G) The main theorem

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **34 (1988)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **29.03.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

the same conclusion in 1966, with his method involving effective lower bounds on linear forms of three logarithms; this is also reported in his article of 1971. At about the same time, unaware of Heegner's result, but with similar ideas, concerning elliptic modular functions, Stark proved that no further possible value for d exists. So were determined all the imaginary quadratic fields with class number 1. It was somewhat an anticlimax when in 1968 Deuring was able to straighten out Heegner's proof. The technical details involved in these proofs are far beyond the scope of the present article.

This is the place to say that Gauss' conjecture was also solved in the affirmative. Thanks to the work of Hecke, Deuring, Mordell and Heilbronn, it was established that if $d < 0$ and $|d|$ tends to infinity, then so does the class number of $\mathbf{Q}(\sqrt{d})$. Hence, for every integer $h \geqslant 1$ there exists only finitely many fields $\mathbf{Q}(\sqrt{d})$ with $d < 0$, having class number h.

The determination of all imaginary quadratic fields with class number 2 was achieved by Baker, Stark, Weinberger.

An explicit estimate of the number of imaginary quadratic fields with a given class number was obtained by the efforts of Siegel, Goldfeld, Gross & Zagier. For this matter, I suggest reading the paper of Goldfeld (1985).

G) The main theorem

THEOREM. *Let q be a prime, let $f_q(X) = X^2 + X + q$. The following conditions are equivalent:*

1) $q = 2, 3, 5, 11, 17, 41$.

2) $f_q(n)$ *is a prime for* $n = 0, 1, 2, \ldots, q - 2$.

3) $\mathbf{Q}(\sqrt{1-4q})$ *has class number* 1.

Proof. The implication $1 \to 2$ is a simple verification.

The equivalence of the assertions 2 and 3 was first shown by Rabinovitch in 1912. In 1936, Lehmer proved once more that $2 \to 3$, while $3 \to 2$ was proved again by Szekeres (1974) and by Ayoub & Chowla (1981), who gave the simplest proof. The proof of $3 \to 1$ follows from the complete determination of all imaginary quadratic fields with class number 1. Since this implication requires deep results, I shall also give the proof of $3 \to 2$.

$2 \to 3$ Let $d = 1 - 4q < 0$, so $d \equiv 1 \pmod 4$. If $q = 2$ or 3 then $d = -7$ or -11 and $\mathbf{Q}(\sqrt{d})$ has class number 1, as it was already seen.

Assume now that $q \geqslant 5$. It suffices to show that every prime $p \leqslant \frac{2}{\pi}\sqrt{|d|}$ is inert in $\mathbf{Q}(\sqrt{d})$.

First let $p = 2$; since $q = 2t - 1$ then $d = 1 - 4q = 1 - 4(2t-1) \equiv 5 \pmod 8$, so 2 is inert in $\mathbf{Q}(\sqrt{d})$.

Now let $p \neq 2$, $p \leqslant \frac{2}{\pi}\sqrt{|d|} < \sqrt{|d|}$ and assume that p is not inert. Then $\left(\frac{d}{p}\right) \neq -1$ and, as it was noted, there exists $b \in \mathbf{Z}$, $0 \leqslant b \leqslant p-1$, such that p divides $N(b+\omega)$, where $\omega = \frac{1+\sqrt{d}}{2}$, that is, p divides

$$(b+\omega)(b+\omega') = b^2 + b(\omega+\omega') + \omega\omega' = b^2 + b + \frac{1-d}{4}$$

$$= b^2 + b + q = f_q(b).$$

It should be also noted that $b \neq p-1$, otherwise as it was shown, p divides $1 - d = 4q$, hence $p = q < \sqrt{|d|} = \sqrt{|1-4q|}$, so $q^2 < 4q - 1$, hence $q = 2$ or 3, against the hypothesis.

By hypothesis, $f_q(b)$ is therefore a prime number, hence $\sqrt{4q-1} > p = f_q(b) \geqslant f_q(0) = q$ and again $q = 2$ or 3, against the hypothesis.

This shows that every prime p less than $\frac{2}{\pi}\sqrt{|d|}$ is inert, hence $h = 1$.

$3 \to 1$ If $\mathbf{Q}(\sqrt{1-4q})$ has class number 1 then $d = 1 - 4q = -7, -11, -19, -43, -67, -163$, hence $q = 2, 3, 5, 11, 17, 41$. □

As I have already said, the proof is now complete, but it is still interesting to indicate the proof of $3 \to 2$.

