UNE MÉTHODE DE FACTORISATION UTILISANT LES FORMES QUADRATIQUES À DISCRIMINANT POSITIF

1- INTRODUCTION

La méthode de factorisation ci-dessous a été découverte par D. SHANKS, probablement en 1974. Ses avantages principaux sont d'une part la simplicité de la programmation (qui lui permet d'être implémentée sur des calculettes type H.P. 67 ou H.P.41) et d'autre part la faible grandeur des nombres à manipuler : pour factoriser N, la presque totalité du programme opère sur des nombres $\leq 2\sqrt{N}$, ce qui évite pour des nombres jusqu'à 20 chiffres la multiprécision.

La théorie des formes quadratiques, essentiellement due à GAUSS (cf [Gau]) se trouve dans plusieurs ouvrages de théorie des nombres, notamment [Dic], dans lequel on trouvera les démonstrations des théorèmes que nous énonçons. L'algorithme est décrit dans la thèse de 3e cycle de L. Monier ([Mon]), qui est une étude des algorithmes de factorisation actuellement connus. Il mentionne notamment la contribution importante de A.K. LENSTRA à l'étude de l'algorithme ci dessous. On trouvera aussi des informations dans [Sch].

On appelera N le nombre à factoriser ; on suppose N impair. On considère l'ensemble $\mathcal{E}(\Delta)$ des formes quadratiques $ax^2 + 2bxy + cy^2$ à coefficients dans $\mathbb{Z}$ et de discriminant fixé : $\Delta = 4(b^2 - ac) = 4N$. On suppose que N n'est pas un carré parfait : ce sera le premier test de l'algorithme. On appelle $E(\Delta)$ le sous ensemble de $\mathcal{E}(\Delta)$ des formes primitives, c'est à dire telles que p.g.c.d. $(a, 2b, c) = 1$.

On a donc, en écrivant (a,b,c) la forme $ax^2 + 2bxy + cy^2$:

$$\mathcal{E}(\Delta) = \{(a, b, c) \in \mathbb{Z}^3 \quad ; \quad 4(b^2 - ac) = \Delta \}$$

$$E(\Delta) = \{(a, b, c) \in \mathcal{E}(\Delta) \; ; \; \text{p.g.c.d. } (a, 2b, c) = 1 \}$$

Il existe une correspondance entre les formes quadratiques de $E(\Delta)$ et les bases des $\mathbb{Z}$-modules du corps $\mathbb{Q}(\sqrt{N})$ qui rend plus claire la relation d'équivalence, et la loi de composition que nous allons définir (cf [Bor], chap. 2 § 7 et [Sch])

2- RELATION D'EQUIVALENCE

Posons $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$, $X = \begin{pmatrix} x \\ y \end{pmatrix}$; $\quad {}^tX = (x \; y)$

On a alors : $ax^2 + 2bxy + cy^2 = {}^tXAX$. Posons $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, $X = MX'$; on a ${}^tX = {}^tX' \, {}^tM$ et

$$ax^2 + 2bxy + cy^2 = {}^tXAX = {}^tX' \, {}^tMAMX' = a'x'^2 + 2b'x'y + c'y'^2$$

avec $X' = \begin{pmatrix} x' \\ y' \end{pmatrix}$ et $A' = {}^tMAM = \begin{pmatrix} a' & b' \\ b' & c' \end{pmatrix}$. On a en particulier

$$b'^2 - a'c' = \det A' = (\det M)^2 \det A$$

Définition- On dit que deux formes de $\mathcal{E}(\Delta)$, (a, b, c) et (a', b', c') sont équivalentes, s'il existe une transformation linéaire $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, $(\alpha, \beta, \gamma, \delta) \in \mathbb{Z}^4$, vérifiant $|\alpha\delta - \beta\gamma| = 1$, telle que la forme $ax^2 + 2bxy + cy^2$ soit transformée en $a'x'^2 + 2b'x'y' + c'y'^2$.

