractions continues. Soit k un petit entier, et supposons que x/d est un convergent de la fraction continue pour $\sqrt{kN}$. Alors $|x^2 - kNd^2|$ est petit, et si on pose

$$x^2 - kNd^2 = a ,$$

on a donc un petit résidu (mod N). Pour plus de détails sur cette méthode, je renvoie à D. KNUTH [1].

Cette méthode possède un gros avantage supplémentaire : même si l'on n'obtient pas de solutions de la congruence, le fait d'obtenir des petits résidus quadratiques entraîne, via la loi de réciprocité, que les diviseurs premiers de N sont dans certaines progressions arithmétiques. Par exemple, si on trouve une solution de $x^2 \equiv 2 \pmod N$, alors on sait que si $p|N$, on doit avoir $p \equiv \pm 1 \pmod 8$; ce qui divise par 2 le nombre de diviseurs possibles, et accélère donc notablement la méthode (D). C'est d'ailleurs ainsi que LEHMER, BRILLHART et JOHNSON ont trouvé que :

$$2^{101} - 1 = 742339208719.341117531003194129 .$$

Cette factorisation n'aurait pas pu être découverte en un temps raisonnable par (D) ou (F) seuls.

1.4. Tests de primalité (P). - Les tests de primalité les plus utiles sont fournis par une réciproque au théorème de Fermat. Ce théorème affirme que si p est premier et $(a , p) = 1$, alors $a^{p-1} \equiv 1 \pmod p$. La réciproque directe est fausse. En effet, il est facile de voir par exemple que, pour $p = 561 = 3.11.17$, alors

$$(a , p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod p .$$

Le résultat correct est le suivant (voir par exemple KNUTH [1]).

THÉORÈME 1.4.1. - Pour que N soit premier, il faut et il suffit que, pour tout diviseur premier p de $N - 1$, il existe un x_p tel que

$$x_p^{N-1} \equiv 1 \pmod N ,$$

mais

$$x_p^{(N-1)/p} \not\equiv 1 \pmod N .$$

Ceci fournit un test extrêmement efficace de primalité. En effet, une expression de la forme $a^b \pmod c$ s'évalue très rapidement (en $O(\log b)$ opérations) en décomposant b en binaire et en calculant a , a^2 , a^4 , a^8 , ... mod c , et multipliant chaque exposant figurant dans la décomposition binaire de b . Le seul problème est que ce test nécessite de connaître la factorisation de $N - 1$ (Il est remarquable que la factorisation de N dépende de celle de $N - 1$!). S'il est trop difficile de trouver cette factorisation, d'autres tests en $O(\log N)$ opérations sont disponibles, utilisant la factorisation de $N + 1$ à la place de $N-1$.

Ce test en $O(\log N)$ opérations est très efficace, et permet de montrer la primalité de nombres très grands. Malheureusement, si on tombe sur un N très grand tel que $3^{N-1} \not\equiv 1 \pmod N$ par exemple, et que la méthode (D) n'a pas fourni de diviseurs de taille raisonnable, on est obligé de recourir à l'algorithme (L), ou (S) ci-dessous.

Rappelons également que, pour des nombres d'une forme particulière, par exemple de la forme $N = h.2^n - 1$, où h est petit, on dispose de tests également en $O(\log N)$ opérations particulièrement bien adaptés. C'est ainsi que l'on a découvert que le nombre

$$2^{19937} - 1$$

était premier. C'est à ce jour le plus grand nombre premier connu explicitement (*).

(*) Voir : TUCKERMAN (Bryant). - The 24th Mersenne prime, Notices of American mathematical Society, t. 18, 1971, p. 608. Plusieurs personnes, dont moi-même, ont indépendamment vérifié le fait que $2^{19937} - 1$ est premier, vérification qui prend entre 10 et 40 heures sur des ordinateurs courants. C'est donc un résultat digne de foi.

2. Rappels sur les formes quadratiques binaires.

Nous noterons (A , B , C) la forme quadratique

$$Ax^2 + Bxy + Cy^2 ,$$

où A , B , C sont entiers ; $-\Delta = B^2 - 4AC$ est le discriminant.

