Алгебра и анализ
Том 25 (2013), № 4

St. Petersburg Math. J.
Vol. 25 (2014), No. 4, Pages 699–711
S 1061-0022(2014)01312-X
Article electronically published on June 5, 2014

# ON THE PROBLEM OF THE 10TH DISCRIMINANT

I. R. SHAFAREVICH

Abstract. An elementary proof is given for Heegner's theorem describing imaginary quadratic fields with class number one.

## Introduction

Gauss proved (see [1, no. 174]) that the number $h(D)$ of equivalence classes of quadratic forms with discriminant $D$ is finite. This led to the natural question of how the misterious number $h(D)$ is expressed in terms of $D$, or at least how $h(D)$ grows as $D$ increases. Tables give a definite answer to this question (at least for positive $D$). Gauss mentioned this, but remarked that "the proof of these statements turned out to be very difficult" (see [1, no. 303]). From the current point of view, we deal with the growth of the class number $h$ of a field $K$ of a given degree over $\mathbb{Q}$ as the discriminant $D$ of the field increases. In the paper [2] C. L. Siegel predicted the relation

$$\frac{\log(hR)}{\log\sqrt{D}} \to 1 \quad \text{as} \quad D \to \infty, \tag{1}$$

where $h$ is the class number and $R$ is the regulator of $K$, but he wrote: "The application of class field theory can give relation (1) only for the fields solvable over a fixed field. The general case remains unproved as long as decomposition laws are unknown for unsolvable extensions".

However, in the book [3, p. 132–139], relation (1) (called there the Siegel–Brauer theorem) was proved with the help of a pure group-theoretic statement (called Brauer's lemma), without "decomposition laws for unsolvable extensions". So, there is some evidence against Siegel's prediction.

However, relation (1) says nothing about the growth of $h$ since we do not know how the regulator $R$ of the field changes. Only for imaginary quadratic fields, for which the regulator is 1, formula (1) implies the relation

$$\frac{\log h}{\log\sqrt{|D|}} \to 1$$

proved by Siegel in the paper [2].

It was not until 1934 that Heilbronn [4], using the results of Deuring [5], managed to prove the following statement seen from the tables presented by Gauss in "Disquesitiones" (no. 303): "the class number of an imaginary quadratic field grows unboundedly with the discriminant" [4] (note that Disquesitiones appeared in 1801!). In other words, for each constant $c$, there exists a constant $C$ such that $h > c$ whenever $|D| > C$. Unfortunately, these results are not efficient, i.e., they do not allow one to find the constant $C$ in terms of $c$. In the same 1934, Heilbronn and Linfoot [6] proved only that, for $h = 1$ (i.e., for $c = 1$), there exist at most 10 imaginary quadratic fields with class number one (the tables show that there are 9 such fields and all these fields have discriminants $D$ with $|D| < 200$).

2010 *Mathematics Subject Classification.* Primary 11R29.
*Key words and phrases.* Quadratic number fields, class numbers, modular functions.

Lemer even proved that if the "tenth discriminant" $D$ exists, then $|D| > 5 \cdot 10^8$. The problem of the existence of the "tenth discriminant" (for imaginary quadratic fields with class number one) was named the problem of the 10th discriminant. The present paper is also devoted to this problem.

In 1952, Heegner published the paper [7], in which he claimed that he had solved this problem. However, the exposition was unclear, and a long time (about 20 years) it was believed that his proof had gaps.

I am very glad that Deuring said in the paper [11]: "It must be admitted that it is hard to understand Heegner's reasoning". Because of this, Heegner's work had not been recognized by mathematicians, and it was believed that the first correct proof was given by Stark in the paper [8], which appeared 16 years after the work of Heegner. In his paper, Stark quoted Heegner but said about Heegner's work: Unfortunately, it is believed that this paper has a gap related, possibly, to the reference to the book of Weber."

In the same year, A.Baker published the paper [9] in which the nonefficiency of Helbronn's arguments mentioned above was eliminated. Baker's approach essentially differs from Heegner's but solves the same problem (see also [10]).

One year after the publication of Stark's result, Deuring [11] and Birch [12], following Heegner's ideas, found a complete proof of the theorem announced in Heegner's paper. In the present exposition, we follow the idea of Heegner with simplifications suggested by Deuring and Birch, and also by Eichler [15] (see Borel's talk), but the calculation showing that some functions are modular is replaced by geometric consideration of the corresponding Riemann surface. As a result, we obtain a proof of Heegner's theorem accessible to everyone who has mastered the basics of algebraic number theory (e.g., at the level of the book [13]). The subsequent exposition is based on the notes of the lectures given in Moscow State University in the 1970th. Thus, our goal in this paper is the proof of the following result.

**Theorem 1** (Heegner theorem). *The only imaginary quadratic fields with class number one are* $\mathbb{Q}(\sqrt{-d})$, *where* $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$.

Heegner's idea is to apply the theory of complex multiplication. The basics of this theory can be found in the book by Füeter [14] or in [15]. Heegner's idea is as follows: the theory of complex multiplication implies that, if $z$ is an algebraic integer belonging to an imaginary quadratic field $k$ and $z \notin \mathbb{Q}$, then the value of the modular function $j(z)$ is an algebraic integer belonging to the Hilbert class filed $K$ of $k$, where $(K : k) = h$. Consequently, if the field $k$ has class number one, then $j(\alpha) \in k$ for an integer $\alpha \in k$. It is easily seen that this number is real, i.e., $j(\alpha) \in \mathbb{Z}$. Heegner also constructed some other functions having the same property and related to each other by some algebraic relations. As a result, the class number one fields turn out to be in one-to-one correspondence with the integral points of a certain algebraic curve. The exact result is as follows: the class number one fields of the form $\mathbb{Q}(\sqrt{-d})$ with $d > 3$ correspond to the integral points of the curve $y^2 = 2x(1 - x^3)$ and are uniquely determined by the corresponding points. To find the integral points on this curve is an elementary problem.

The exposition is divided into three parts. In §1, we study the values of some modular functions of level $n$ at the points belonging to an imaginary quadratic field. In §2, we construct some special modular functions. In §3, we consider the values of these functions, which gives the solution of the problem on the tenth discriminant.

## §1. The values of modular functions of level $n$

Let $\Gamma$ be the modular group and $G \subset \Gamma$ a normal subgroup of finite index. Let $H = \{z, \operatorname{Im} z > 0\}$, and let $S = \mathbb{P}^1(\mathbb{Q})$ be the set of rational point of the boundary of $H$.