Il est facile de montrer que c'est une relation d'équivalence, que toute forme équivalente à une forme primitive est primitive, et donc que la trace de cette relation sur $E(\Delta)$ est encore une relation d'équivalence. On notera que $(a, b, c) \sim (a, a+b, a + 2b + c)$ avec $M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $(a, b, c) \sim (c, -b, a)$ avec $M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

3) FORME REDUITE

Définition- On dit que la forme $ax^2 + 2bxy + cy^2 \in E(\Delta)$ est réduite si l'on a :
$|\sqrt{\Delta} - |2a|| < 2b < \sqrt{\Delta}$.

Propriété 1 : Les valeurs absolues des coefficients a, 2b, c d'une forme réduite sont $< \sqrt{\Delta} = 2\sqrt{N}$.

Propriété 2 : Les formes réduites forment un sous ensemble fini de $E(\Delta)$.

Propriété 3 : Dans une forme réduite, on a $b>0$ et $ac<0$.

Propriété 4 : (a, b, c) réduite $\Longleftrightarrow$ (c, b, a) réduite.

Propriété 5 : Une forme réduite de $E(\Delta)$ est déterminée par a et par la valeur de b modulo a.

Propriété 6 : Si l'on pose $\omega_1 = \frac{1}{a}(-b + \sqrt{N})$; $\omega_2 = \frac{1}{a}(-b - \sqrt{N})$, on a :

(a, b, c) réduite $\Longleftrightarrow$ $(|\omega_1|<1 \ ; \ |\omega_2|>1 \ ; \ \omega_1 \omega_2 < 0)$.

Ces propriétés sont faciles à démontrer (cf. [Dic] , p. 100)

Algorithme de listage des formes réduites :

1- Pour $-\sqrt{\Delta} < a < \sqrt{\Delta}$

2- Pour $|\sqrt{\Delta} - |2a|| < 2b < \sqrt{\Delta}$

3- Tester si a divise $N - b^2$

Théorème 1 - Toute forme de E (Δ) est équivalente à une forme réduite.

Démonstration : On pourra consulter [Dic], p. 101, ou vérifier l'efficacité de l'algorithme suivant :

1- Si $|a|<\sqrt{\Delta}$, changer b mod a pour que $\sqrt{\Delta} - 2|a| < 2b < \sqrt{\Delta}$

2- Si $|a|>\sqrt{\Delta}$, changer b mod a pour que $2|b| \leqslant |a|$

3- Si la forme n'est pas réduite, changer (a, b, c) en (c, -b, a)

et recommencer en 1.

4 - REDUCTION

Théorème 2- Soit $\phi = (a, b, a_1) \in E(\Delta)$ une forme réduite ; il existe une et une seule forme $\phi_1 = (a_1, b_1, a_2) \in E(\Delta)$ telle que $b_1 = b \bmod a_1$. On pose $\phi_1 = \sigma\phi$. L'application σ, appelée réduction, est une bijection sur l'ensemble des formes réduites de E (Δ). On a $\sigma\phi \sim \phi$ et si $\phi_1 \sim \phi_2$, $\exists\, k \in \mathbb{Z}$ tel que $\phi_2 = \sigma^k \phi_1$. Enfin il existe $r \geqslant 1$ tel que $\sigma^{2r}\phi = \phi$

Démonstration : cf [Dic] p. 102.

On déduit de ce théorème la description de l'ensemble des formes réduites de E (Δ) : soit h le nombre de classes d'équivalence de E (Δ). D'après le théorème 1 et la propriété 2, ce nombre est fini. Soit $\phi_o^{(1)}, \ldots, \phi_o^{(h)}$ des formes réduites représentant chacune une classe d'équivalence. Soit r_i le plus petit nombre $\geqslant 1$ tel que $\sigma^{2r_i}\phi_o^{(i)} = \phi_o^{(i)}$. Alors l'ensemble des formes réduites de E (Δ) est la réunion des chaines :

$$1 \leqslant i \leqslant h \quad \{ \sigma^k \phi_o^{(i)} \quad , \quad 0 \leqslant k \leqslant 2r_i - 1 \} \quad .$$