Nous supposerons toujours dans la suite $\Delta > 0$, i. e. que le déterminant est négatif. A et C sont alors de même signe et il est clair que l'on peut se restreindre à étudier les formes positives (i. e. avec $A , C > 0$).

Nous supposerons le lecteur familier avec les notions de forme primitive, de réduction, et de composition des formes binaires, que nous utiliserons fondamentalement dans la suite.

Voici deux algorithmes efficaces pour effectuer la réduction et la composition.

Algorithme de réduction. - On cherche une forme réduite équivalente à (A,B,C) . On itère le procédé suivant jusqu'à ce qu'on obtienne une forme réduite. Soit D l'entier tel que $-C < B + 2DC \leqslant C$; alors on pose

$$B_1 = -(B + 2DC) , \quad C_1 = A + \tfrac{1}{2}(B - B_1) D , \quad A_1 = C$$

et on continue sur (A_1 , B_1 , C_1) si elle n'est pas réduite.

Algorithme de composition. - Soient $F_1 = (A_1 , B_1 , C_1)$ et $F_2 = (A_2 , B_2 , C_2)$ deux f. q. p. p. de même discriminant, et supposons $A_1 \leqslant A_2$ par exemple. On pose

$$S = \tfrac{1}{2}(B_1 + B_2) , \quad N = B_2 - S , \quad D = (A_1 , A_2) ;$$

soient X_1 , Y_1 tels que

$$A_2 Y_1 - A_1 X_1 = D .$$

Posons $D_1 = (D , S)$, et soient X_2 , Y_2 tels que

$$SX_2 - DY_2 = D_1 .$$

Posons

$$V_1 = A_1/D_1 , \quad V_2 = A_2/D_2 , \quad X = C_2 D_1 , \quad M = Y_1 Y_2 N - C_2 X_2 .$$

Par division euclidienne, on détermine Q , R tels que $M = QV_1 + R$, et on pose $Y = X + R(B_2 + V_2 R)$.

Alors on prend

$$A_3 = V_1 V_2$$
$$B_3 = B_2 + 2V_2 R$$
$$C_3 = Y/V_1$$

et il suffit de réduire (A_3 , B_3 , C_3) par l'algorithme de réduction ci-dessus pour obtenir le composé de F_1 , F_2 .

Je laisse au lecteur le soin de montrer la validité de cet algorithme.

3. Théorie de la méthode.

3.1. On dit qu'une f. q. p. p. F est ambige si $F^2 = I$.

THÉORÈME 3.1.1. - Pour qu'une forme réduite $F = (A , B , C)$ soit ambige, il faut et il suffit que l'une des trois conditions suivantes soit vérifiée

(i) $B = 0$

(ii) $A = B$

(iii) $A = C$.

Or la possession d'une forme ambige fournit immédiatement une factorisation du discriminant $-\Delta$:

(i) $\Delta = 4AC$ (ii) $\Delta = A(4C - A)$ (iii) $\Delta = (2A - B)(2A + B)$.

On a même le théorème fondamental suivant.

THÉORÈME 3.1.2. - Les classes ambiges correspondent biunivoquement aux factorisations $\Delta = fg$ avec $(f , g) = 1 , 2 , 4$.

Exemple. - Si $-\Delta \equiv 1 \pmod 4$, on ne peut qu'avoir $(f , g) = 1$, et si $\Delta = fg$ et $f < g$, on a la forme ambige

$$(f , f , \tfrac{1}{4}(f + g)) \quad \text{si} \quad 3f < g$$
$$(\tfrac{1}{4}(f + g) , \tfrac{1}{2}(g - f) , \tfrac{1}{4}(f + g)) \quad \text{si} \quad f < g < 3f .$$

Bien entendu dans ce cas (i) ne peut pas se produire puisque B est impair.

On voit donc que factoriser Δ revient à trouver les classes ambiges, i. e. la structure du 2-sous-groupe de Sylow.