The space $\Gamma \setminus H$ is noncompact, but it can be compactified by embedding it in $\Gamma \setminus \bar{H}$, where $\bar{H} = H \cup S$, and extending the action of $\Gamma$ to $\bar{H}$. The space $\Gamma \setminus \bar{H}$ is already compact if we put a neighborhood of the point $\infty \in S$ equal to $\operatorname{Im} z > c$, $c \in \mathbb{R}$, and a neighborhood of a point $s \neq \infty \in S$ equal to the interior of the disk in $H$ tangent to the real axis $\operatorname{Im} z = 0$ at $s$. The space $\Gamma \setminus \bar{H}$ is denoted by $X_\Gamma$. Since $\Gamma \setminus S =$ (a point), the space $\Gamma \setminus H$ is compactified by adding one point. Since $G \setminus \bar{H} = \Gamma \setminus G \Big\backslash \Gamma \setminus \bar{H}$, we see that $G \setminus \bar{H}$ is compact. We can transfer the complex structure on $\Gamma \setminus H$ to $X_\Gamma$. For this, we introduce the local parameter $q_s$ equal to $q_\infty = e^{2\pi i z}$ for $s = \infty \in \mathbb{P}(Q)$ and $q_s = \gamma^*(q_\infty)$ for $s \neq \infty$, and a transformation $\gamma \in \Gamma$ such that $\gamma(\infty) = 1$. We call a function on $\bar{H} \setminus \Gamma$ meromorphic if it is meromorphic on $H$ and is representable by a series (in a neighborhood of a point $s \in S$) containing only a finite number of terms $q_s^{-n}$ with $n > 0$. The field of meromorphic functions on $G \setminus \bar{H}$ is denoted by $K_G$. The space $\Gamma \setminus \bar{H}$ is complex isomorphic to $\mathbb{P}^1(\mathbb{C})$. The function providing the isomorphism is denoted by $j(z)$ (as a function on $H$). This definition can be carried over to $G \setminus \bar{H}$ by the covering $G \setminus \bar{H} \to \Gamma \setminus \bar{H}$. The field of meromorphic functions on $G \setminus \bar{H}$ is denoted by $K_G$.

Let $\Gamma(n)$ be the principal congruence subgroup of level $n$, i.e., the set of transformations $\gamma \in F$ such that $\gamma(z) = \frac{az+b}{cz+d}$ and $A \equiv E \bmod n$, where $A$ is the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. The field $K_{\Gamma(n)}$ is denoted by $K_n$. This field has a subring $R_n$ consisting of all functions $f \in K_n$ such that 1) $f$ is regular at all points $z \in H$ and 2) the coefficients of the $q_s$-expansions of $f$ at the points $s \in S$ belong to the ring $\Sigma_n$ of integers of the field $\mathbb{Q}(\zeta_n)$, where $\zeta_n = e^{2\pi i/n}$.

We formulate a generalization of the main theorem of the classical theory of complex multiplication.

**Theorem 2.** *Let $\alpha$ be an algebraic integer belonging to an imaginary quadratic field $k$, and let $\alpha \notin \mathbb{Q}$. If $f \in R_n$, then $f(\alpha)$ is contained in the class field of $k$ with conductor $n$.*

Let $p$ be a prime, $p \equiv 1 \bmod n$. We denote by $M_p(n)$ the set of all $(2 \times 2)$-matrices $A$ over $\mathbb{Z}$ such that $\det A = p$ and $A \equiv E \bmod n$. The group $\Gamma(n)$ acts on this set. The inclusion $M_p(n) \hookrightarrow M_p$ ($M_p = M_p(1)$) gives rise to the mapping $\varphi : \Gamma(n) \setminus M_p(n) \to \Gamma \setminus M_p$. We check that $\varphi$ is one-to-one. If $a, b \in M(n)$ and $a = b\gamma$ for a $\gamma \in \Gamma$, then $\gamma \equiv e \bmod n$, i.e., $\gamma \in \Gamma(n)$, and, therefore, $\varphi$ is an embedding. If $A \in M_p$, then $A \bmod n \in \mathrm{SL}(2, \mathbb{Z}/n)$. It can easily be verified that this homomorphism is surjective (e.g., by decomposing the elements of $\mathrm{SL}(2, \mathbb{Z}/n)$ into elementary matrices). Therefore, $A \equiv \gamma \bmod n$ for a $\gamma \in \Gamma$ and $A\gamma^{-1} \in M_p(n)$. Consequently, $\varphi$ is surjective.

Let $G$ be a group acting on a set $X$, let $Y \subset X$, and let $H$ be a subgroup of $G$. Assume that the following conditions are fulfilled:

- (1) if $y_1, y_2 \in Y$ and $g(y_2) = y_1$ for $g \in G$, then $g \in H$;
- (2) $GY$ (i.e., the set of all $x \in X$ of the form $g(y)$ for $g \in G, y \in Y$)$= X$.

Then, by restriction, the embedding $Y \to X$ gives rise to a map

$$\varphi : G \setminus X \to H \setminus Y.$$

We claim that $\varphi$ is one-to-one. Since $GY = X$, every $x \in X$ has the form $g(y)$. We put $\varphi(Gx) = Hy$. By condition (1), the class $Hy$ is uniquely determined by the class $Gx$. Let $x_1, x_2 \in X$ and $\varphi(x_1) = \varphi(x_2)$. Then $x_1 = g(y_1)$, $x_2 = g(y_2)$, $y_2 = h(y_1)$, $h \in H$, which, in its turn, means that $Gx_2 = Gx_1$. We apply this to the case where $X = M_p$, $G = \Gamma$, $Y = M_p(n)$, and $H = \Gamma(n)$. We have already proved properties (1) and (2).

Using the map $\varphi$, we can easily find that the number of elements in $\Gamma(n) \setminus M_p(n)$ is equal to $p + 1$ and find a system of represenatives of the classes; for example, if $n = 1$,

we have:

$$\begin{cases} P_a = \begin{pmatrix} 1 & a \\ 0 & p \end{pmatrix} a \bmod p, \\ P_\infty = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}. \end{cases} \tag{2}$$

If $f \in R_n$ and $g \in M_p(n)$, then the function $f_g(z) = f(gz)$ depends only on the class $\Gamma(n)g$. We denote the function $f_g$, $g \in \alpha \subset \Gamma(n) \setminus M(n)$, by $f_\alpha$ and consider the polynomial

$$G_f(T) = \prod_{\alpha \in \Gamma_p(n) \setminus M_p(n)} (T - f_\alpha).$$

**Lemma 1.** $G_f(T) \in R_n[T]$.

Let $\gamma \in \Gamma(n)$, and let $G_f^\gamma(T)$ be the polynomial obtained by applying the transformation $\gamma$ to all coefficients of $G_f$. Since $f_\alpha(\gamma z) = f_{\alpha\gamma}(z)$ and $\Gamma(n)$ acts by permutations on the set $\Gamma(n)\setminus M(n)$, we have $G_f^\gamma(T) = G_f(T)$. To prove that the coefficients of $G_f$ belong to $R_n$, it remains to show that the coefficients of their $q_s$-expansions at the vertices $s \in S$ belong to $\Sigma_n \subset \mathbb{Q}(\zeta_n)$.

We consider the case where $s = \infty$, $q_s = e^{2\pi i z/n}$. Using the system of representatives (2), we obtain $f_a(z) = f\left(\frac{z+na}{p}\right)$ and $f_\infty(z) = f(pz)$. If $f = u(q_s)$, then $f_a = u\left(q_s^{1/p}\varepsilon^a\right)$, $\varepsilon = e^{2\pi i z/p}$, and $f_\infty = u\left(q_s^p\right)$. Therefore, the coefficients of the polynomial $G_f$ can be expanded in powers of $e^{2\pi i z/np}$ with finite number of negative terms. But these functions are invariant under the action of $\Gamma(n)$ and, in particular, under the action of the transformation $z \to z + n$. Consequently, they have series expansions in powers of $e^{2\pi i z/n}$, and from the above it follows that these series have a finite number of negative terms. It remains to prove that the coefficients of these series lie in the ring $\Sigma_n$. By definition, they are integers of the field $\mathbb{Q}(\zeta_{np})$, and it suffices to prove that they are contained in $\mathbb{Q}(\zeta_n)$. For every residue $c \bmod p$, the permutations $f_a \to f_{ea}$, $f_\infty \to f_\infty$ can be expressed in terms of power series as $u\left(q_s^{1/p}\varepsilon^a\right) \to u\left(q_s^{1/p}\varepsilon^{ca}\right)$, i.e., as the authomorphism $\varepsilon \to \varepsilon^c$ of the field $\mathbb{Q}(\zeta_n, \varepsilon)/\mathbb{Q}(\zeta_n)$. Therefore, the coefficients appearing in the Loran expansions of the coefficients of the polynomial $G_f$ are invariant under these authomorphisms, and, consequently, belong to $\mathbb{Q}(\zeta_n)$.

