Assignment # 13

Igor Rapinchuk

The goal of this write-up is to prove that the only integer solution of the equation $y^2 = x^3 - 13$ are $(17, \pm 70)$ (cf. Theorem 3). The argument hinges on results about rings of algebraic integers (the ring relevant for analysis of the above equation is $\mathbb{Z}\left[\sqrt{-13}\right]$), particularly on the fact that every nonzero ideals admits a unique factorization as a product of prime ideals. In §1, we introduce rings of algebraic integers in quadratic fields and prove one result (the Main Lemma) that plays a crucial role in the proof of the theorem on prime factorization of ideals (Theorem 1), which we establish in §2. The latter section also contains a construction of the ideal class group. §3 contains a lemma, due to Minkowski, that enables one to prove the finiteness of the ideal class group, obtain a bound on its size, and ultimately to determine its structure. Finally, in §4, we use the results of §3 to describe the class group of the ring $\mathbb{Z}\left[\sqrt{-13}\right]$, which will enable us to prove Theorem 3.

1. Algebraic integers in quadratic fields and the Main Lemma

Let d be a square-free integer $\neq 0, 1$, and $F = \mathbb{Q}\left[\sqrt{d}\right]$ be the corresponding quadratic field. Furthermore, we let σ denote the conjugation map on F defined by $\sigma\colon a + b\sqrt{d} \mapsto a - b\sqrt{d}$ (notice that if $d < 0$ then σ is nothing but the map induced by the usual complex conjugation). One easily verifies that σ is an automorphism of the field F.

Definition. An element $x \in F$ is called an *algebraic integer* if it satisfies a monic quadratic polynomial with integer coefficients.

(This definition is an adaptation for elements of F of the general definition of algebraic integers, which states that an element $x \in \mathbb{C}$ is an algebraic integer if it satisfies some monic polynomial with integer coefficients (cf. Artin, p. 410). Proposition 11.6.7 of Artin asserts that this condition is equivalent to the integrality of the coefficients of the monic irreducible polynomial of x over $\mathbb{Q}$, which immediately implies that for elements of F our definition is equivalent to the general definition.)

Algebraic integers in F allow the following explicit description.

Proposition 1. *Let $x = a + b\sqrt{d} \in F$. If $d \equiv 2$ or $3 \pmod 4$ then x is an algebraic integer iff $a, b \in \mathbb{Z}$. If $d \equiv 1 \pmod 4$ then x is an algebraic integer iff $2a, 2b \in \mathbb{Z}$ and $2a \equiv 2b \pmod 2$. Thus the set of all algebraic integers in F is $\mathbb{Z} + \mathbb{Z}\omega$ where*

$$\omega = \begin{cases} \sqrt{d} & , \quad d \equiv 2, 3 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & , \quad d \equiv 1 \pmod 4 \end{cases}$$

Proof. If $b = 0$ then $x = a \in \mathbb{Q}$. However, we proved in Problem 8 of Assignment # 12 that a rational number that satisfies a monic polynomial with integer coefficients is necessarily an integer. So $x = a \in \mathbb{Z}$, which agrees with the description given in the statement.Now, suppose $b \neq 0$. Then x satisfies the monic quadratic polynomial

$$f(X) = (X - (a + b\sqrt{d}))(X - (a - b\sqrt{d})) = X^2 - 2aX + (a^2 - b^2 d)$$

In fact, $f(X)$ is the only monic quadratic polynomial with rational coefficients for which x is a root. Indeed, if $g(X) \in \mathbb{Q}[X]$ is a quadratic polynomial that has $x = a + b\sqrt{d}$, $b \neq 0$, as a root then its other root is $a - b\sqrt{d}$, so $g(X)$ must coincide with $f(X)$. It

follows that x is an algebraic integer iff $2a, a^2 - b^2 d \in \mathbb{Z}$. This, in particular, implies that if $a, b \in \mathbb{Z}$ then $x = a + b\sqrt{d}$ is an algebraic integer. Conversely, suppose that x is an algebraic integer. Then

