F) The class number

F) THE CLASS NUMBER

The theory of quadratic number fields originated with the study of binary quadratic forms $aX^2 + bXY + cY^2$ (where a, b, c are integers and $ac \neq 0$). The discriminant of the form is, by definition, $D = b^2 - 4ac$. Note that $D \equiv 0$ or $1 \pmod 4$; let $d = \frac{D}{4}$ or $d = D$, respectively.

An integer m is said to be represented by the form if there exist integers x, y such that $m = ax^2 + bxy + cy^2$.

If a form $a'X'^2 + b'X'Y' + c'Y'^2$ is obtained from the above form by a linear change of variables

$$\begin{cases} X = hX' + kY' \\ Y = mX' + nY' \end{cases}$$

where h, k, m, n are integers and the determinant is $hn - km = 1$, then the two forms represent the same integers. In this sense, it is reasonable to consider such forms as being equivalent. Clearly, equivalent forms have the same discriminant.

In "Disquisitiones Arithmeticae" Gauss classified the binary quadratic forms with a given discriminant D. Gauss defined an operation of composition between equivalence classes of forms of a given discriminant. The classes constitute a group under this operation. Gauss showed that, for any given discriminant D, there exist only finitely many equivalence classes of binary quadratic forms.

The theory was later reinterpreted, associating to each form $aX^2 + bXY + cY^2$ of discriminant D, the ideal I of $\mathbf{Q}(\sqrt{d}) = \mathbf{Q}(\sqrt{D})$ generated by a and $\frac{-b + \sqrt{D}}{2}$. Define two non-zero ideals I, I' to be equivalent when there exists a non-zero element $\alpha \in \mathbf{Q}(\sqrt{d})$ such that $I = A\alpha . I'$. Then, equivalent binary quadratic forms correspond to equivalent ideals, and the composition of classes of forms corresponds to the multiplication of equivalence classes of ideals. Thus, $\mathbf{Q}(\sqrt{d})$ has finitely many classes of ideals. Denote by $h = h(d)$ the number of classes of ideals, or class number of the field $\mathbf{Q}(\sqrt{d})$.

The class number $h(d) = 1$ exactly when every ideal of $\mathbf{Q}(\sqrt{d})$ is a principal ideal.

Gauss conjectured that for every $h \geqslant 1$ there exist only finitely many imaginary quadratic fields $\mathbf{Q}(\sqrt{d})$ (with $d < 0$) such that the class number is equal to h. Soon, I shall say more about this conjecture.

I shall now indicate how to calculate the class number of the quadratic field $\mathbf{Q}(\sqrt{D})$. Define the real number θ as follows:

$$\theta = \begin{cases} \frac{1}{2}\sqrt{D} & \text{if} \quad D > 0\,, \\ \\ \frac{2}{\pi}\sqrt{-D} & \text{if} \quad D < 0\,. \end{cases}$$

A non-zero ideal I of A is said to be normalized if $N(I) \leqslant [\theta]$ (the largest integer less than or equal to θ). The ideal I is said to be primitive if there does not exist any prime number p such that Ap divides I.

Let $\mathcal{N}$ denote the set of normalized primitive ideals of A.

If $I \in \mathcal{N}$, if p is a ramified prime then $p^2 \nmid N(I)$, and if p is an inert prime, then $p \nmid N(I)$. So,

$$N(I) = \prod_{r \text{ ramified}} r \times \prod_{p \text{ decomposed}} p^{e(p)}\,.$$

It may be shown that every class of ideals contains a primitive normalized ideal. Since for every $m \geqslant 1$ there exist at most finitely many ideals I of A such that $N(I) = m$, this implies, once more, that the number of classes of ideals is finite.

Note that if $\mathcal{N}$ consists only of the unit ideal $A = A.1$, then $h = 1$. Thus, if every prime p such that $p \leqslant [\theta]$ is inert, then $h = 1$. Indeed, if $I \in \mathcal{N}$ then $N(I) = 1$, so I is the unit ideal, hence $h = 1$.