Enfin, soit $\phi_o = (Q_o, P_1, -Q_1)$ une forme réduite de E (Δ) ; on aura $\phi_n = \sigma^n \phi_o = ((-1)^{n-1} Q_{n-1}, P_n, (-1)^n Q_n)$. On peut, par l'étude de σ et les propriétés de développement en fractions continue de $\sqrt{N}$ (cf. [Sha]) donner les formules de récurrence :

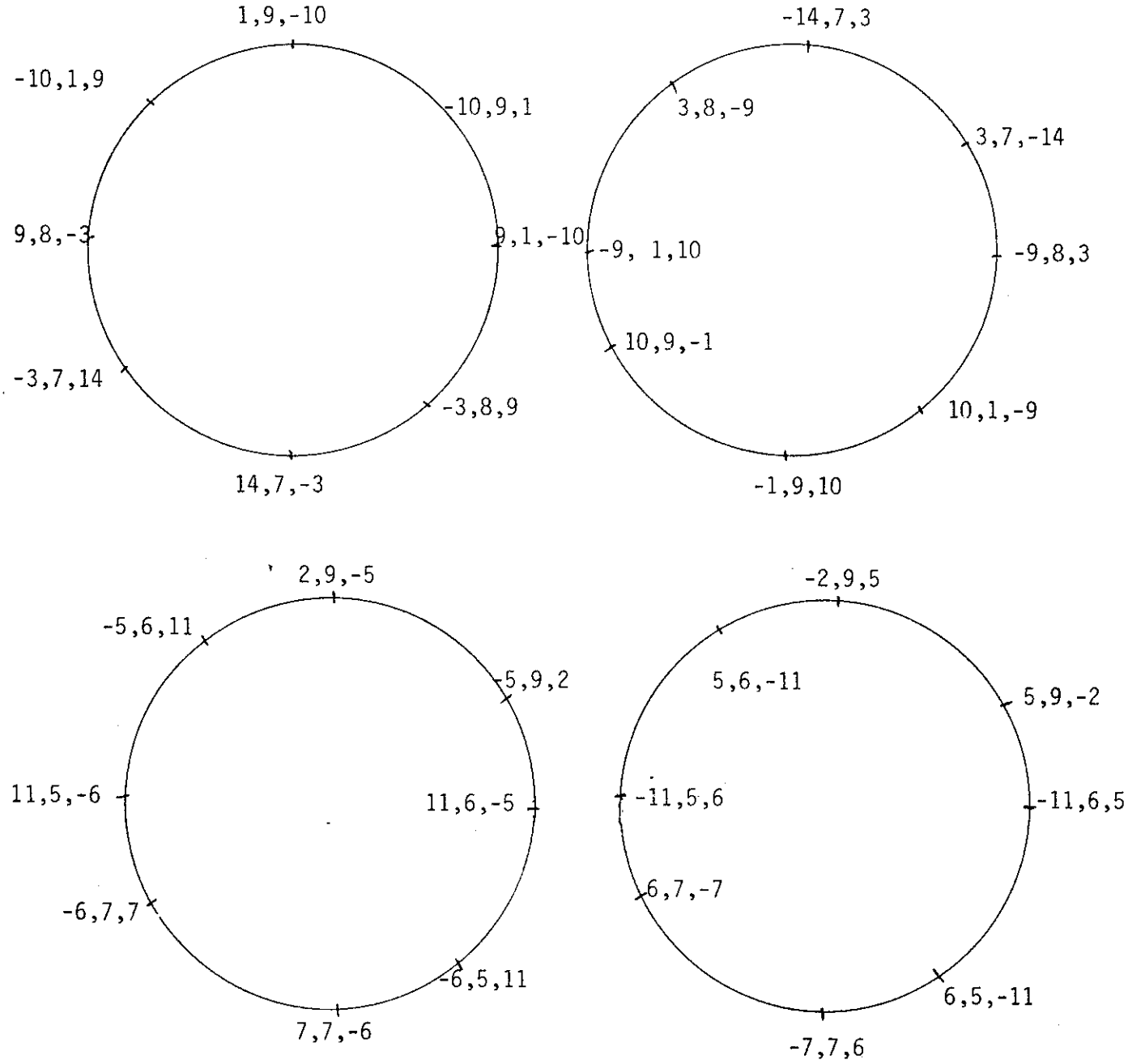
$$q_n = \left[\frac{\sqrt{N} + P_n}{Q_n} \right] ; \qquad P_{n+1} = q_n Q_n - P_n$$

$$Q_{n+1} = Q_{n-1} + q_n (P_n - P_{n+1})$$

On notera que, par la définition de σ et la propriété 3 des formes réduites, le premier coefficient de ϕ_n change de signe avec la parité de n, ce qui explique pourquoi la longueur d'une chaine est paire.