Now, we consider an arbitrary vertex $s \in S$. Instead of the system of representatives (1), we consider the system $P'_a = \gamma^{-1}P_a\gamma$, where the $P_a$ are taken from (1), $\gamma \in \Gamma$, and $\gamma\infty = s$. Then $q_s(P'_a z) = q_\infty(\gamma\gamma^{-1}P_a\gamma z) = q_\infty(P_a\gamma z)$. Therefore, $q_s(P'_a z) = q_s^{1/p}\varepsilon^a$ and $q_s(P'_\infty z) = q_s^p$, and all previous arguments remain valid. The lemma is proved.

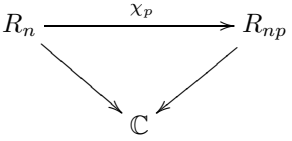
**Lemma 2.** *If $f \in R_n$, $\alpha \in k = \mathbb{Q}\left(\sqrt{-d}\right)$, $d > 0$, and $\alpha \notin \mathbb{Q}$, then $f(\alpha)$ is an algebraic number.*

Let $\alpha = \lambda/\mu$ be the quotient of two integers of the field $k$, and let $\pi$ be a prime in $k$ of order 1, $\pi \equiv 1 \bmod n$, $p = N\pi$. The numbers $\pi\lambda$ and $\pi\mu$ can be expressed in terms of $\lambda$ and $\mu$ by means of the matrix $M_p(n)$. Consequently, there is $P \in M_p(n)$ such that $P(\alpha) = \alpha$. Hence, for each function $f \in R_n$, we have $f(P(\alpha)) = f(\alpha)$.

The ring $R_n$ is of finite type over $\mathbb{Z}$. Indeed, $R_n$ is invariant under $\Gamma/\Gamma(n)$. The elementary symmetric functions of the elements $f^\sigma$, where $\sigma \in \Gamma/\Gamma(n)$ and $f \in R_n$, are contained in $R_1[\zeta_n]$. Therefore, $R_n$ is integral over $R_1[\zeta_n]$, and the latter is isomorphic to $\Sigma_n[j]$. It follows that $R_n$ is of finite type and has transcendence degree 1. As we saw in the proof of Lemma 1, the map $f(z) \to f(P(z))$ gives rise to a homomorphism

$$\chi_p : R_n \to R_{np}.$$

The map $f \to f(\alpha)$ yields homomorphisms $R_n \to \mathbb{C}$ and $R_{np} \to \mathbb{C}$, and we have seen that there is $P \in M_p(n)$ such that the diagram

(3)



is commutative.

If at least one of the values $f(\alpha)$, where $f \in R_n$, is transcendent, then the homomorphisms $R_n \to \mathbb{C}$ and $R_{np} \to \mathbb{C}$ do not decrease the transcendence degree over $\mathbb{Q}$ and, therefore, are isomorphisms. However, in this case diagram (3) shows that $\chi_p$ is the identity map. It remains to prove that this is not the case. Indeed, $\chi_p f = f$ means that $f(P(z)) = f(z)$ identically. In particular, $j(P(z)) = j(z)$, i.e., there is $\gamma \in \Gamma$ such that $P(z) = \gamma(z)$, $\gamma^{-1}P(z) = z$. Now it suffices to choose $z$ distinct from the fixed points of the transformations $g \in M_p$ to make the last identity invalid.

**Lemma 3.** *The following congruence is valid in the ring* $R_n[T]$:

$$G_f(T) \equiv \big(T^p - f\big)\big(T - f^p\big) \bmod p. \tag{4}$$

Obviously, it suffices to prove that the above congruence is valid if we replace $f$ by its $q_s$-expansion at a vertex $s \in S$. We check this for $s = \infty$. The general case is obtained as in the proof of Lemma 1.

Let $s = \infty$. Then

$$G_f(T) = (T - f_\infty)\prod_a (T - f_a),$$
$$f_\infty(z) = f(pz), \quad f_a(z) = f(P_a(z)),$$

where the $P_a$ are the matrices occurring (2). If $f = u(q_s)$, then $f_\infty(z) = u(q_s^p) \equiv (u(q_s))^p \bmod p$. This follows from the fact that $p \equiv 1 \bmod n$, and, therefore, $\xi^p \equiv \xi \bmod p$ for $\xi \in \Sigma_n$. Similarly,

$$f_a(z) = u\big(q_s^{1/p}\varepsilon^a\big) \equiv u\big(q_s^{1/p}\big) \bmod (1 - \varepsilon)$$

and

$$\prod (T - f_a) \equiv T^p - u(q_s) \bmod (1 - \varepsilon).$$

Thus,

$$\prod (T - f_\alpha) \equiv (T - u^p)(T^p - u) \bmod (1 - \varepsilon).$$

Since, on the other hand, the coefficients of all these series are contained in $\mathbb{Q}(\zeta_n)$ and $(1 - \varepsilon) \cap \Sigma_n = (p)$, we obtain the congruence (4).

*Proof of the theorem.* Let $\pi \equiv 1 \bmod n$ be a prime of degree 1 in $\Sigma_n$, let $\alpha \in k$, and let $P \in M_p(n)$ be a transformation such that $P(\alpha) = \alpha$. Then $G_f(Pf) = 0$. We replace all the functions by thier values at $\alpha$. By Lemma 2, we obtain a homomorphism of the ring $R_{np}$ to the field of all algebraic integers. By Lemma 3, we have the relation

$$\big(f(\alpha)^p - f(\alpha)\big)^e \equiv 0 \bmod p.$$

It follows that, for each prime divisor $\mathfrak{p}$ of $p$ in the field $k(f(\alpha))$, we have $f(\alpha)^p \equiv f(\alpha) \bmod \mathfrak{p}$ (if we exclude a finite number of primes dividing the denominators of the numbers $f(\alpha)$). Therefore, almost all prime divisors of degree 1 that split completely in the class field $k_n$ with conductor $n$ split completely in the field $k(f(\alpha))$. It is well known (see [3, Chapter V, §3, Theorem 2]) that this implies the relation $k(f(\alpha)) \subset k_n$. The theorem is proved. □

*Remark* 1. Since we can change arbitrarily a finite set of divisors in the proof of the theorem, the requirement $f \in R_n$ can be relaxed. Namely, it suffices to require that the coefficients of the $q_s$-expansions of $f$ be elements of the field $\mathbb{Q}(\zeta_n)$ the denominators of which are divisible only by primes from a prescribed finite set $S$ of prime divisors of this field.