Denote by $N(\mathcal{N})$ the set of integers $N(I)$, where $I \in \mathcal{N}$.

In order to decide if the ideals $I, J \in \mathcal{N}$ are equivalent, it will be necessary to decide which integers $m \in N(\mathcal{N})$ are of the form $m = N(A\alpha)$.

Let $m \geqslant 1$, let

$$\alpha = \begin{cases} u + v\sqrt{d} & \text{when} \quad d \equiv 2 \text{ or } 3 \pmod 4, \quad \text{with} \quad u, v \in \mathbf{Z}\,, \\ \\ \dfrac{u + v\sqrt{d}}{2} & \text{when} \quad d \equiv 1 \pmod 4, \qquad \text{with} \quad u, v \in \mathbf{Z},\ u \equiv v \pmod 2\,. \end{cases}$$

Then: $A\alpha$ is a primitive ideal with $N(A\alpha) = m$ if and only if

$$\begin{cases} m = |\,u^2 - dv^2\,|\,, \ gcd\,(u, v) = 1 & \text{if} \quad d \equiv 2 \text{ or } 3 \pmod 4 \\ m = \dfrac{|\,u^2 - dv^2\,|}{4}, \ gcd\left(\dfrac{u-v}{2},\ v\right) = 1 & \text{if} \quad d \equiv 1 \pmod 4 \end{cases}$$

(this is called the primitive representation of m).

Proof. Let $d \equiv 2$ or $3 \pmod 4$, $m = N(A\alpha) = |u^2 - dv^2|$, also $gcd(u, v) = 1$, because $A\alpha$ is primitive.

Let $d \equiv 1 \pmod 4$, $m = N(A\alpha) = \dfrac{|u^2 - dv^2|}{4}$, also if p divides $\dfrac{u - v}{2}$ and p divides v then p divides $\alpha = \dfrac{u - v}{2} + v\left(\dfrac{1+\sqrt{d}}{2}\right)$, against the hypothesis.

Conversely, let $d \equiv 2$ or $3 \pmod 4$, so $N(A\alpha) = m$: if p divides $A\alpha$, since $\{1, \sqrt{d}\}$ is an integral basis then $p \mid u$, $p \mid v$, which is absurd.

Let $d \equiv 1 \pmod 4$, so $N(A\alpha) = m$; if p divides $A\alpha$, since

$$\alpha = \frac{u - v}{2} + v\left(\frac{1+\sqrt{d}}{2}\right) \quad \text{and} \quad \left\{1, \frac{1 + \sqrt{d}}{2}\right\}$$

is integral basis, then p divides $\dfrac{u - v}{2}$ and v, which is absurd. □

Calculation of the class number.

Let $d > 0$, so $\theta = \frac{1}{2}\sqrt{D}$.

$[\theta] = 1$.

Since $1 \leqslant \frac{1}{2}\sqrt{D} < 2$ then $4 \leqslant D < 16$, with $D \equiv 0$ or $1 \pmod 4$, hence $D \in \{4, 5, 8, 9, 12, 13\}$, and therefore $d \in \{5, 2, 3, 13\}$.

Now $N(\mathcal{N}) = \{1\}$, hence $\mathcal{N}$ consists only of the unit ideal, and therefore $h = 1$.

$[\theta] = 2$.

Since $2 \leqslant \frac{1}{2}\sqrt{D} < 3$ then $16 \leqslant D < 36$, with $D \equiv 0$ or $1 \pmod 4$, hence $D \in \{16, 17, 20, 21, 24, 25, 28, 29, 32, 33\}$ and therefore $d \in \{17, 21, 6, 7, 29, 33\}$.

Now $N(\mathcal{N}) = \{1, 2\}$.

