Remark. If g.c.d. $(a_1, \ldots, a_n) = 1$, then for each n, Conjecture I holds for all but a finite number of sequences $\{a_1 < a_2 < \ldots < a_n\}$, since by Lemma 2, all counterexamples must have $a_i | \text{l.c.m.}\{1, 2, \ldots, n\}$.

References

[1] R. L. Graham, Personal communication.

[2] J. Marica and J. Schönheim, *Differences of sets and a problem of Graham*, Canad. Math. Bull. 12 (5) (1969), pp. 635–637.

[3] E. Szemerédi, Oral Communication.

[4] Riko Winterle, *A problem of R. L. Graham in Combinatorial Number Theory*, Proceedings of the Louisiana Conference on Combinatorics, Louisiana State University, Baton Rouge, March 1–5, 1970, pp. 357–361.

Received on 10. 6. 1975 (725)

ACTA ARITHMETICA
XXXII (1977)

Unités de norme -1 de $Q(\sqrt{p})$ et corps de classes de degré 8 de $Q(\sqrt{-p})$ où p est un nombre premier congru à 1 modulo 8

par

PIERRE KAPLAN (Nancy)

Introduction. Soit p un nombre premier congru à 1 modulo 8. Il s'écrit:

$$p = 2e^2 - d^2 = e'^2 - 32d'^2. \tag{1}$$

Soit $\varepsilon = \varepsilon_p = S + T\sqrt{p}$ une unité de norme -1 du corps quadratique $Q(\sqrt{p})$; les nombres S et T sont des entiers rationnels tels que $S^2 - T^2 p = -1$, et, comme $p \equiv 1 \pmod 8$, T est impair et S est divisible par 4.

Soient k_2 le corps quadratique $Q(\sqrt{-p})$, $h(-p)$ le nombre de ses classes d'idéaux. Le 2-sous-groupe des classes d'idéaux de k_2 est cyclique d'ordre multiple de 4(1) et on sait (cf. [2], page 402 et ci-dessous § 2) que le corps $k_8 = k_2(i, \sqrt{\varepsilon})$ est l'extension cyclique de degré 4 non ramifiée de k_2.

Dans un travail récent ([3]), H. Cohn et G. Cooke ont trouvé que, si $h(-p) \equiv 0 \pmod 8$, l'extension cyclique de degré 8 non ramifiée de k_2 est le corps $k_{16} = k_8\left(\sqrt{(d + \sqrt{-p})(1-i)\sqrt{\varepsilon}}\right)$ où $\sqrt{-p} = i\sqrt{p}$ et où les signes de d et de T doivent être choisis de manière que $d \equiv -T \pmod 4$. Simultanément ils prouvent que S est divisible par 8 si et seulement si, $h(-p)$ est divisible par 8, c'est-à-dire que $h(-p) \equiv S \pmod 8$.

Dans cette note, nous donnons une démonstration considérablement plus simple de ces résultats. Nous prouvons directement la congruence $S \equiv h(-p) \pmod 8$ à partir d'une condition pour que $h(-p)$ soit divisible par 8. Puis nous montrons que le corps k_{16} est une extension cyclique de degré 8 de k_2 et que cette extension est non ramifiée quand le nombre S est divisible par 8.

Notre démonstration utilise (au § 1) la théorie des formes quadratiques binaires c'est-à-dire la théorie des corps quadratiques et (au § 2)

(1) Si $p \equiv 5 \pmod 8$, $h(-p) \equiv 2 \pmod 4$ et si $p \equiv 3 \pmod 4$, $h(-p)$ est impair.

des rudiments de théorie des corps de nombres, mais, contrairement à H. Cohn et G. Cooke, nous n'avons pas besoin d'utiliser la théorie du corps de classes.

1. Démonstration de la congruence $h(-p) \equiv S \pmod 8$. On connaît plusieurs conditions équivalentes pour que $h(-p) \equiv 0 \pmod 8$. Celles qui nous seront utiles ici sont résumées par les égalités:

$$(2) \qquad (-1)^{\frac{h(-p)}{4}} = \left(\frac{p}{2}\right)_4 \left(\frac{2}{p}\right)_4 = \left(\frac{e}{p}\right)$$

où $\left(\frac{p}{2}\right)_4 = 1$ ou -1, suivant que $p \equiv 1$ ou $9 \pmod{16}$.

Les formules (2) sont prouvées dans [7] par une méthode qui n'utilise que la théorie des formes quadratiques binaires; la deuxième égalité n'est utilisée que dans la remarque ci-dessous.