*Remark* 2. A more accurate calculation of the coefficients of the $q$-expansion of $j$ makes it possible to prove similarly that the values $j(\alpha)$ are algebraic integers. See [15], Serre's talk.

## §2. Some special subgroups of the modular group

a) Consider the group $\Gamma_0(2)$ (as usual, $\Gamma_0 = \left\{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)\right\}$ and $\Gamma_0(n) = \Gamma_0 \cap \Gamma(n)$). We need explicit equations for the field corresponding to this subgroup. We consider the functions

$$e_\alpha(\omega_1, \omega_2) = \wp\Big(\frac{a_1\omega_1 + a_2\omega_2}{2}, \omega_1, \omega_2\Big), \quad a_1, a_2 \in \mathbb{Z},$$

where $a_1$ and $a_2$ are not even simultaneously. These functions depend only on $a_i$ mod 2 and, therefore, there exist three such $e_\alpha$ with $\alpha = (1,0)$, $(0,1)$, and $(1,1)$. We index them by $1, 2$, and 3, respectively. The function

$$\lambda = \frac{e_1 - e_2}{e_1 - e_3}$$

depends only on $\frac{\omega_1}{\omega_2}$, and it is easy to prove that $\lambda$ is a modular function of level 2. Under the transformations $\gamma \in \Gamma$, the functions $e_i$ undergo all possible permutations, because $(\Gamma : \Gamma(2)) = |S_3| = 6$. The function $\lambda$ transforms to the following six distinct functions:

$$\lambda,\ 1-\lambda,\ 1/\lambda,\ 1-1/\lambda,\ 1/(1-\lambda),\ \lambda/(\lambda-1).$$

Hence $K_1(\lambda) = K_2$. There is a subfield in $K_2/K_1$ corresponding to $\Gamma_0(2)$. Since $(\Gamma_0(2) : \Gamma(2)) = 2$, we see that this subfield corresponds to a subgroup of order 2 in $\mathrm{Gal}(K_1(\lambda)/K_1)$. Changing, if necessary, the numeration of $e_i$, we may assume that this subgroup is generated by the authomorphism $\lambda \mapsto 1 - \lambda$. Then our subfield is generated by the function $\mu = \lambda(1-\lambda)$.

Since $(\Gamma : \Gamma_0(2)) = 3$, we have $[K_1(\mu) : K_1] = 3$, and $\mu$ satisfies a third degree equation over $K_1 = \mathbb{C}(j)$.

To find this equation, we use the fact that $e = e_1, e_2$, and $e_3$ are the roots of the equation

$$4e^3 - g_2 e - g_3 = 0.$$

By direct calculation, we obtain

$$\mu = \lambda(1-\lambda) = \frac{(e_1-e_2)(e_2-e_3)}{(e_3-e_1)^2} = \frac{(e_1-e_2)(e_2-e_3)(e_3-e_1)}{(e_3-e_1)^3},$$

$$\mu^2 = \frac{(e_1-e_2)^2(e_2-e_3)^2(e_3-e_1)^2}{(e_3-e_1)^6} = \frac{-4(-g_2/4)^3 - 27(-g_3/4)^2}{(e_3-e_1)^6} = \frac{g_2^3 - 27g_3^2}{4^2(e_3-e_1)^6},$$

$$\mu - 1 = \frac{(e_1-e_2)(e_2-e_3) - (e_3-e_1)^2}{(e_3-e_1)^2} = \frac{e_1e_2 - e_1e_3 - e_2^2 + e_2e_3 - e_3^2 + 2e_1e_3 - e_1^2}{(e_3-e_1)^2}$$

$$= \frac{e_1e_2 + e_1e_3 + e_2e_3 - e_1^2 - e_2^2 - e_3^2}{(e_3-e_1)^2} = \frac{3(e_1e_2 + e_1e_3 + e_2e_3)}{(e_3-e_1)^2} = -\frac{3g_2}{4(e_3-e_1)^2},$$

$$(e_1 + e_2 + e_3 = 0!),$$

$$(\mu-1)^3 = -\frac{27g_2^3}{4^3(e_3-e_1)^6}, \quad \frac{(\mu-1)^3}{\mu^2} = -\frac{3^3g_2^3}{4(g_2^3 - 27g_3^2)} = -\frac{1}{4^4}j, \quad \Big(j = \frac{4^3 3^3 g_2^3}{g_2^3 - 27g_3^2}\Big),$$

$$(\mu-1)^3=-\frac{1}{4^4}j\mu^2,\quad (\mu_1-1)^3=-\frac{1}{4^4}j\mu_1,\quad \mu_1=\frac{1}{\mu},\quad u=4^2\mu_1,$$

$$(u-4^2)^3=ju. \tag{5}$$

This is the required equation. Since the field corresponding to the group $\Gamma_0(2)$ has the form $\mathbb{C}(j,u)$, we see by (5) that this field is generated by a single function $u$.

b) $G$ is a subgroup of $\Gamma$ such that $G\supset\Gamma(3)$ and $(\Gamma:G)=3$. The group $\Gamma/\Gamma(3)\simeq \mathrm{PSL}(1,\mathbb{F}_3)$ can be regarded as the transformation group of $\mathbb{P}^1(\mathbb{F}_3)$. We recall that $|\mathrm{PGL}(1,\mathbb{F}_3)|=24$ and $|\mathrm{PSL}(1,\mathbb{F}_3)|=12$. Hence, the transformations in $\mathrm{PGL}(1,\mathbb{F}_3)$ induce on $\mathbb{P}^1(\mathbb{F}_3)$ all permutations in $S_4$. It is easily seen that $\mathrm{PSL}(1,\mathbb{F}_3)$ yields even permutations, and thus $\mathrm{PSL}(1,\mathbb{F}_3)\simeq A_4$. The group $A_4$ has a normal subgroup of index 3 and order 4 that consists of the permutations (1), (12)(34), (13)(24), and (14)(23). The corresponding normal subgroup of $\mathrm{PSL}(1,\mathbb{F}_3)$ contains the transformation $x\mapsto -1/x$ and all conjugate transformations. We denote the corresponding normal subgroup of index 3 in $\Gamma$ by $G$. Then $K\subset K_G\subset K_3$ and $[K_3:K]=3$. It is obvious that $K_G=K\big(\sqrt[3]{f}\big)$ for some $f\in K$. We must find $f$. The Riemann surface $X_G$ is a three-fold covering of $X=X_1$. The ramification points of the covering $X_G\to X_1$ correspond to the fixed points of $\Gamma/G$ on $X_G$. In other words, they are the classes of $G$-equivalent points on $\bar H$ fixed under the transformations $\gamma\in\Gamma$ such that $\gamma\notin G$. However, only automorphisms of order two and three and automorphisms in parabolic subgroups have fixed points on $\bar H$. The group $G$ contains an automorphism of order 2 since $(\Gamma:G)=3$. Thus, the covering $X_G\to X$ has only two ramification points: $\rho$, where $\rho^3=1$, and $\infty$. The function $j$ gives rise to a map from $X_1$ to $\mathbb{P}^1(\mathbb{C})$ that takes $\rho$ to 0 and $\infty$ to $\infty$. Indeed, $j=\frac{4^3 3^3 g_2^3}{g_2^3-27g_3^2}$ and $g_2=\sum'_\alpha \frac{1}{\alpha^4}$, where $\alpha$ runs through the nonzero points of a lattice $\mathcal{O}$ such that $\rho\mathcal{O}=\mathcal{O}$. This means that $g_2=\sum'_\alpha\frac{1}{(\rho\alpha)^4}=\rho^{-4}g_2$ and $g_2=j=0$. Thus, $X_G\to X_1$ has two ramification points, 0 and $\infty$, and, therefore, $K_G=K_1(\sqrt[3]{j})=\mathbb{C}(\sqrt[3]{j})$. Consequently, $\sqrt[3]{j}$ is a modular function of level 3. We denote this function by $\gamma$.