Take, for example $d = 17$. Since $17 \equiv 1 \pmod 8$ then $A2 = P \cdot P'$, $N(P) = N(P') = 2$, $2 = \dfrac{|3^2 - 17 \times 1^2|}{4}$, $gcd\left(\dfrac{3-17}{2}, 17\right) = 1$, hence

$$P = A\alpha, \quad \alpha = \frac{3 + \sqrt{17}}{2},$$

$$P' = A\alpha', \quad \alpha' = \frac{3 - \sqrt{17}}{2}.$$

Therefore the class number is $h = 1$.

Let $d = 21$. Since $21 \equiv 5 \pmod 8$ then $A2$ is a prime ideal, 2 is inert, hence $h = 1$.

Let $d = 6$, then 2 divides $24 = D$, so 2 is ramified, $A2 = P^2$, and $2 = |2^2 - 6 \times 1^2|$, $gcd(2, 1) = 1$, hence $P = A\alpha$, with $\alpha = 2 + \sqrt{6}$. Therefore $h = 1$.

$[\theta] = 3$.

Since $3 \leqslant \frac{1}{2}\sqrt{D} < 4$ then $36 \leqslant D < 64$, with $D \equiv 0$ or $1 \pmod 4$, hence

$$D \in \{36, 37, 40, 41, 44, 45, 48, 49, 52, 53, 56, 57, 60, 61\}$$

and therefore

$$d \in \{37, 10, 41, 11, 53, 14, 57, 15, 61\}.$$

Now $N(\mathcal{N}) = \{1, 2, 3\}$.

Take, for example $d = 10$. Since 2 divides $40 = D$ then 2 is ramified, $A2 = R^2$. Since $\left(\frac{10}{3}\right) = \left(\frac{1}{3}\right) = 1$ then 3 is decomposed, $A3 = P.P'$. The ideals R, P, P' are primitive.

2 has no primitive representation: if $2 = |u^2 - 10v^2|$ then $u^2 = 10v^2 \pm 2 \equiv \pm 2 \pmod{10}$, which is impossible.

3 has no primitive representation: if $3 = |u^2 - 10v^2|$ then $u^2 = 10v^2 \pm 3 \equiv \pm 3 \pmod{10}$, which is impossible.

Thus, R, P, P' are not principal ideals. The ideals RP, RP' are primitive. Also

$$-2 \times 3 = -6 = 2^2 - 10 \times 1^2, \quad gcd(2, 1) = 1, \quad 2 \times 3 = N(RP) = N(RP'),$$

hence RP, RP' are principal ideals. In conclusion, $h = 2$.

Let $d < 0$, so $\theta = \frac{2}{\pi}\sqrt{-D}$.

$[\theta] = 1$.

Since $1 \leqslant \frac{2}{\pi}\sqrt{-D} < 2$ then $\frac{\pi^2}{4} \leqslant |D| < \pi^2$, and $|D| \equiv 0$ or $3 \pmod 4$, hence $|D| \in \{3, 4, 7, 8\}$, therefore $d \in \{-3, -1, -7, -2\}$. Now $N(\mathcal{N}) = 1$, hence $\mathcal{N}$ consists only of the unit ideal, so $h = 1$.

$[\theta] = 2$.

Since $2 \leqslant \frac{2}{\pi}\sqrt{-D} < 3$ then $\pi^2 \leqslant |D| < \frac{9}{4}\pi^2$, and $|D| \equiv 0$ or $3 \pmod 4$, hence $|D| \in \{11, 12, 15, 16, 19, 20\}$, therefore $d \in \{-11, -15, -19, -5\}$.

Take, for example, $d = -11$. Since $-11 \equiv 5 \pmod 8$ then 2 is inert, and therefore $h = 1$.

Let $d = -5$. Since 2 divides $D = -20$ so 2 is ramified, $A2 = P^2$.

2 has no primitive representation: if $2 = |u^2 + 5v^2|$ then $u^2 = -5v^2 + 2 \equiv 2 \pmod 5$, which is impossible. Also $-5 \equiv 3 \pmod 4$. So P is not principal and $h = 2$.