Exercice de programmation : Pour N fixé, écrire toutes les formes réduites, et écrire les différentes chaînes.

Exemple : N = 91



Il y a 4 chaînes de longueur 8. Pour d'autres valeurs de N, les chaînes ne sont pas d'égale longueur.

5- LOI DE COMPOSITION

Soit deux formes (a_1, b_1, c_1) et (a_2, b_2, c_2) dans E (Δ) ; on veut les multiplier de façon que le produit (a_3, b_3, c_3) vérifie $a_3 = a_1 a_2$ et $b_3 = b_1 \bmod a_1$ et $b_3 = b_2 \bmod a_2$.

Lemme. Si p.g.c.d. $(a_1, a_2, b_1+b_2) = 1$, il existe une et une seule solution mod (a_1a_2) des congruences

$$x \equiv b_1 \bmod a_1 \; ; \quad x \equiv b_2 \bmod a_2 \; ; \quad x^2 \equiv N \bmod a_1a_2 .$$

Démonstration : Les deux premières congruences donnent :

$$(x-b_1)\,(x-b_2) \equiv 0 \bmod a_1a_2$$

en développant, on peut remplacer la 3e congruence par

$$(b_1+b_2)x \equiv N + b_1b_2 \bmod a_1a_2 .$$

On se ramène alors à un système classique de congruences linéaires (cf. [Dic], p. 134)

Définition : Si p.g.c.d. $(a_1, a_2, b_1+b_2) = 1$, on dit que la forme $\phi_3 = (a_3, b_3, c_3)$ est obtenue par composition de $\phi_1 = (a_1, b_1, c_1)$ et $\phi_2 = (a_2, b_2, c_2)$ et on écrit $\phi_1 * \phi_2 = \phi_3$ si l'on a $a_3 = a_1a_2$ et si b_3 est une solution des congruences du lemme précédent.

Remarque 1. $I = (1, [\sqrt{N}], -(N - [\sqrt{N}]^2))$ est un élément neutre pour cette composition : $\phi * I = I * \phi = \phi$

Remarque 2. Si ϕ_1 et ϕ_2 sont réduites, ϕ_3 n'est pas en général réduite. En particulier $a_3 = a_1a_2$ ne vérifie pas toujours $|a_3| < 2\sqrt{N}$

Remarque 3. Si p.g.c.d. $(a_1, a_2, b_1+b_2) = d$, soit u, v, w, les coefficients de Bezout :

$$u\,a_1 + v\,a_2 + w\,(b_1 + b_2) = d$$

On adapte alors la définition ci-dessus avec $a_3 = a_1a_2/\,d^2$,

$$b_3 = v\,b_1\,\frac{a_2}{d} + u\,b_2\,\frac{a_1}{d} + w\,\frac{b_1b_2 + N}{d} \pmod{a_3}$$

$$c_3 = (b_3^2 - N)/a_3$$

Remarque 4. La composition $*$ permet de définir une loi de composition dans l'ensemble $F(\Delta)$, quotient de $E(\Delta)$ par la relation d'équivalence :

$$(a, b, c) \overset{\sim}{\sim} (a', b', c') \Longleftrightarrow a = a' \text{ et } b = b' \bmod a$$

On a : $\phi \overset{\sim}{\sim} \phi' \Longrightarrow \phi \sim \phi'$.

Théorème 3. La composition $*$ permet de définir une loi de composition sur l'ensemble quotient $E(\Delta)/\sim$ qui en fait un groupe abélien appelé groupe des classes. L'élément unité est la classe de I et les classes de (a, b, c) et (c, b, a) sont inverses.