$$(2b)^2 d = (2a)^2 - 4(a^2 - b^2 d) \in \mathbb{Z},$$

so $2b \in \mathbb{Z}$ as d is square-free. Similarly, if $a \in \mathbb{Z}$ then $b \in \mathbb{Z}$, and if $b \in \mathbb{Z}$ then $a \in \mathbb{Z}$. Thus, the situation where x is an algebraic integer and a, b are not both in $\mathbb{Z}$ can occur only when $a = a_0/2$, $b = b_0/2$ where a_0, b_0 are both odd. But then $a_0^2 - b_0^2 d \equiv 0 (\mathrm{mod}\, 4)$, hence d is a square modulo 4 and therefore $d \equiv 1 (\mathrm{mod}\, 4)$. Thus, if $d \equiv 2, 3 (\mathrm{mod}\, 4)$ then $a, b \in \mathbb{Z}$, proving our first assertion. Furthermore, if $d \equiv 1 (\mathrm{mod}\, 4)$ then $x = a + b\sqrt{d}$ is an algebraic integer iff either $a, b \in \mathbb{Z}$ or $a = a_0/2$, $b = b_0/2$ where both a_0, b_0 are odd, which is precisely our second assertion. Notice that

$$x = \frac{2a - 2b}{2} + (2b)\frac{1 + \sqrt{d}}{2},$$

from which our last assertion follows. □

Corollary 1. (1) *The set R of all algebraic integers in F is a subring of F.*

(2) *σ induces an automorphism of R.*

Proof. (1): Since $R = \mathbb{Z} + \mathbb{Z}\omega$ it is enough to show that $\omega^2 \in R$. However, ω satisfies a polynomial $X^2 + \alpha X + \beta$ with $\alpha, \beta \in \mathbb{Z}$, and our assertion follows.

(2): For any $x \in R$, the element $\sigma(x)$ satisfies the same polynomial with integer coefficients as x, and therefore remains an algebraic integer. Since $\sigma^2 = \mathrm{id}$, σ induces an automorphism of R. □

One can write out explicitly the irreducible polynomial for ω : it is $X^2 - d$ if $d \equiv 2, 3 (\mathrm{mod} 4)$, and $X^2 - X - (d-1)/4$ if $d \equiv 1 (\mathrm{mod} 4)$. The discriminant D of this polynomial is called the *discriminant of F* (or R). So,

$$D = \begin{cases} 4d & \text{if} \quad d \equiv 2, 3 (\mathrm{mod}\, 4) \\ d & \text{if} \quad d \equiv 1 (\mathrm{mod}\, 4) \end{cases}$$

For $x = a + b\sqrt{d} \in F$, we define the norm $N(x)$ by

$$N(x) = x\sigma(x) = a^2 - b^2 d \in \mathbb{Q}.$$

Using the fact that σ is an automorphism of F, one easily verifies that N is multiplicative:

$$N(xy) = (xy)\sigma(xy) = (x\sigma(x))(y\sigma(y)) = N(x)N(y),$$

for any $x, y \in F$. Besides, if $x \in R$ then

$$N(x) = x\sigma(x) \in R \cap \mathbb{Q} = \mathbb{Z}.$$

Lemma 1. *$x \in R$ is a unit iff $N(x) = \pm 1$.*

Proof. If $x \in R^\times$ then there exists $y \in R$ such that $xy = 1$. Taking the norm yields

$$N(xy) = 1 = N(x)N(y)$$

Since $N(x), N(y) \in \mathbb{Z}$, we conclude that $N(x) \in \mathbb{Z}^\times = \{\pm 1\}$. Conversely, if $x \in R$ and $N(x) = \pm 1$ then

$$x^{-1} = \frac{\sigma(x)}{N(x)} \in R,$$

so $x \in R^\times$. □

Before formulating the Main Lemma, we observe that since σ induces an automorphism of R, for any ideal $I \subset R$, the set $\sigma(I) = \{\sigma(x) \mid x \in I\}$ is also an ideal of R.

Main Lemma. *Let R be the ring of algebraic integers in $F = \mathbb{Q}\left[\sqrt{d}\right]$. Then for any ideal $I \subset R$ one has*

$$I\sigma(I) = (n)$$

for some $n \in \mathbb{Z}$.

Proof. We can assume that $I \neq \{0\}$. Since $I \subset \mathbb{Z} + \mathbb{Z}\omega$, it follows, for example, from Theorem 12.4.11 in Artin that $I = \mathbb{Z}\alpha + \mathbb{Z}\beta$ for some $\alpha, \beta \in I$. Then $\sigma(I) = \mathbb{Z}\sigma(\alpha) + \mathbb{Z}\sigma(\beta)$, and therefore $I\sigma(I)$ is the $\mathbb{Z}$-span of the following four elements:

$$\alpha\sigma(\alpha)\ ,\ \alpha\sigma(\beta)\ ,\ \beta\sigma(\alpha)\ ,\beta\sigma(\beta).$$