**N. B.** It is well known that $\Gamma$ is a free product of a group of order 2 and a group of order 3 (see [16, §43]). Therefore, $\Gamma/(\Gamma,\Gamma)\simeq\mathbb{Z}/2\times\mathbb{Z}/3$. It follows that there exist modular functions $\varphi$ and $\psi$ such that $\sqrt{\varphi}$ and $\sqrt[3]{\psi}$ belong, respectively, to normal subgroups of index 2 and 3 in $\Gamma$. We have proved that $\psi=j$, It can be proved that $\varphi=j-4^3\cdot 3^3$.

c) Schläfli modular functions. We consider congruence subgroups $G\subset\Gamma_0(2)$ of levels $2^k$ with Abelian factors. In other words, $\Gamma_0(2)\supset G\supset\Gamma\big(2^k\big)$ for some $k$, and $\Gamma_0(2)/G$ is Abelian. To find them, it suffices to consider the quotient group of $F=\Gamma_0(2)/\Gamma(2^k)$ by its commutator subgroup for sufficiently large $k$. The elements of $F$ can be written in the matrix form

$$\begin{pmatrix}a & b\\ 2c & d\end{pmatrix},\quad ad-2bc=1,\ \ a,b,c,d\in\mathbb{Z}/2^k. \tag{6}$$

It is easy to describe the structure of $F$, by using the fact that, under condition (6), we have $a\equiv 1 \bmod 2$, $a^{-1}\in\mathbb{Z}/2^k$, and

$$\begin{pmatrix}a & b\\ 2c & d\end{pmatrix}=\begin{pmatrix}1 & 0\\ 2c/a & 1\end{pmatrix}\begin{pmatrix}a & 0\\ 0 & 1/a\end{pmatrix}\begin{pmatrix}1 & b/a\\ 0 & 1\end{pmatrix}.$$

We put $S_\alpha=\left(\begin{smallmatrix}1 & 0\\ 2\alpha & 1\end{smallmatrix}\right)$, $T_\beta=\left(\begin{smallmatrix}1 & \beta\\ 0 & 1\end{smallmatrix}\right)$, and $U_\gamma=\left(\begin{smallmatrix}\gamma & 0\\ 0 & \gamma^{-1}\end{smallmatrix}\right)$, where $2\alpha,\beta\in\mathbb{Z}/2^k$, and $\gamma\in(\mathbb{Z}/2^k)^*$. Each element $f\in F$ can be represented uniquely in the form $f=S_\alpha U_\gamma T_\beta$, and the multiplication in $F$ will be given if we describe how to represent the product of two

such elements in the same form. This is determined by the relations

$$\begin{aligned} U_\gamma S_\alpha U_\gamma^{-1} = S_{\gamma^{-2}\alpha}, \quad U_\gamma T_\beta U_\gamma^{-1} = T_{\gamma^2\beta}, \\ T_\beta S_\alpha = S_{\alpha/1+2\alpha\beta} U_{1/1+2\alpha\beta} T_{\beta/1+2\alpha\beta}, \end{aligned} \tag{7}$$

which can be checked directly.

Thus, formulas (7) are defining relations for the group $F$ generated by the subgroups $\{S_\alpha, 2\alpha \in 2\mathbb{Z}/2^k\}$, $\{T_\beta, \beta \in \mathbb{Z}/2^k\}$, and $\{U_\gamma, \gamma \in (\mathbb{Z}/2^k)^*\}$.

We consider the group $F/(F,F)$, where, as usual, $(F,F)$ is the commutator subgroup of $F$.

**Lemma 4.** *The group $F/(F,F)$ is generated by the images $s$ and $t$ of the matrices $S_1$ and $T_1$, respectively. For $k > 3$, the defining relations of this group have the form $s^8 = t^8 = 1$, $(st^{-1})^4 = 1$.*

We denote the images of the elements $S_\alpha$, $T_\beta$, and $U_\gamma$ in $F/(F,F)$ by $s_\alpha$, $t_\beta$, and $u_\gamma$, respectively. Relations (7) yield the following defining relations for the group $F/(F,F)$:

$$s_\alpha s_{\alpha'} = s_{\alpha+\alpha'}, \quad t_\beta t_{\beta'} = t_{\beta+\beta'}, \quad u_\gamma u_{\gamma'} = u_{\gamma\gamma'},$$

$$s_{(1-\gamma^{-2})\alpha} = 1, \quad t_{(1-\gamma^2)\beta} = 1, \tag{8}$$

$$(s_\alpha t_\beta)^{2\alpha\beta} = u_{1/1+2\alpha\beta}^{1+2\alpha\beta}. \tag{9}$$

Equation (8) implies that $s_\alpha = t_\alpha = 1$ for $\alpha \equiv 0 \bmod 8$. In what follows, we shall assume that $\alpha, \beta \in \mathbb{Z}/8$. Putting $\alpha = 2$ and $\beta \equiv 0(2)$ in (9), we deduce that $u_\gamma^2 = 1$ if $\gamma \equiv 1 \bmod 8$.

Thus, the group $F/(F,F)$ is finite and has quite simple defining relations. The elements $u_\gamma$ can take four distinct values 1, $u_3$, $u_7$, and $u_5$, and formulas (8) and (9) yield the following complete system of defining relations for $F/(F,F)$:

$$\begin{aligned} s^2t^2 = u_3, \\ s^2t^{-2} = u_7, \quad u_3^2 = u_7^2 = u_5^2 = 1, \\ s^4 = u_5, \quad u_3u_7 = u_5, \end{aligned}$$

where $s = s_1$ and $t = t_1$. It follows that the group $F/(F,F)$ is generated by the elements $s$ and $t$ satisfying $s^8 = t^8 = 1$ and $(st^{-1})^4 = 1$. The lemma is proved.

We denote by $G$ the preimage of the subgroup $\{st^{-1}\} \subset F/(F,F)$ in $\Gamma_0(2)$. By Lemma 4, we have $\Gamma_0(2)/G \simeq \mathbb{Z}/8$. Let $K_2^0$ be the field of modular functions with respect to $\Gamma_0(2)$. Then $[K_G : K_2^0] = 8$ and $K_G = K_2^0\big(\sqrt[8]{h}\big)$. By Example a), we have $K_2^0 = \mathbb{C}(\mu)$, and so $h$ is a rational function of $\mu$. Let us find this function. Arguing as in Example b), we see that the ramification points of the covering $X_G \to X_{\Gamma_0(2)}$ correspond to the classes of $G$-equivalent points $z \in \bar{H}$ that contain fixed points of the automorphisms $\gamma \in \Gamma_0(2)$, $\gamma \notin G$. Again we must consider the automorphisms of orders 2 and 3 and the automorphisms in parabolic groups. If $\gamma \in \Gamma_0(2)$ and $\gamma^3 = 1$, then $\gamma \in G$ because $(\Gamma_0(2) : G) = 8$. The automorphisms of order 2 are conjugate in $\Gamma$. One of them is given by the matrix $\left(\begin{smallmatrix} 1 & -1 \\ 2 & -1 \end{smallmatrix}\right)$ and is contained in $\Gamma_0(2)$. This automorphism is the image of the element $S_1T_1^{-1}$ under the homomorphism $\mathrm{SL}(2,\mathbb{Z}) \to \Gamma$. It can be checked that an automorphism in $\Gamma_0(2)$ conjugate to the above automorphism in $\Gamma$ is also conjugate to this automorphism in $\Gamma_0(2)$. Since $S_1T_1^{-1} \in G$, we see that there are no corresponding ramification points.