De $p = e'^2 - 32d'^2$ résulte d'abord $p \equiv e'^2 \pmod{16}$ d'où $\left(\frac{p}{2}\right)_4 = \left(\frac{2}{e'}\right)$. En outre, si d'' désigne la partie impaire de d', on a, puisque $p \equiv 1 \pmod 8$, $\left(\frac{d'}{p}\right) = \left(\frac{d''}{p}\right) = \left(\frac{p}{d''}\right) = 1$, d'après la loi de réciprocité quadratique et la congruence $p \equiv e'^2 \pmod{d''}$.

Soit maintenant (S, T) une solution entière rationnelle de $S^2 - T^2 p = -1$. Comme $S \equiv 0 \pmod 4$, $pT^2 \equiv 1 \pmod{16}$, donc $\left(\frac{2}{T}\right) = \left(\frac{p}{2}\right)_4$.

D'autre part des relations $-1 = S^2 - pT^2$ et $32d'^2 = e'^2 - p$ résulte:

$$(3) \qquad -32d'^2 = (Se' + pT)^2 - p(S + Te')^2.$$

On déduit de (3) d'abord que $\left(\frac{2p}{Se' + pT}\right) = 1$, puis:

$$\left(\frac{2}{p}\right)_4 = \left(\frac{-32d'^2}{p}\right)_4 = \left(\frac{Se' + pT}{p}\right) = \left(\frac{p}{Se' + pT}\right) = \left(\frac{2}{Se' + pT}\right).$$

Nous avons utilisé le fait que $\left(\frac{d'}{p}\right) = 1$ et la loi de réciprocité quadratique.

Comme $p \equiv e'^2 \pmod{32}$, $Se' + pT \equiv Se' + e'^2 T \pmod 8$, donc:

$$\left(\frac{2}{p}\right)_4 = \left(\frac{2}{Se' + e'^2 T}\right) = \left(\frac{2}{e'}\right)\left(\frac{2}{S + e'T}\right) = \left(\frac{p}{2}\right)_4 \left(\frac{2}{S + e'T}\right).$$

On a aussi $(e'T)^2 \equiv pT^2 \equiv 1 \pmod{16}$, donc $e'T \equiv \pm 1 \pmod 8$.

Il en résulte immédiatement que $(-1)^{\frac{S}{4}} = \left(\frac{2}{S + e'T}\right) = \left(\frac{p}{2}\right)_4 \left(\frac{2}{p}\right)_4$. ∎

Remarque. Comme e' est une racine carrée de p modulo 8, $S + e'T \equiv \varepsilon_p \pmod 8$ et la formule

$$(4) \qquad \left(\frac{2}{S + e'T}\right) = \left(\frac{p}{2}\right)_4 \left(\frac{2}{p}\right)_4$$

est l'équivalent pour $p' = 2$ de la formule de Scholz [9]:

$$(5) \qquad \left(\frac{\varepsilon_p}{p'}\right) = \left(\frac{p}{p'}\right)_4 \left(\frac{p'}{p}\right)_4 = \left(\frac{\varepsilon_{p'}}{p}\right) \quad \text{où} \quad p \equiv p' \equiv 1 \pmod 4 \text{ et } \left(\frac{p}{p'}\right) = 1.$$

Notre démonstration de (4) est analogue à celle de D. Estes et G. Pall ([4], page 431) pour la formule (5). Pour vérifier la formule symétrique on remarque que $e'(4d')^{-1}$ est une racine carrée de 2 modulo p, d'où:

$$\left(\frac{\varepsilon_2}{p}\right) = \left(\frac{1 + \sqrt{2}}{p}\right) = \left(\frac{4d'}{p}\right)\left(\frac{4d' + e'}{p}\right) = \left(\frac{d'}{p}\right)\left(\frac{e}{p}\right) = \left(\frac{p}{2}\right)_4 \left(\frac{2}{p}\right)_4,$$

car $4d' + e'$ est une valeur de e.

2. Corps de classes non ramifiés de degrés 2, 4 et 8 de $Q(\sqrt{-p})$. Soit $k(\sqrt{a})$ une extension quadratique du corps de nombres k, où a est un nombre de k premier à 2. On sait que si l'idéal principal (a) est un carré et si la congruence $x^2 \equiv a \pmod 4$ a des solutions dans k, l'extension $k(\sqrt{a})/k$ est non ramifiée.