Démonstration : cf [Dic], p. 134-140.

6- CARRES

Supposons p.g.c.d. (a, b) = 1. Si a est impair, un carré de $(a, b, -ta)$ $(t \in \mathbb{N})$ est $(a^2, b, -t)$; si a est pair, on trouve $(\frac{a^2}{4}, b, -4t)$. Même si (a, b, -ta) est réduite, il n'y a pas forcément de carré réduit.

Dans l'autre sens, si la forme $(a^2, b, -c)$ est réduite, il existe une racine carrée réduite (si a est impair), de la forme :

$$(a, b+a\left[\frac{\sqrt{N} - b}{a}\right], - c')$$

7- FORMES AMBIGUES

On dit qu'une forme réduite est ambigüe si elle admet un carré égal à I.

La relation (a, b, c) = I entraîne :

$1 = \frac{a^2}{d^2}$ avec d = p.g.c.d. (a, 2b) et donc a divise 2b.

Les formes ambigües triviales vérifient $|a| = 1$ ou $|a| = 2$. La connaissance d'une forme ambigüe non triviale fournit la factorisation de : $\Delta = a(\frac{4b^2}{a} - 4c)$ et un facteur non triviale de N.

8- DESCRIPTION DE LA METHODE DE FACTORISATION

On part de la forme identité I et on décrit la chaine de I en calculant σI, $\sigma^2 I$, ..., $\sigma^n I$ à l'aide des formules de récurrence du §4. On s'arrête lorsqu'on a trouvé une forme carrée F, reconnaissable à son premier coefficient qui est un carré.

Si $F = (a^2, b, -c)$ on calcule alors G par la formule :

$$G = \left(a, -b+a\left[\frac{\sqrt{N}+b}{a}\right], c'\right)$$

On calcule enfin σG, $\sigma^2 G$,... , $\sigma^k G$ jusqu'à trouver une forme ambigüe A reconnaissable au fait suivant : si $\sigma^k G$ et $\sigma^{k+1} G$ ont même coefficient central, alors $\sigma^k G$ est ambigüe.

On peut montrer, par des arguments probabilistes que, si $F = \sigma^{2n} I$ (remarquer que l'exposant doit être pair) et $A = \sigma^k G$, k est voisin de n.

Enfin, il faut écarter les formes carrées F qui conduisent à une forme ambigüe triviale. On peut démontrer que F serait alors le carré d'une forme H qui la précède dans la chaine principale. Une telle forme H serait réduite, de carré réduit, c'est-à-dire vérifie : $H = (a, b, c)$ avec $\begin{cases} a^2 < 2\sqrt{N} & \text{si a est impair} \\ a^2 < 8\sqrt{N} & \text{si a est pair} \end{cases}$

On conserve le carré de ces formes H dans une "queue", et si la forme carré F ne se trouve pas dans la queue elle conduit à une forme ambigüe non triviale et à une factorisation de N.

9- ALGORITHME

1- On s'assure que $\sqrt{N} \notin \mathbb{Z}$

2- On pose $F = I$

3- On fait $F = \sigma F$

- si $F = I$, le programme ne factorise pas N
- si F^2 est réduite, on place F^2 dans la queue
- Si F est un carré qui n'est pas dans la queue on va en 4, sinon on va en 3

4- On calcule G

5- On itère $G = \sigma G$ jusqu'à trouver une forme ambigüe (α, β, γ)

6- α ou $\alpha/2$ est un diviseur de N.

Remarques : 1) La longueur de l'algorithme peut se mesurer au nombre d'appels du sous-programme de calcul de σ. Un argument probabiliste donne pour ce nombre la valeur (cf [Mon])

$$C = \frac{N^{1/4}}{2^P - 1} \quad \text{si} \quad N \text{ a } P+1 \text{ facteurs premiers}$$

avec $C = (9 \log 2)/ (8 - 4\sqrt{2}) = 2{,}66237$.

2) Le nombre de formes à mettre dans la queue est en général de quelques unités ; plus de 10 est exceptionnel.