It remains to consider the ramification points belonging to $S$. They correspond to the elements of the set $\Gamma/\Gamma_0(2)$, i.e., $\mathbb{P}^1(\mathbb{F}_2)$. The group $\Gamma_0(2)$ acts on the ramification points by translations, and, therefore, the two finite points in $\mathbb{P}^1(\mathbb{F}_2)$ are equivalent, but $\infty$ is

not equivalent to them. These two points are unique ramification points of the covering $X_G \to X_{\Gamma_0(2)}$, i.e., they are the zeros and poles of the function $h$.

The preimages of the point $j = \infty$ under the covering $X_{\Gamma_0(2)} \to X_\Gamma$ are the points $\mu = \infty$ and $\mu = 0$. This is seen from (4). Thus, the ramification points of $X_G \to X_{\Gamma_0(2)}$ correspond to the values $\mu = \infty$ and $\mu = 0$. This shows that $\mu = h$, and, therefore, the function $\sqrt[8]{u} = f$ is also a modular function of level 16. This function is called Schläfli's modular function.

*Remark* 1. Using the undetermined coefficients method, we can easily prove that the functions $\sqrt[3]{j}$, $u$, and $f = \sqrt[8]{u}$ have $q_s$-expansions with coefficients belonging, respectively, to the fields $\mathbb{Q}(\zeta_3)$, $\mathbb{Q}$, and $\mathbb{Q}(\zeta_8)$. This is not immediately obvious only for the function $u$. However, the extension $\mathbb{Q}(u)/\mathbb{Q}(j)$ has degree 3, and there are two points, $u = 0$ and $u = \infty$, over $j = \infty$ having ramification indices 1 and 2, respectively. It follows that the inertia degrees of these points are equal to 1, i.e., the coefficients of the $q_s$-expansions lie in $\mathbb{Q}$.

Eisenstein's theorem implies that the denominators of the coefficients of all $q_s$-expansions of these functions are divisible only by primes from a certain finite set. Theorem 2 shows that, for $\alpha \in k$ such that $\alpha \notin \mathbb{Q}$, the field $k$ is an imaginary quadratic field with class number one, $\sqrt[3]{j(\alpha)} \in k_3$, $u(\alpha) \in k_2$, and $f(\alpha) \in k_{16}$.

*Remark* 2. In what follows, $k_n$ is regarded as a class field with conductor $n$ (but not as a function of level $n$). The extension $k_n/\mathbb{Q}$ is Galois and coincides with the composite $kk_n^0$, where $k_n^0$ is the maximal real subfield of $k_n$. The functions $\sqrt[3]{j}$, $u$, and $f$ can be normalized so that their values at the points $\alpha \in k$ be real, i.e., lie in $k_n^0$. For this, we must use the fact that the $q$-expansions of $j$,

$$j = \frac{1}{q} + \sum c_n q^n,$$

have real (even integral) coefficients. Therefore, if $z = \frac{1}{2} + it$, then $q$, and, consequently, also $j(z)$ is real. Since $q < 0$, we see that if $t$ is sufficiently large, then $|q|$ is sufficiently small to make $j(z)$ negative. Since $j\big(\frac{1}{2} + i\frac{\sqrt{3}}{2}\big) = 0$ and the ray $\frac{1}{2} + it$ with $t > \frac{\sqrt{3}}{2}$ lies in the fundamental region of the group $\Gamma$, we see that $j(z) \neq 0$ on this ray, so that $j(z)$ is negative. We choose the branch of the function $\gamma = \sqrt[3]{j}$ for which $\gamma\big(\frac{1}{2} + it\big) < 0$ if $t > \frac{\sqrt{3}}{2}$.

If $j < 0$, then the equation $(u - 16)^3 = ju$ has a unique real root, which is positive. We denote it by $u$, i.e., we define $u$ by the condition that $u\big(\frac{1}{2} + it\big)$ is real and $u > 0$ for $t > \frac{\sqrt{3}}{2}$. Similarly, we define $f$ by the condition $f\big(\frac{1}{2} + it\big) > 0$ for $t > \frac{\sqrt{3}}{2}$.

Under the above normalizations, the values of the functions $\gamma$, $u$, and $f$ at the points $\alpha \in k$ are real and lie in the corresponding fields $k_n^0$.

## §3. List of fields with class number one

We begin with some obvious simplifications of the problem. If an imaginary quadratic field $k$ has class number one and its discriminant is not divisible by 2, then $k = \mathbb{Q}\big(\sqrt{-1}\big)$ or $k = \mathbb{Q}\big(\sqrt{-2}\big)$. Indeed, in this case the field $k$ has integral basis of the form 1, $\sqrt{-d}$. Since 2 does not divide the discriminant, we see that $(2) = \mathfrak{p}^2$ and $N\mathfrak{p} = 2$. Since $k$ has class number one, we have $\mathfrak{p} = (\pi) = \big(x + y\sqrt{-d}\big)$ and $x^2 + dy^2 = 2$. The latter equation has integral solution only if $d$ is 1 or 2.

Thus, except for these two cases, we have $k = \mathbb{Q}\big(\sqrt{-d}\big)$, where $d \equiv 3 \bmod 4$, and the integral basis of the field $k$ has the form 1, $\omega$, where $\omega = \frac{1+\sqrt{-d}}{2}$. If $d \equiv 7 \bmod 8$, then 2 splits into two prime factors in $k$, and again we have the relation $2 = N(x + y\omega) =$

$\left(x+\frac{y}{2}\right)^2+\frac{dy^2}{4}$. If $d>7$, then this equation has no integral solutions. It follows that for $d\neq 7$ we may assume that $d\equiv 3 \bmod 8$.

Finally, we note that the discriminant of a field with class number one must be prime. If $d=d'd''$ and $d\equiv 3 \bmod 4$, then $d'\equiv 3 \bmod 4$ and $d''\equiv 1 \bmod 4$, and it is easy to show that the extension $\mathbb{Q}\left(\sqrt{-d'},\sqrt{-d''}\right)/\mathbb{Q}\left(\sqrt{-d}\right)$ is unramified, which, by class field theory, contradicts the fact that the field $k$ has class number one.

Thus, removing the three fields $\mathbb{Q}\left(\sqrt{-1}\right)$, $\mathbb{Q}\left(\sqrt{-2}\right)$, and $\mathbb{Q}\left(\sqrt{-7}\right)$ from consideration, we may assume that $k=\mathbb{Q}\left(\sqrt{-p}\right)$, where $p$ is a prime such that $p\equiv 3 \bmod 8$. In what follows, all these conditions are assumed to be fulfilled.