Assume that $d = 1 - 4q$ and that the class number of $\mathbf{Q}(\sqrt{-d})$ is 1. Then either $d = -1, -2, -3, -7$, or $d < -7$, so $d = -p$ with $p \equiv 3 \pmod 4$ and $q > 2$.

As noted before, 2 is inert in $\mathbf{Q}(\sqrt{-p})$, so $p \equiv 3 \pmod 8$. Next, I show that if l is any odd prime, $l < q$, then $\left(\frac{l}{p}\right) = -1$. Indeed, if $\left(\frac{l}{p}\right) = 1$ then l splits in $\mathbf{Q}(\sqrt{-p})$. But $h = 1$, so there exists an algebraic integer $\alpha = \frac{a + b\sqrt{-p}}{2}$ such that $Al = A\alpha \,.\, A\alpha'$. Then $l^2 = N(Al) = N(A\alpha) \,.\, N(A\alpha')$ $= N(A\alpha)^2 = N(\alpha)^2$, so $l = N(\alpha) = \frac{a^2 + b^2 p}{4}$. Hence $p + 1 = 4q > 4l$

$= a^2 + b^2p$, thus $1 > a^2 + (b^2-1)p$ and necessarily $a^2 = 0, b^2 = 1$, hence $4l = p$, which is absurd.

Now assume that there exists $m, 0 \leqslant m \leqslant q-2$, such that $f_q(m) = m^2 + m + q$ is not a prime. Then there exists a prime l such that $l^2 \leqslant m^2 + m + q$ and $m^2 + m + q = al$, with $a \geqslant 1$. Since $m^2 + m + q$ is odd then $l \neq 2$. Also $4l^2 \leqslant (2m+1)^2 + p < \left(\frac{p-1}{2}\right)^2 + p = \left(\frac{p+1}{2}\right)^2$, hence $l < \frac{p+1}{4} = q$. As it was shown, $\left(\frac{l}{p}\right) = -1$. However,

$$4al = (2m+1)^2 + 4q - 1 = (2m+1)^2 + p,$$

hence $-p$ is a square modulo l, so by Gauss' reciprocity law,

$$1 = \left(\frac{-p}{l}\right) = \left(\frac{-1}{l}\right)\left(\frac{p}{l}\right) = (-1)^{\frac{l-1}{2}}\left(\frac{l}{p}\right)(-1)^{\frac{l-1}{2}\times\frac{p-1}{2}} = \left(\frac{l}{p}\right),$$

and this is absurd. □

BIBLIOGRAPHY

[1] AYOUB, R. and S. CHOWLA. On Euler's polynomial. *J. Nb. Th. 13* (1981), 443-445.

[2] BOREVICH, Z. I. and I. R. SHAFAREVICH. *Number Theory*. Academic Press, New York, 1966.

[3] COHN, H. *Advanced Number Theory*. Dover Publ., New York, 1962.

[4] GOLDFELD, D. Gauss' class number problem for imaginary quadratic fields. *Bull. Amer. Math. Soc. 13* (1985), 23-37.

[5] LEHMER, D. H. On the function $x^2 + x + A$. *Sphinx 6* (1936), 212-214.

[6] PRITCHARD, P. A. Long arithmetic progressions of primes: some old, some new. *Math. of Comp. 45* (1985), 263-267.

[7] RABINOVITCH, G. Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörper. *Intern. Congress of Math.*, Cambridge, 1912, vol. 1, 418-421.

[8] RIBENBOIM, P. *Algebraic Numbers*. Wiley-Interscience, New York, 1972.

[9] —— *The Book of Prime Number Records*. Springer Verlag, New York, 1988.

[10] SCHINZEL, A. and W. SIERPIŃSKI. Sur certaines hypothèses concernant les nombres premiers. Remarques. *Acta Arithm. 4* (1958), 185-208 and *5* (1959), p. 259.

[11] SCHINZEL, A. Remarks on the paper « Sur certaines hypothèses concernant les nombres premiers ». *Acta Arithm. 7* (1961), 1-8.

[12] SZEKERES, G. On the number of divisors of $x^2 + x + A$. *J. Nb. Th. 6* (1984), 434-442.

(Reçu le 4 avril 1987)

Paulo Ribenboim

Queen's University
Kingston, Ontario
Canada K7L 3N6