(a) Considérons l'extension k_4/k_2, où $k_4 = k_2(i) = Q(\sqrt{p}, \sqrt{-p}, i)$ avec $p \equiv 1 \pmod 4$. Ici $a = -1$ et pour résoudre la congruence $x^2 = (y + z\sqrt{-p})^2 \equiv -1 \pmod 4$ il suffit de prendre pour y et z des entiers rationnels, y pair et z impair.

(b) Le groupe de Galois de k_4/k_2 est engendré par la substitution

$$\tau: \sqrt{p} \to -\sqrt{p}; \; i \to -i.$$

Soit $k_8 = k_4(\sqrt{\varepsilon})$ et soit $\varepsilon' = S - T\sqrt{p}$. La substitution τ se prolonge à une substitution $\bar{\tau}$ du groupe de Galois de k_8/k_2 par $\sqrt{\varepsilon} \to \sqrt{\varepsilon'}$. Comme $\sqrt{\varepsilon}\sqrt{\varepsilon'} = \pm i$, $\sqrt{\varepsilon'}$ appartient à k_8, donc $\bar{\tau}$ est un automorphisme de k_8 qui transforme $\sqrt{\varepsilon'}$ en $-\sqrt{\varepsilon}$. Donc $\bar{\tau}^2$ transforme $\sqrt{\varepsilon}$ en $-\sqrt{\varepsilon}$ et $\sqrt{\varepsilon'}$ en $-\sqrt{\varepsilon'}$, si bien que $\bar{\tau}$ est d'ordre 4. Donc l'extension k_8/k_2 est cyclique d'ordre 4.

(c) Supposons à partir de maintenant $p \equiv 1 \pmod 8$. On vérifie alors que k_8/k_2 est une extension non ramifiée. Pour être complet, nous reproduisons la démonstration de [2], page 402:

L'idéal principal (2) se décompose $(2) = \bar{2}^2 = (1+i)^2 = \bar{2}_1\bar{2}_2$ dans les corps k_2, $Q(i)$, $Q(\sqrt{p})$ respectivement. Donc $(2) = \bar{\bar{2}}_1^2\bar{\bar{2}}_2^2$ dans k_4. On a

$$\frac{\varepsilon-1}{2}\cdot\frac{\varepsilon'-1}{2} = \frac{(S-1)^2-T^2p}{4} \equiv 0 \pmod 2$$

et les nombres $\frac{\varepsilon-1}{2}$ et $\frac{\varepsilon'-1}{2}$ étant premiers entre eux:

$$\varepsilon \equiv 1 \pmod{\bar{\bar{2}}_1^4, \bar{\bar{2}}_2^2}; \quad \varepsilon' \equiv 1 \pmod{\bar{\bar{2}}_1^2, \bar{\bar{2}}_2^4}; \quad \varepsilon = -\frac{1}{\varepsilon'} \equiv -1 = i^2 \pmod{\bar{\bar{2}}_3^4}.$$

Soit λ un nombre de k_4 tel que $\lambda \equiv 1 \pmod{\bar{\bar{2}}_1^4}$ et $\lambda = i \pmod{\bar{\bar{2}}_2^4}$.

On a $\varepsilon \equiv \lambda^2 \pmod 4$, ce qui prouve que k_8/k_4, et donc k_8/k_2, sont bien des extensions non ramifiées.

(d) Considérons le corps $k_{16} = k_8(\sqrt{\eta})$ où $\eta = (d+\sqrt{-p})\,(1-i)^{-1}\sqrt{\varepsilon}$.

Soit $\bar{\bar{\tau}}$ l'élément du groupe de Galois de k_{16}/k_2 qui prolonge τ et qui envoie $\sqrt{\eta} = \sqrt{(d+\sqrt{-p})(1-i)^{-1}\sqrt{\varepsilon}}$ sur $\bar{\bar{\tau}}(\sqrt{\eta}) = \sqrt{(d+\sqrt{-p})(1+i)^{-1}\sqrt{\varepsilon'}}$. On a:

$$\frac{\bar{\bar{\tau}}(\sqrt{\eta})}{\sqrt{\eta}} = \sqrt{\frac{1-i}{1+i}\sqrt{\frac{\varepsilon'}{\varepsilon}}} = \sqrt{\frac{-1}{i}\sqrt{\frac{-1}{\varepsilon^2}}} = \sqrt{\frac{-1}{i}\frac{i}{\varepsilon}} = \sqrt{\varepsilon'} \in k_8.$$

Donc $\bar{\bar{\tau}}(\sqrt{\eta})$ appartient à k_{16} et $\bar{\bar{\tau}}$ est un automorphisme de k_{16}.