**Lemma 1.** *Let $\omega\in k$, $\omega=\frac{1+\sqrt{-p}}{2}$. Then $\gamma(\omega)\in\mathbb{Z}$ (for the definition of $\gamma$, see §2).*

By Theorem 2 in §1, we obtain $\gamma(\omega)\in k_3$. In the general case, we have

$$[k_n:k_1]=|(\mathcal{O}/n\mathcal{O})^*/\mathcal{E}|, \tag{10}$$

where $\mathcal{O}$ is the ring of integers of $k$, and $\mathcal{E}$ is the subgroup of $(\mathcal{O}/n\mathcal{O})^*$ generated by the images of the units of $k$. In the case of $k_3$, we immediately deduce that $[k_3:k_1]$ is 2 or 4 depending on whether 3 splits into two factors in $k$ or remains prime. On the other hand, since $\gamma=\sqrt[3]{j}$ and $j(\omega)\in k_1$, we obtain $\gamma(\omega)\in k_1$. Since $k$ has class number one, we have $k=k_1$. Finally, $\gamma(\omega)$ is real, and so $\gamma(\omega)\in\mathbb{Q}$. Since $j(\omega)$ is an algebraic integer, the same is true for $\gamma(\omega)$. Thus, $\gamma(\omega)\in\mathbb{Z}$.

**Lemma 2.** $f(\omega)^2\in k_2^0$.

Relation (10) and the condition $p\equiv 3 \bmod 8$ imply that $[k_2:k]=3$ and, therefore, $[k_2^0:\mathbb{Q}]=3$. The equation $(u-16)^3=ju$ can be represented in the form $(u-16)^3=\gamma^3 u$, i.e.,

$$v^3-16=\gamma v, \tag{11}$$

where

$$v=\frac{u-16}{\gamma},\quad v^3=u.$$

By Theorem 2, we have $v(\omega)\in k_2$. The number $f(\omega)^4=\sqrt{u(\omega)}=v(\omega)^{3/2}$ belongs, on the one hand, to a quadratic extension $K$ of the field $k_2$, and, on the other hand, to an Abelian extension of $k$. Therefore, $K=k_2\left(\sqrt{\alpha}\right)$ with $\alpha\in k_1$, and either $f(\omega)^4\in k_2$ or $f(\omega)^8=\alpha\beta^2$ with $\beta\in k_2$. In the second case, we have $v(\omega)=\alpha\beta_1^2$, whence $N_{K_2/k}(v(\omega))=\alpha^3(N_{k_2/k}(\beta_1))^2$. However, by (2) we obtain $N_{k_2/k}(v(\omega))=4^2$ and, consequently, $\alpha\in(k_2^*)^2$, $K=k_2$. Thus, $f(\omega)^4\in k_2$ and $(N_{k_2/k}(f(\omega)^4))=2^2$, so that $N_{k_2/k}(f(\omega)^4)=\pm 8^2$. Since the number $f(\omega)^4$ is real and positive and $N_{k_2/k}(f(\omega)^4)>0$, we obtain $N_{k_2/k}(f(\omega)^4)=8^2$. Now, repeating the argument, we arrive at the fact that $f(\omega)^2\in k_2$. Since $f(\omega)$ is real, we have $f(\omega)^2\in k_2^0$. Lemma 2 is proved.

We have arrived at the following situation. For $\omega=\frac{1+\sqrt{-p}}{2}$, the value $\theta=v(\omega)=\frac{u(\omega)-16}{\gamma(\omega)}$ satisfies the equation

$$\theta^3-a\theta-16=0,\quad a=\gamma(\omega)\in\mathbb{Z},$$

over $\mathbb{Q}$ and $\sqrt[4]{\theta}\in\mathbb{Q}(\theta)$.

It turns out that all such cubic irrationalities $\theta$ can be found easily. We put $F(T)=T^3-aT-16$. Let $\theta_1=\sqrt{\theta}$, and let $F_1(T)=T^3+2AT^2+2BT+4C$ be the minimal polynomial of this number. Then $F(T^2)=-F_1(T)F_1(-T)$, whence

$$B=A^2,\quad 4(B^2-2AC)+a=0,\quad C^2=4.$$

Since $\sqrt{\theta_1} \in \mathbb{Q}(\theta)$ is real, we have $-C = N\big(\sqrt{\theta_1}\big)^2 > 0$. Therefore, $C = -2$ and $F_1(T) = T^3 + 2AT^2 + 2A^2T - 4$. Similarly, $F_1(T^2) = -F_2(T)F_2(-T)$, where $F_2(T) = T^3+2pT^2+2qT+2t$. We obtain $t^2 = 1$, $2(q-p^2) = A$, and $2(q^2-2p) = A^2$. Consequently, $2(q-p^2)^2 = q^2 - 2p$ or $(q-2p^2)^2 = 2p^4 - 2p$, and, for $s = q - 2p^2$, we have

$$s^2 = 2p(p^3 - 1). \tag{12}$$

We note that a solution $(s, p)$ of equation (12) determines $A = 2(q - p^2)$ and $a = -4(A^4 + 4A)$, and since $a = \gamma(\omega)$, it also determines $j(\omega) = a^3$. Therefore, the number of solutions of equation (12) does not exceed the number of the fields with properties that interest us.

Now, the full list of fields with class number one can be obtained from the following elementary statement.

**Lemma 3.** *The equation*

$$s^2 = 2p(p^3 - 1) \tag{13}$$

*has only the following solutions in* $\mathbb{Z}$:

$$(p, s) = (0, 0),\ \ (1, 0),\ \ (-1, \pm 2),\ \ (-2, \pm 6).$$

Indeed, we know 9 fields with class number one, which have the discriminants $-3$, $-4$, $-7$, $-8$, $-11$, $-19$, $-43$, $-67$, and $-163$. All the fields, except the three ones with discriminants $-4$, $-8$, and $-7$, correspond to the solutions of the above equation, and each field is uniquely determined by the corresponding solution. But the total number of solutions is also 6. Therefore, there are six fields with class number one and discriminant distinct from $-4$, $-8$, and $-7$.