Clearly, $a = \alpha\sigma(\alpha)$ and $b = \beta\sigma(\beta)$ are integers. Furthermore, $c = \alpha\sigma(\beta) + \beta\sigma(\alpha)$ is fixed by σ, hence belongs to $\mathbb{Q}$, and also belongs to R, so in fact $c \in \mathbb{Q} \cap R = \mathbb{Z}$. Let n be the g.c.d. of a, b and c. Then n can be written as a linear combination of a, b, c and therefore $n \in I\sigma(I)$, implying that $(n) \subset I\sigma(I)$. To prove the opposite inclusion, we observe that

$$\frac{\alpha\sigma(\alpha)}{n}\ ,\ \frac{\beta\sigma(\beta)}{n} \in \mathbb{Z} \subset R$$

by construction, so it remains to establish that

$$\frac{\alpha\sigma(\beta)}{n}\ ,\ \frac{\beta\sigma(\alpha)}{n} \in R \tag{1}$$

For this we notice that the elements in (1) satisfy the equation $X^2 - rX + s$ where

$$r = \frac{\alpha\sigma(\beta) + \beta\sigma(\alpha)}{n}\ ,\ s = \frac{\alpha\sigma(\beta)}{n}\frac{\beta\sigma(\alpha)}{n} = \frac{\alpha\sigma(\alpha)}{n}\frac{\beta\sigma(\beta)}{n}$$

By our construction, $r, s \in \mathbb{Z}$, implying that the elements in (1) are algebraic integers, and therefore belong to R. □

Remark. The fact that we consider the ring R of all algebraic integers in F and not just the ring $R' = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ is essential. For example, take $d = -3$ and consider the ideal I of R' generated by 2 and $1 + \sqrt{-3}$. Then $I \neq R'$. Indeed, otherwise there would be $u, v \in R'$ such that $2u + (1 + \sqrt{-3})v = 1$. Multiplying by $1 - \sqrt{-3}$, we would get

$$1 - \sqrt{-3} = 2u(1 - \sqrt{-3}) + 4v,$$

which is impossible because the right-hand side is divisible by 2, while the left-hand side is not. Furthermore, one shows that 2 and $1 + \sqrt{-3}$ are non-associated irreducibles in R', which implies that I is a non-principal ideal in R' (notice, however, that these elements are associated in R!). Clearly, $I \neq (2)$ and $\mid R'/(2) \mid = 4$, which implies that the index $[I : (2)]$ in the sense of additive groups is 2. Then any additive subgroup $H \subset I$ strictly containing (2) must coincide with I. Using this, it is easy to see that

$$I = 2\mathbb{Z} + (1 + \sqrt{-3})\mathbb{Z}. \tag{2}$$

Indeed, $H = 2\mathbb{Z} + (1 + \sqrt{-3})\mathbb{Z}$ contains 2 and $2\sqrt{-3} = 2(1 + \sqrt{-3}) - 2$, and therefore contains (2). On the other hand, H is contained in I and is different from (2). So, by the above remark, $H = I$. It follows from (2) that $J = I\sigma(I)$ is the $\mathbb{Z}$-span of 4 and

$2(1 \pm \sqrt{-3})$. Since $1 - \sqrt{-3} = 2 - (1 + \sqrt{-3})$, we see that $J = 2I$. But since I is non-principal, J is also non-principal, so the conclusion of the Main Lemma is false in this situation.

2. Factorization of ideals and the ideal class group

A partial fix for non-unique factorization of elements in rings of algebraic integers is given by unique factorization of ideals.

Theorem 1. *Let R be the ring of integers in a quadratic field $F = \mathbb{Q}\left[\sqrt{d}\right]$. Every nonzero ideal of R which is not the whole ring is a product of prime ideals. This factorization is unique up to order of the factors.*

The proof relies on the following

Lemma 2. (1) *If $I \subset J$ are nonzero ideals of R then there exist an ideal $K \subset R$ such that $I = JK$.*

(2) (Cancellation Law) *Let I, J, K be nonzero ideals of R. If $IJ \supset IK$ then $J \supset K$, and if $IJ = IK$ then $J = K$.*

Proof. (1): By the Main Lemma, $J\sigma(J) = (n)$ for some nonzero $n \in \mathbb{Z}$. We have

$$I\sigma(J) \subset J\sigma(J) \subset (n),$$

so

$$K := (1/n)I\sigma(J) \subset R.$$

Since $I\sigma(J)$ is an ideal of R, we see that K is also an ideal of R. Furthermore,

$$JK = (1/n)IJ\sigma(J) = I,$$

as required.