Soit $h(-\Delta) = 2^S.T$ le nombre de classes de f. q. p. p., avec T impair. Le 2-sous-groupe de Sylow est d'ordre 2^S . L'application $F \longrightarrow F^T$ envoie les h classes dans ce sous-groupe. Si $G = F^T$, on élève G successivement au carré : G , G^2 , G^4 , ... jusqu'à obtenir une forme ambige, que nous appellerons la forme déduite de F . Cette forme ne sera pas l'identité (à moins que G ne le soit déjà, et alors on prend un autre F), et fournira donc une factorisation, peut-être triviale, de Δ . Une application répétée de ce procédé permet facilement de déterminer la structure du groupe des classes ambiges, et donc la factorisation de Δ .

Il est à remarquer que si l'on obtient deux fois la factorisation triviale de Δ à l'aide d'une classe ambige $\mathfrak{A}$, avec $G_1^2 = \mathfrak{A}$, $G_2^2 = \mathfrak{A}$, alors $G_1 G_2^{-1}$ sera ambige, différente de l'identité et de $\mathfrak{A}$.

4. Méthode rapide de calcul de $h(-\Delta)$.

Comme on vient de le voir, tout repose sur le calcul exact de $h(-\Delta)$, où

$$-\Delta \equiv 0 \quad \text{ou} \quad 1 \pmod 4 .$$

On a $h(-3) = h(-4) = 1$. Si $\Delta > 4$, alors on sait que

$$h(-\Delta) = (\sqrt{\Delta}/\pi)\, L(1 , \chi_\Delta)$$

où

$$L(1 , \chi_\Delta) = \sum_{n=1}^{\infty}((-\Delta/n)/n) = \prod_{p \text{ premier}}(p/(p - (-\Delta/p))) .$$

La méthode classique de Dirichlet donnant $L(1 , \chi_\Delta)$ comme une somme finie, ou la méthode de Gauss consistant à compter les formes réduites de discriminant $-\Delta$, prennent toutes $O(\Delta)$ opérations et pas moins. C'est beaucoup trop long si on veut l'appliquer à des Δ de l'ordre de 10^{16} ou plus, ce qui est notre but.

D'autre part, il est facile de voir qu'une fois $h(-\Delta)$ trouvé, le reste des opérations nécessaires pour factoriser Δ prend $O(\log \Delta)$ opérations, ce qui est négligeable.

Voici donc comment l'on procède pour calculer $h(-\Delta)$.

Dans un premier temps, on calcule une approximation à $h(-\Delta)$ par la formule

$$h'(-\Delta) = \frac{\sqrt{\Delta}}{\pi} \prod_{p \leqslant P}(p/(p - (-\Delta/p))) ,$$

où P est un nombre premier assez grand (un bon choix est $P \# 2\Delta^{\frac{1}{4}}$), et on calcule $(-\Delta/p)$ rapidement grâce à la loi de réciprocité.

Pour des nombres Δ de l'ordre de 10^{20} , on peut montrer que l'erreur relative sera presque toujours $< \frac{1}{1000}$. En fait, la probabilité pour que l'erreur relative soit $> z$ est

$$f(P , z) \leqslant 2A \exp(-BP(\log(1 + z))^2) \quad \text{avec} \quad A , B \text{ voisins de } 1 ,$$

ce qui est ridiculement petit pour $z = 1/20$ par exemple.

Dans un deuxième temps, on cherche les relations du type

$$h(-\Delta) \equiv k \pmod{b}$$

que l'on connait.

Si on n'en connaît pas, on met $b = 1$, $k = 0$. On connaît beaucoup de relations de ce type. Par exemple, si $\Delta = 4N$,

$$N \equiv 1 \pmod 4 \Rightarrow h(-\Delta) \equiv 0 \pmod 2 ,$$

pour ne citer que la plus simple, ce qui se démontre aisément en constatant, par exemple, que la forme $(2 , 2 , (N + 1)/2)$ est ambige.