*Proof of Lemma* 3. We have $s = 0$ if $p$ is equal to 0 or 1 and $s = \pm 2$ if $p = -1$. Let $s \neq 0, \pm 2$. We may assume that $|p| > 1$. Since $p$ is prime to $p^3 - 1$, we have the following possible cases: a) $p$ is a square, b) $-p$ is a square, c) $2p$ is a square, and d) $-2p$ is a square.

a) In this case $p^3 - 1 = 2v^2$, $p^3 = N\big(1 + v\sqrt{-2}\big)$. Thus, $1 + v\sqrt{-2} = (a + b\sqrt{-2})^3$ and $1 = a(a^2 - 6b^2)$. The latter equation has only the solution $a = 1$, $b = 0$, i.e., $p = 1$, which contradicts the condition $|p| > 1$.

b) $-p = q^2$ and $1 - p^3 = 1 + q^6 = 2v^2$, i.e., $2v^2 = (1 + q^2)(\rho + q^2)(\rho^2 + q^2)$. All three factors are relatively prime because they are not divisible by $\sqrt{-3}$. Therefore, two of them are squares and one is twice a square. Since $\rho + q^2$ and $\rho^2 + q^2$ are conjugate, we see that they must be squares, $\pm(\rho + q^2) = (a + b\rho)^2$. Hence $\pm 1 = b(2a - b)$ and $\pm q^2 = a^2 - b^2$. For $+$ signs, we obtain $b = \pm 1$, $a = \pm 1$, and $q = 0$, which is impossible because $1 + q^6 = 2v^2$. For $-$ signs, we have $b = \pm 1$, $a = 0$, and $q = \pm 1$, arriving at the solutions $p = -1$, $s = \pm 2$.

c) In this case we have $p^3 - 1 = v^2$ and $p^3 = (1 + iv)(1 - iv)$. Here, $v$ must be even because otherwise $p^3 \equiv 0(2)$ and $p^3 \not\equiv 0(8)$. It follows that the factors must be relatively prime. Consequently, $1 + iv = (a + bi)^3$ and $1 = a(a^2 - 3b^2)$, i.e., $a = 1$, $b = 0$, and $p = 1$, i.e., $2p$ is not a square.

d) In this case we deal with the equation $1 - p^3 = v^2$.

Euler found all rational solutions of this equation. He proved that if $p \neq 0$, then the solutions are exhausted by $v = \pm 3$, $p = -2$, $s = \pm 6$. Euler's proof can be found in [15] (Borel's talk). The lemma is proved. □

Finally, we obtain the following one-to-one correspondence between the fields with class number one and discriminant $-d \equiv 3 \bmod 8$ and the solutions $(p, s)$ of equation (3):

| $-d$ | 3 | 11 | 19 | 43 | 67 | 163 |
|---|---|---|---|---|---|---|
| $p$ | 0 | $-1$ | 1 | $-2$ | $-1$ | $-2$ |
| $s$ | 0 | $-2$ | 0 | $-6$ | 2 | 6 |

Theorem 1 is proved.

All who wrote about this topic (Deuring [11], Siegel [17]) pointed out the striking fact that not only a field with class number one determines an integral point on the curve given by equation (13), but also each integral point of this curve corresponds to such a field. This shows that this elliptic curve plays the role of a "moduli space" for the imaginary quadratic fields with class number one (see a discussion of "moduli spaces" in [18, Chapter 5, §1]).

Seemingly, Heegner's success was due to the fact that he constructed the first example of this notion. This guess is confirmed by the fact that, for the case of imaginary quadratic fields with class number two and an even discriminant, the three elliptic curves given by the equations $x^3 + 3x = y^2$, $x^3 + 3x = 2y^2$, and $9x^4 - 1 = 2y^2$ (i.e., the union of the sets of integral points) play the same role. Here, the integral points of the first curve correspond to the fields $\mathbb{Q}(\sqrt{-5})$, $\mathbb{Q}(\sqrt{-13})$, and $\mathbb{Q}(\sqrt{-37})$; the integral points of the second curve correspond to the fields $\mathbb{Q}(\sqrt{-10})$ and $\mathbb{Q}(\sqrt{-58})$, and the integral points of the third curve correspond to the field $\mathbb{Q}(\sqrt{-22})$. As in the case of fields with class number one (the condition $p > 7$), the field with a small discriminant $\mathbb{Q}(\sqrt{-6})$ is studied "by hand" separately (see [19]).

It should be noted that, refining his method, Stark determined all fields with class number two (without any restriction on the discriminant, see [20]).

## References


[1] C. E. Gauss, *Disquistiones Arithemeticae*, 2nd ed., Springer-Verlag, New York, 1986. MR0837656 (87f:01105)

[2] C. L. Siegel, *Über die Klassenzahl quadratischer Körper*, Gesammelte Abhandlungen, Bd. I, Springer-Verlag, Berlin–New York, 1966, p. 406. MR0197270 (33:5441)

[3] S. Lang, *Algebraic Numbers*, Addison–Wessley Publ., Reading, Mass., 1964. MR0160763 (28:3974)

[4] H. Heilbronn, *On the class numbers of imaginary quadratic fields*, Quart. J. Math. **5** (1935), 150–160.

[5] M. Deuring, *Imaginäre quadratische Zahlkörper mit der Klassenzahl* I, Math. Z. **37** (1933), no. 1, 405–415. MR1545403

[6] H. Heilbronn and E. H. Linfoot, *On the imaginary quadratic corpora of class number one*, Quart. J. Math. **5** (1934), 293–301.

[7] K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z. **56** (1952), 227–253. MR0053135 (14:725j)

[8] H. M. Stark, *A complete determination of the complex quadratic fields of class number one*, Michigan Math. J. **14** (1966), 1–23. MR0222050 (36:5102)

[9] A. Baker, *Linear forms in logarithms of algebraic numbers*, Mathematica **15** (1968), 204–216. MR0258756 (41:3402)

[10] ———, *A remark on the class numbers of quadratic fields*, Bull. London Math. Soc. **1** (1969), 98–102. MR0241383 (39:2723)

[11] M. Deuring, *Imaginäre quadratische Zahlkörper mit der Klassenzahl Eins*, Invent. Math. **5** (1968), no. 3, 169–179. MR0228464 (37:4044)

[12] B. Birch, *Diophantine analysis and modular functions*, Algebraic Geometry, Intern. Colloq., (Bombay, 1968), Tata Inst. Fund. Res., Oxford Univ. Press, London, 1969, pp. 35–42. MR0258832 (41:3478)

[13] Z. I. Borevich and I. R. Shafarevich, *The theory of numbers*, 3nd. ed., Nauka, Moscow, 1985. (Russian) MR816135 (88f:11001)

[14] R. Füeter, *Vorlesungen über die singulären Moduln und die komplexe Multiplikation der elliptischen Funktionen*, Bd. 1, Teubner, Berlin, 1924.

[15] A. Borel, S. Chowla, C. Herz, K. Iwasawa, and S.-P. Serre, *Seminar on complex multiplication*, Lectures Notes in Math., vol. 21, Springer-Verlag, Berlin, 1966. MR0201394 (34:1278)
[16] A. G. Kurosh, *The theory of groups*, Gosudarstv. Izdat. Teh.-Teor. Liit., Moscow-Leningrad, 1944; English transl., Chelsea Publ. Co., New York, 1956. MR0080089 (18:188f)
[17] C. L. Siegel, *Gesammelte Abhandlungen*, Bd. IV, Springer-Verlag, Berlin–New York, 1979, p. 41. MR543842 (80k:01066)
[18] D. Mumford and J. Fogarty, *Geometric invariant theory*, Ergeb. Math. Grenzgeb., vol. 34, Springer-Verlag, Berlin, 1982. MR719371 (86a:14006)
[19] V. A. Abrashkin, *Determination of the two-class imaginary quadratic fields with an even discriminant by Heegner's method*, Mat. Zametki **15** (1974), no. 2, 241–246; English transl., Math. Notes **15** (1974), 137–139. MR0354608 (50:7086)
[20] H. M. Stark, *On complex quadratic fields with class-number two*, Math. Comput. **29** (1975), no. 129, 289–302. MR0369313 (51:5548)

Steklov Mathematical Institute, Russian Academy of Sciences, 8 Gubkin str., 119991 Moscow, Russia

Received 20/DEC/2012

Translated by B. M. BEKKER