(2): By the Main Lemma, $I\sigma(I) = (n)$. Then the inclusion $IJ \supset IK$ implies

$$I\sigma(I)J = nJ \supset I\sigma(I)K = nK,$$

hence $J \supset K$, proving the first claim. To prove the second claim, we observe that the equality $IJ = IK$ is equivalent to the two inclusions, $\subset$ and $\supset$. By the first part, these inclusions imply the inclusions $J \subset K$ and $J \supset K$, so $J = K$ as claimed. □

Proof of Theorem 1. Existence. First, we observe that any nonzero ideal $I \subset R$ contains a nonzero integer n (indeed, if $x \in I$, $x \neq 0$, then $n = N(x) = x\sigma(x) \in I$). The numbers $a + b\omega$, where $a, b = 0, \ldots, n-1$, form a complete set of representatives of cosets $R/(n)$, so $\mid R/(n) \mid = n^2$. Since $(n) \subset I$, we have a canonical surjective homomorphism $R/(n) \to R/I$, which yields the finiteness of R/I. By Proposition 10.4.3, the ideals of R that contain I correspond bijectively to the ideals of R/I, so the finiteness of the latter implies that the number of the ideals of R that contain I is finite. As a finite ring without zero divisors is a field, the finiteness of R/I also implies that a nonzero prime ideal of R is automatically maximal.

Now, let $I \subset R$ be an arbitrary nonzero ideal $\neq R$. If it is a prime ideal, there is nothing to prove. If it is not prime, it is strictly contained in some maximal ideal $P_1 \subset R$. By Lemma 2(1), we can write $I = P_1 I_1$ for some proper ideal $I_1 \subset R$. We have $I = P_1 I_1 \subset I_1$, and it follows from Lemma 2(2) that $I \neq I_1$. If I_1 is a prime ideal, we set $P_2 = I_1$ and then $I = P_1 P_2$ is a required factorization. If I_1 is not prime, we can repeat the above

argument to conclude that there is a factorization $I_1 = P_2 I_2$ for some prime ideal P_2 and some proper ideal $I_2 \subset R$ strictly containing I_1. Then $I = P_1 P_2 I_2$ with a strictly ascending chain $I \subset I_1 \subset I_2$. Since the number of the ideals of R containing I is finite, this process of splitting off prime ideals is bound to terminate, yielding thereby a required factorization of I as a product of prime ideals.

Uniqueness. We need to show that if

$$P_1 \cdots P_r = Q_1 \cdots Q_s, \tag{3}$$

with P_i, Q_j prime, then $r = s$ and after a permutation of ideals we have $P_i = Q_i$ for all $i = 1, \ldots, r = s$. We first observe that if $P \subset R$ is a prime ideal that contains $Q_1 \cdots Q_s$ then $Q_j \subset P$ for some j. Indeed, otherwise we would be able to pick $q_j \in Q_j \setminus P$ for every $j = 1, \ldots, s$. Then

$$q_1 \cdots q_s \in Q_1 \cdots Q_s \subset P,$$

so $q_j \in P$ for some j because P is prime, contrary to our choice of the q_j's. We will now analyze (3) by induction of r. If $r = 1$ then $P_1 = Q_1 \cdots Q_s$. By the above observation, $P_1 \supset Q_j$ for some j, and then actually $P_1 = Q_j$ because every prime ideal of R is maximal. After renumbering, we can assume that $j = 1$. Using the cancellation property of Lemma 2(2), we see that if $s > 1$ then $R = Q_2 \cdots Q_s$, which is impossible because the Q_j's are proper ideals. Thus, $s = 1 = r$ and $P_1 = Q_1$, as required. Suppose the uniqueness holds if the left-hand side of (3) contains $r = k$ factors, and prove it for $r = k + 1$ factors. The argument for $r = 1$ shows that $P_{k+1} = Q_j$ for some j, and after renumbering we can assume that $j = s$. Then the cancellation property implies that

$$P_1 \cdots P_{r-1} = Q_1 \cdots Q_{s-1}$$

By the induction hypothesis, $r - 1 = s - 1$, hence $r = s$, and after renumbering $P_i = Q_i$ for $i = 1, \ldots r - 1 = s - 1$. Since we already know that $P_r = Q_r$, this completes the proof of uniqueness.