Dans une troisième étape, on choisit H vérifiant les relations obtenues, le plus proche de l'approximation $h'(-\Delta)$. De plus, au cours du calcul de $h'(-\Delta)$, on a en particulier déterminé les petits nombres premiers $p > 2$ tels que

$$(-\Delta/p) = +1 .$$

Pour chacun de ces p , on a $-\Delta \equiv B_p^2 \pmod p$ pour un certain B_p que nous choisirons pair si $\Delta \equiv 0 \pmod 4$, impair si $\Delta \equiv 3 \pmod 4$. Alors $\Delta + B_p^2 = 4p\, C_p$,

et nous garderons un petit stock des formes

$$F_p = (p\ ,\ B_p\ ,\ C_p)\ .$$

L'idée essentielle est simple : si $h = h(-\Delta)$ est le nombre correct de classes, on doit avoir $F^h = I$ pour tout F. On calcule donc F^H (rapidement, en exprimant H en binaire, comme pour tout calcul de puissance ; ceci ne nécessite que $O(\log H)$ opérations). Si $F^H \neq I$, on doit apporter une correction pour obtenir h :

$$h = H + C\ .$$

Bien sûr on peut essayer successivement $C = \pm b\ ,\ \pm 2b$, etc... jusqu'à ce que l'on obtienne $H + C$ satisfaisant à $F^{H+C} = I$. Toutefois, si H est grand, ceci risque d'être long, et la méthode suivante est beaucoup plus rapide.

Pour un entier s à déterminer, on calcule

$$F^{bn} = (A_n\ ,\ B_n\ ,\ C_n) \qquad (n = 1\ ,\ 2\ ,\ \ldots\ ,\ s)\ .$$

(d'où immédiatement $F^{-bn} = (A_n\ ,\ -B_n\ ,\ C_n)$).

Si pour un $n = -s\ ,\ \ldots\ ,\ s$ on obtient

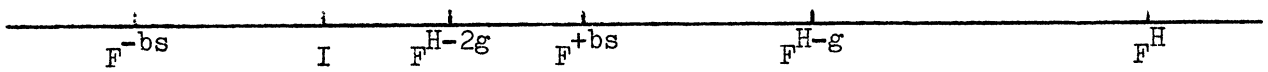
$$F^H = F^{bn} \quad (\text{i. e. } A_H = A_n \text{ et } B_H = \pm B_n\ ),$$

alors on a $F^{H-bn} = I$. On identifie deux formes aisément grâce à l'unicité de leur forme réduite.

Si l'on n'obtient pas une telle identification, on pose $g = 2sb$, et on calcule F^{H+rg} pour $r = +1\ ,\ -1\ ,\ +2\ ,\ -2\ ,\ \ldots$ jusqu'à ce qu'on obtienne $F^{H+rg} = F^{bn}$. On a alors

$$F^{H+rg-bn} = I\ .$$

Graphiquement



On translate H par la largeur de la bande $-bs < n \leqslant bs$, jusqu'à ce que l'on tombe dans la bande permise. Pour minimiser le nombre de compositions, on veut

$$|2r| \simeq s\ .$$

Puisque $C = rg - bn$ et que, en gros, on suppose $C \leqslant H/1000$, on pense que

$$rg \simeq s^2\, b \simeq \frac{H}{1000}$$

semble donner une bonne valeur de s. On prendra donc

$$s = \left(\frac{H}{1000b}\right)^{\frac{1}{2}}\ .$$

Puisque $h = O(\Delta^{\frac{1}{2}+\varepsilon})$ le nombre de compositions nécessaires est

$$2s = O(H^{\frac{1}{2}}) = O(\Delta^{\frac{1}{4}+\varepsilon})\ .$$

Nous ne sommes pas encore entièrement sûrs que le $h = H + C$ soit correct. La vraie valeur de h peut-être un multiple. Pour être sûr, on doit déterminer la

structure de groupe toute entière, ce qui se fait en généralisant la technique expliquée ci-dessus pour le 2-sous-groupe de Sylow. De toutes façons, l'éventualité d'une erreur, même sans vérifications, est comme on l'a déjà dit très faible.

5. Méthode de factorisation de Shanks (S).

On veut factoriser un nombre N. Si $N \equiv 0, 3 \pmod 4$, on prend $\Delta = N$. Sinon, on prend $\Delta = 4N$.