Let $d = -15$. Since $-15 \equiv 1 \pmod 8$ then $A2 = P \,.\, P'$.

2 has no primitive representation: if

$$2 = \frac{|u^2 + 15v^2|}{4}, \quad \text{with} \quad gcd\left(\frac{u-v}{2}, v\right) = 1,$$

then $u^2 + 15v^2 = 8$, so $u^2 \equiv 3 \pmod 5$, which is impossible. Also $-15 \equiv 1 \pmod 4$. Since P, P' are not principal ideals, then $h = 2$.

Let $d = -19$. Since $-19 \equiv 5 \pmod 8$ so 2 is inert, hence $h = 1$.

$[\theta] = 3$.

Since $3 \leqslant \frac{2}{\pi}\sqrt{-D} < 4$ then $\frac{9\pi^2}{4} \leqslant |D| < 4\pi^2$, and $|D| \equiv 0$ or $3 \pmod 4$, hence

$$|D| \in \{23, 24, 27, 28, 31, 32, 35, 36, 39\},$$

and therefore

$$d \in \{-23, -6, -31, -35, -39\}.$$

Take $d = -31$. Since $-31 \equiv 1 \pmod 8$ then $A2 = P \,.\, P'$. Since $\left(\frac{-31}{3}\right) = \left(\frac{-1}{3}\right)\left(\frac{1}{3}\right) = -1$, so $A3$ is a prime ideal.

2 has no primitive representation: if

$$2 = \frac{|u^2 + 31v^2|}{4}, \quad \text{with} \quad gcd\left(\frac{u-v}{2}, v\right) = 1,$$

then $8 = u^2 + 31v^2$, which is impossible. Since $-31 \equiv 1 \pmod 4$ then P, P' are not principal ideals. If P, P' are equivalent then $P = P' \,.\, A\alpha$ so $P^2 = P \,.\, P' \,.\, A\alpha = A(2\alpha)$, so $4 = N(P^2) = 4N(A\alpha)$, hence $N(A\alpha) = 1$, thus $A\alpha = A$, and $P = P'$, which is absurd. In conclusion, $h = 3$.

These examples are enough to illustrate how to compute the class number, at least for small values of the discriminant.

Determination of all quadratic fields with class number 1.

Let $d > 0$.

It is conjectured that there exist infinitely many $d > 0$ such that $\mathbf{Q}(\sqrt{d})$ has class number 1. This question is difficult to settle, but it is expected that the conjecture is true.

For example, there exist 142 fields $\mathbf{Q}(\sqrt{d})$, with $2 \leqslant d < 500$ having class number 1.

Let $d < 0$.

It was seen that if $\mathcal{N}$ consists only of the unit ideal, then $h = 1$. But conversely:

If $d < 0$ and $h = 1$ then $\mathcal{N} = \{A\}$.

Proof. If $|D| \leqslant 7$, it is true. Let $|D| > 7$, let $I \in \mathcal{N}$, $I \neq A$, so there exists a prime ideal P dividing I. Then $N(P) = p$ or p^2, where p is a prime number. If $N(P) = p^2$ then p is inert and $Ap = P$ divides I, so I would not be primitive, which is a contradiction. If $N(P) = p$, since P divides I then $p \leqslant N(I) \leqslant [\theta] \leqslant \frac{2}{\pi}\sqrt{|D|}$. If p has a primitive representation:

if $d \equiv 2$ or $3 \pmod 4$ then $d = \frac{D}{4}$, so $p = u^2 - dv^2$, hence $v \neq 0$, therefore $\frac{2}{\pi}\sqrt{|D|} \geqslant p \geqslant |d| = \frac{|D|}{4}$, so $7 \geqslant \frac{64}{\pi^2} \geqslant |D|$, which is absurd;

if $d \equiv 1 \pmod 4$ then $d = D$, so $p = \frac{u^2 - dv^2}{4}$, hence $v \neq 0$, therefore $\frac{2}{\pi}\sqrt{|D|} \geqslant p \geqslant \frac{|d|}{4} = \frac{|D|}{4}$, and again $7 \geqslant D$, which is absurd.