D'autre part,

$$\bar{\bar{\tau}}^2(\sqrt{\eta}) = \sqrt{(d+\sqrt{-p})(1-i)^{-1}(-\sqrt{\varepsilon})} = i\sqrt{\eta}.$$

Ceci prouve que k_{16}/k_2 est une extension cyclique de degré 8 de k_2.

(e) Comme $p = 2e^2 - d^2$, on a, dans k_2: $\bar{2}^2 e^2 = (d+\sqrt{-p})(d-\sqrt{-p})$.

L'idéal $\bar{2}$ est invariant par le groupe de Galois de k_2/Q, donc $\bar{2}$ divise $d+\sqrt{-p}$ et $d-\sqrt{-p}$; d'autre part, tout diviseur commun à $d+\sqrt{-p}$ et $d-\sqrt{-p}$ divise $2d$ et $2\sqrt{-p}$, donc 2, et, comme e est impair, $(d+\sqrt{-p}) = \bar{2}\mathfrak{a}^2$.

Considérons le nombre $\eta = (d+\sqrt{-p})(1-i)^{-1}\sqrt{\varepsilon}$. Comme dans k_4 et k_8 l'idéal $\bar{2}$ est égal à l'idéal principal $(1-i)$, dans k_4 et k_8 l'idéal principal (η) est égal à $\mathfrak{a}^2$.

Pour prouver que k_{16}/k_8 est non ramifiée, il suffit de vérifier que $\eta \equiv x^2 \pmod 4$ a des solutions $x \in k_8$.

Or on a dans k_4:

$$\eta^2 = (d+\sqrt{-p})^2(1-i)^{-2}(S+T\sqrt{p})$$
$$= (d^2-p+2d\sqrt{-p})\,\frac{i}{2}(S+T\sqrt{p}) \equiv -d\sqrt{p}(S+T\sqrt{p}) \pmod 8,$$

car $p-d^2 = 2(e^2-d^2) \equiv 0 \pmod{16}$ et $\sqrt{-p} = i\sqrt{p}$.

Supposons $h(-p) \equiv 0 \pmod 8$. Alors $S \equiv 0 \pmod 8$, donc $\eta^2 \equiv -dT \pmod 8$.

Choisissons $d \equiv -T \pmod 4$. Comme $T^2 \equiv p \equiv d^2 \pmod{16}$, $-dt \equiv 1 \pmod 8$, donc $\eta^2 \equiv 1 \pmod 8$.

Dans k_8, on a donc $(\eta-1)(\eta+1) \equiv 0 \pmod 8$ et, comme un diviseur commun à $\eta-1$ et $\eta+1$ divise 2, on a soit $\eta \equiv 1$, soit $\eta \equiv i^2 \pmod 4$. Ceci achève de prouver que, si $h(-p) \equiv 0 \pmod 8$, k_{16} est une extension cyclique non ramifiée de degré 8 de $Q(\sqrt{-p})$

Bibliographie

[1] P. Barrucand et H. Cohn, *Note on primes of type x^2+32y^2, class number, and residuacity*, J. Reine Angew. Math. 238 (1969), p. 67–70.

[2] — — *On some class fields related to primes of type x^2+32y^2*, ibid., 262/263 (1973), p. 400–414.

[3] H. Cohn et G. Cooke, *Parametric form of an eight class field*, Acta Arith. 30 (1976), p. 367–377.

[4] D. Estes et G. Pall, *Spinor genera of binary quadratic forms*, J. Number Theory 5 (1973), p. 421–432.

[5] P. Kaplan, *Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-sous-groupe des classes est cyclique et réciprocité biquadratique*, J. Math. Soc. of Japan, 25 (1973), p. 596–608.

[6] — *Sur le 2-groupe des classes d'idéaux des corps quadratiques*, J. Reine Angew. Math. 283/284 (1976), p. 313–363.

[7] — *Cours d'Arithmétique*, U. E. R. de Mathématiques, Nancy 1972.

[8] E. Lehmer, *On the quadratic character of some quadratic surds*, J. Reine Angew. Math. 250 (1971), p. 42–48.

[9] A. Scholz, *Über die Lösbarkeit der Gleichung $t^2-Du^2 = -4$*, Math. Zeitschr. 39 (1935), p. 95–111.

Reçu le 25. 6. 1975 (731)
et dans la forme modifiée le 24. 10. 1975