On calcule $h(-\Delta)$ par la méthode du § 4, et on trouve le 2-sous-groupe de Sylow par la méthode du § 3. On trouve ainsi toutes les factorisations $f - g = \Delta$ avec $(f, g) = 1, 2, 4$. Si on a trouvé une factorisation non triviale, on a gagné. Sinon ce n'est pas encore tout à fait fini. Pour simplifier, supposons

$$N \equiv 3 \pmod 4,$$

donc $\Delta = N$.

Si les seules factorisations obtenues avec $(f, g) = 1$ sont $\Delta = 1.\Delta = \Delta.1$, cela prouve seulement que Δ est puissance d'un nombre premier, d'exposant impair puisque $\Delta \equiv 3 \pmod 4$. Or il est facile de montrer que si $p^3 | \Delta$, alors $p | h(-\Delta)$. Il suffit donc de calculer $(\Delta, h(-\Delta))$ par l'algorithme d'Euclide (en $O(\log \Delta)$ opérations). Si c'est plus grand que 1, cela donne un diviseur de Δ, sinon Δ est premier.

Cette méthode a donc l'avantage d'être à la fois un test de primalité et une méthode de factorisation.

6. Exemples.

(a) Supposons que l'on veuille factoriser $N = 49649$. Je donne cet exemple pour montrer comment on fait les calculs à la main, mais bien entendu, dans ce cas, il est beaucoup plus rapide d'utiliser la méthode (D).

Puisque $N \equiv 1 \pmod 4$, on prend $\Delta = 4N = 198596$. On trouve $2.\Delta^{\frac{1}{4}} \simeq 42$ et les symboles de Legendre, pour

$$p = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,$$

sont respectivement

$$0, 1, 1, 1, 1, -1, 1, 1, 1, 1, -1, -1, 1,$$

et on trouve une approximation $h' \# 186$ qui satisfait à $h' \equiv 0 \pmod 2$ que l'on connaît a priori. On choisit donc $H = 186$.

On prend maintenant la première forme F stockée, soit

$$F_3 = F = (3, -2, 16550) ;$$

on obtient successivement :

$F^2 = (9 , 4 , 5517)$ $(F \times F)$

$F^4 = (81 , 4 , 613)$ $(F^2 \times F^2)$

$F^8 = (105 , 22 , 474)$ $(F^4 \times F^4)$

$F^{16} = (146 , -130 , 369)$ $(F^8 \times F^8)$

$F^{32} = (45 , -22 , 1106)$ $(F^{16} \times F^{16})$

$F^{64} = (77 , 36 , 649)$ $(F^{32} \times F^{32})$

$F^{128} = (165 , -58 , 306)$ $(F^{64} \times F^{64})$

$F^{192} = (105 , 92 , 493)$ $(F^{128} \times F^{64})$

$F^{190} = (81 , 4 , 613)$ $(F^{192} \times F^{-2} = F^{192}) \times (9 , -4 , 5517)$

et on constate que $F^{190} = F^4$, donc $F^{186} = I$. Nous sommes donc pratiquement certains que $h(-\Delta) = 186$. Pour en être sûr, nous allons déterminer la structure du groupe. Ici nous avons de la chance : montrons que F est un générateur (donc que le groupe est cyclique). Au passage nous déterminerons la factorisation de Δ grâce à F^{93} .

D'abord les diviseurs premiers de 186 sont 31 , 3 , 2 . On a

$$F^{186/31} = F^6 \neq I \quad \text{car sinon} \quad F^8 = F^2$$

$$F^{186/3} = F^{62} \neq I \quad \text{car sinon} \quad F^{64} = F^2 .$$

Enfin calculons $F^{93} = F^{186/2}$.

$F^3 = (27 , 4 , 1839)$ $(F \times F^2)$

$F^{96} = (61 , -52 , 825)$ $(F^{32} \times F^{64})$

$F^{93} = (131 , 0 , 379)$ $(F^{96} \times F^{-3})$

Donc $F^{93} \neq I$, et F est d'ordre exactement 186 .