3) Si N est un nombre premier, on parcourt le cycle principal sans trouver de carré, et le programme s'arrête. Il faut prévoir un test de primalité avant cet algorithme.

Le programme ne donne rien dans quelques autres cas, par exemple si $N = m^2 + 1$, le cycle principal contient deux formes. On peut essayer de factoriser kN, pour $k = 3$ ou 5. Il vaut,mieux alors traiter comme triviales les formes ambigües qui fournissent k comme facteur. Lorsque N est grand, ces cas sont très rares.

10 - PROGRAMME BASIC

Remarques : 1) Le sous programme 20 calcule la nouvelle forme $(P,Q)=(P_{n+1}, Q_{n+1})$ en fonction de l'ancienne $(U, V) = P_n, Q_n)$

2) Le sous programme 40 met éventuellement une forme dans la queue.

3) En 180 et 190, le test utilisé pour vérifier si Q est un carré parfait ne marche pas sur tous les ordinateurs.

4) Pour une machine qui a c chiffres significatifs, on peut factoriser par ce programme un nombre de 2 c chiffres à condition de remplacer dans 95 et 100, P et Q par leur vraie valeur. Le programme en effet ne calcule que des formes réduites, dont les coefficients, (propriété 1) sont $< 2\sqrt{N}$.

5) Le compteur K indique le nombre d'appels au sous programme 20 de calcul de σ.

```
10 K=0
11 DIM Z(100)
15 GOTO 90
20 U=P @ W=Q @ A=INT((R+U)/Q) @
    K=K+1
30 P=A*Q-U @ Q=V+A*(U-P) @ V=W
32 RETURN
40 IF Q>=L THEN RETURN
50 IF Q MOD 2=0 THEN GOTO 51 EL
   SE GOTO 60
51 A=Q/2
52 GOTO 70
60 IF Q>=L/2 THEN RETURN ELSE A
   =Q
70 J=J+1 @ Z(J)=A
80 RETURN
90 INPUT N
95 R=SQR(N) @ L=SQR(8*R) @ J=0
100 V=1 @ P=INT(R) @ Q=N-P*P
110 IF Q#0 THEN GOTO 150
114 DISP "N est le carre de ",P
116 GOTO 290
140 GOSUB 20
150 GOSUB 40
160 GOSUB 20
170 GOSUB 40
180 A=SQR(Q)
190 IF Q#INT(A)^2 THEN GOTO 140
200 IF Q#1 THEN GOTO 210
203 DISP "cycle trop court"
205 GOTO 290
210 IF J=0 THEN GOTO 250
220 FOR I=1 TO J
230 IF A=Z(I) THEN GOTO 140
240 NEXT I
250 U=P @ W=INT((R-U)/A) @ P=U+A
    *W
251 Q=A*(V-W*(W+2*INT(U/A)))-2*(
    U MOD A)*W
252 V=A
255 DISP "K=  ",K
260 GOSUB 20
270 IF P#U THEN GOTO 260
282 DISP "K=  ",K
283 DISP "queue =",J
285 DISP "un facteur de N est",V
    /(2-V MOD 2)
290 END
```

REFERENCES

[Bor] Z.I. BOREVITCH et I.F. CHAFAREVITCH - Théorie des nombres - Gauthier-Villars, Paris, 1967.

[Dic] L.E. DICKSON - Introduction to the theory of numbers - Dover Publications, New-York, 1929.

[Gau] G.F. GAUSS - Disquisitiones Arithmeticae - Traduction française, Blanchard, Paris.

[Mon] L. MONIER - Algorithmes de factorisation d'entiers - thèse de 3e cycle de Paris-Sud, Orsay 1980.

[Sch] R.J. SCHOOF - Quadratic fields and factorization - Studieweek Getaltheorie en computers - Publication du Mathematisch centrum - Amsterdam 1980, p. 165 - 206.

[Sha] D. SHANKS - Solved and unsolved problems in number theory - 2e édition, Chelsea New-York, 1978.

J.L. NICOLAS
Département Mathématiques
U.E.R. des Sciences Limoges
123, rue Albert Thomas
87060 LIMOGES Cédex