Therefore P is not a principal ideal and $h \neq 1$, which is against the hypothesis. □

Gauss developed a theory of genera and proved:

If $d < 0$ and if t is the number of distinct prime factors of D, then 2^{t-1} divides the class number of $\mathbf{Q}(\sqrt{d})$.

Hence if $h = 1$ then $D = -4$, -8 or $-p$, where p is a prime, $p \equiv 3 \pmod 4$, hence $d = -1$, -2 or $-p$.

From this discussion, it follows:

If $D = -3$, -4, -7, -8 then $h = 1$.
If $D \neq -3$, -4, -7, -8 and $D = -p$, $p \equiv 3 \pmod 4$ then $h = 1$ if and only if $\mathcal{N} = \{A\}$ and this is equivalent to the following conditions:

2 is inert in $\mathbf{Q}(\sqrt{-p})$, and if q is any odd prime, $q \leqslant [\theta]$, then $\left(\frac{-p}{q}\right) = -1$, i.e., q is inert in $\mathbf{Q}(\sqrt{-p})$.

This criterion is used in the determination of all $D < 0$, $|D| \leqslant 200$, such that $h = 1$.

$[\theta] = 1$. This gives the discriminants $D = -3, -4, -7, -8$.

$[\theta] = 2$. Now $-20 \leqslant D \leqslant -11$, with $D = -p$, $p \equiv 3 \pmod 4$, so $D = -11$ or -19.

Since $-11 \equiv 5 \pmod 8$ then 2 is inert, so if $D = -11$ then $h = 1$.

Similarly, since $-19 \equiv 5 \pmod 8$ then 2 is inert, so if $D = -19$ then $h = 1$.

$[\theta] = 3$. Now $-39 \leqslant D \leqslant -23$, with $D = -p$, $p \equiv 3 \pmod 4$, so $D = -23$ or -31. But $-23 \not\equiv 5 \pmod 8$, $-31 \not\equiv 5 \pmod 8$, so the class numbers of $\mathbf{Q}(\sqrt{-23})$ and of $\mathbf{Q}(\sqrt{-31})$ are not 1.

$[\theta] = 4$. Now $-59 \leqslant D \leqslant -40$, $D = -p$, $p \equiv 3 \pmod 4$, so $D = -43$, -47, -59. Since $-43 \equiv 5 \pmod 8$ and $\left(\frac{-43}{3}\right) = -1$ then $\mathbf{Q}(\sqrt{-43})$ has class number 1. Since $-47 \not\equiv 5 \pmod 8$ and $\left(\frac{-59}{3}\right) = 1$ then 3 is not inert. So the class numbers of $\mathbf{Q}(\sqrt{-47})$ and of $\mathbf{Q}(\sqrt{-59})$ are not equal to 1.

The same calculations yield:

$[\theta] = 5$: $D = -67$, with class number 1

$[\theta] = 6$: no discriminant

$[\theta] = 7$: no discriminant

$[\theta] = 8$: $D = -163$, with class number 1.

This process may continued beyond 200, but leads to no other discriminant for which the class number is 1. Of course, this does not allow to decide whether there exists any other such discriminant, nor to decide whether there are only finitely many imaginary quadratic fields with class number 1.

In a classical paper, Heilbronn and Linfoot showed in 1934, with analytical methods, that besides the above examples there exists at most another value of $d < 0$ for which $\mathbf{Q}(\sqrt{d})$ has class number 1. Lehmer showed that if such a discriminant d exists at all, then $|d| > 5 \times 10^9$. In 1952, Heegner proved that no other such d could exist, but his proof contained some steps which were unclear, perhaps even a gap. Baker reached

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.