D'autre part, on obtient également immédiatement la factorisation voulue de N .

$$N = 49649 = 131 \times 379 .$$

(b) $\Delta = 328878692999$. C'est le plus petit Δ tel que $(-\Delta/p) = +1$ pour $p = 2 , 3 , \ldots , 127$. $L(1 , \chi_\Delta)$ est donc très grand, et en fait on a

$$L(1 , \chi_\Delta) = 8 , 21554 \ldots ,$$

d'où

$$h(-\Delta) = 1499699 .$$

On en déduit immédiatement que le 2-sous-groupe de Sylow se réduit à l'identité, donc on n'obtient qu'une seule factorisation $\Delta = 1.\Delta$. Comme il est expliqué au § 5, la vérification $(\Delta , h(-\Delta)) = 1$ montre que Δ est premier.

(c) $\Delta = 928\,185\,925\,902\,146\,563$. Ici $L(1 , \chi_\Delta) = 0,17198$ et

$$h(-\Delta) = 52739552 = 2^5 . 1648111 .$$

Le premier F_p stocké est $F = F_{73} = (73 , 71 , 3178718924322437)$. On calcule alors $G = F^{1648111}$, puis G^2 , G^4 qui est ambige.

$$G^4 = (1189633 , 1189633 , 195057496961) ,$$

d'où la factorisation $\Delta = 1189633.780228798211$.

On ne sait pas encore que cette factorisation est complète. On sait seulement que le 2-sous-groupe de Sylow a un élément d'ordre 8 , donc est

$$S = \underset{\sim}{Z}/32\underset{\sim}{Z} , \quad \underset{\sim}{Z}/16\underset{\sim}{Z} \times \underset{\sim}{Z}/2\underset{\sim}{Z} , \quad \underset{\sim}{Z}/8\underset{\sim}{Z} \times \underset{\sim}{Z}/4\underset{\sim}{Z} \text{ ou } \underset{\sim}{Z}/8\underset{\sim}{Z} \times \underset{\sim}{Z}/2\underset{\sim}{Z} \times \underset{\sim}{Z}/2\underset{\sim}{Z} .$$

On pourrait maintenant choisir un autre F_p , et trouver le $\mathfrak{a}$ correspondant, mais parmi les formes stockées on s'aperçoit que

$$F_{199} = (199 , 101 , 1166062720982609) \text{ vérifie } \left(\frac{199}{1189633}\right) = -1 .$$

et en fait $F_{199}^{1648111}$ est d'ordre 32 , donc $S = \underset{\sim}{Z}/32\underset{\sim}{Z}$, donc aucun autre $\mathfrak{a}$ n'existe ($\neq I$) . Vérifiant enfin $(\Delta , h(-\Delta)) = 1$, on en déduit que la factorisation est complète.

7. Conclusion.

La méthode de Shanks présentée ci-dessous possède plusieurs avantages.

D'abord, elle est en $O(\Delta^{\frac{1}{4}+\varepsilon})$, ce qui est plus rapide que toutes les autres méthodes citées. Malheureusement, la composition étant une opération lente, ne serait-ce qu'à cause des deux p. g. c. d. à faire, la constante devant le grand O est grande. La méthode commence donc à être utile seulement pour des $N > 10^{14}$ pour fixer les idées.

D'autre part, elle a un aspect esthétique indéniable. Au lieu de chercher à tatons un diviseur de N , on va le chercher directement grâce à l'application

$$F \longrightarrow F^T = G$$

qui aboutit dans le 2-sous-groupe de Sylow. On va ainsi à une "adresse" bien déterminée pour trouver la factorisation. Pour de très grands nombres (disons $> 10^{26}$) le calcul de $h(-\Delta)$ peut commencer à devenir trop long. La méthode ne sert alors plus à rien, et il faut se rabattre sur la combinaison (L)-(D) discutée plus haut, qui semble être la plus efficace connue pour d'aussi grands nombres.

BIBLIOGRAPHIE

[1] KNUTH (D.). - Seminumerical algorithms, The Art of Computer Programming, vol 2, p. 338-359. - Reading, Addison-Wesley, 1969.

[2] SHANKS (D.). - Class number, a theory of factorization, and genera, 1969 Number theory institute, p. 415-440. - Providence, American mathematical Society, 1971 (Proceedings of Symposia in pure Mathematics, 20).

Henri COHEN
Université de Bordeaux-I, Mathématiques
351 cours de la Libération
33405 TALENCE

(Texte reçu le 4 juin 1973)