Remark. Continuing the remark made in the end of the previous section, we would like to point out that most of the above results fail for the ring $R' = \mathbb{Z}[\sqrt{-3}]$. For example, the ideal (2) is not maximal because it is strictly contained in the ideal $I = (2, 1 + \sqrt{-3})$. In fact, I is the only proper ideal of R' that strictly contains (2). Indeed, if $I' \subset R'$ strictly contains (2) that it must contain one of the elements 1, $\sqrt{-3}$ or $1 + \sqrt{-3}$. In the first case, $I' = R'$. In the second case, is contains $-3 = \sqrt{-3}\sqrt{-3}$, and therefore also 1, so again $I' = R'$. In the remaining case, I' contains I and therefore $I' = I$ as $[R' : I'] = 2$. It is easy to see that $\sigma(I) = I$, so our computation in the previous section shows that $I^2 = 2I \neq (2)$, which implies that (2) is a product of prime ideals. Furthermore, the equality $I^2 = 2I$ also shows that the cancellation property, which is crucial for proving uniqueness, also fails.

We now describe a construction of the *ideal class group.* Two nonzero ideals I, J of R are called equivalent ($I \sim J$) if there exist nonzero $\alpha, \beta \in R$ such that

$$\alpha I = \beta J.$$

In other words, $I \sim J$ iff there exists $\lambda \in F^\times$ such that $J = \lambda I$. Then it is easy to see that $\sim$ is an equivalence relation on the set of all nonzero ideals. Indeed, $I \sim I$ because $I = 1 \cdot I$. If $I \sim J$ then $J \sim I$ because $J = \lambda I$ implies $I = \lambda^{-1} J$. Finally, if $I \sim J$ and $J \sim K$ then $I \sim K$ because $J = \lambda I$ and $K = \mu J$ imply $K = (\lambda\mu) I$. The equivalence

classes for this relation are called *ideal classes,* and the equivalence class of an ideal I will be denoted by $\langle I\rangle$. Notice that $\langle R\rangle$ is precisely the set of all principal ideals.

Proposition 2. *The ideal classes form an abelian group $\mathcal{C}$ with law of composition induced by multiplication of ideals:*

$$\langle I\rangle\langle J\rangle = \langle IJ\rangle \tag{4}$$

Proof. If $I \sim I'$ and $J \sim J'$ then $I' = \lambda I$ and $J' = \mu J$ for some $\lambda, \mu \in F^\times$ implying that $I'J' = (\lambda\mu)IJ$, hence $IJ \sim I'J'$. This shows that the law of composition given by (4) is well-defined. Since multiplication of ideals is associative and commutative, the multiplication of ideal classes defined by (4) also has these properties. The relation $IR = I$ for any ideal I implies that the class of principal ideals $\langle R\rangle$ is an identity element of $\mathcal{C}$. Finally, the relation $I\sigma(I) = (n)$ from the Main Lemma implies that $\langle\sigma(I)\rangle$ is an inverse for $\langle I\rangle$. □

Corollary 2. *Let R be the ring of algebraic integers of $F = \mathbb{Q}\left[\sqrt{d}\right]$. Then the following conditions are equivalent:*

(1) *R is a principal ideal domain;*
(2) *R is a unique factorization domain;*
(3) *the ideal class group $\mathcal{C} = \mathcal{C}(R)$ is a trivial group.*

Indeed, (3) means that every ideal of R is principal, so (1) $\Leftrightarrow$ (3). Every PID is UFD (Theorem 11.2.12), so (1) $\Rightarrow$ (2). Conversely, suppose R is UFD. Let P be a prime ideal of R. Then P contains an irreducible element π. Since R is UFD, π is a prime element, and therefore the ideal (π) is prime. However, we observed in the proof of Theorem 1 that every prime ideal of R is maximal. Thus, the inclusion $(\pi) \subset P$ implies that actually $P = (\pi)$, proving that every prime ideal of R is principal. Since any ideal of R is a product of prime ideals by Theorem 1, we see that all ideals of R are principal. So, (2) $\Rightarrow$ (1), completing the proof.

3. Minkowski's Lemma and its applications

An additive subgroup $L \subset \mathbb{R}^2$ is called a *lattice* if there exist two nonproportional vectors $a, b \in L$ such that $L = \mathbb{Z}a + \mathbb{Z}b$. The pair a, b is called a *basis* of L. If c, d is another basis of L then the transition matrix from a, b to c, d belongs to $GL_2(\mathbb{Z})$; in particular, it has determinant ± 1. Given a basis a, b of L, we let $\Pi(a, b)$ denote the parallelogram spanned by a, b; clearly

$$\Pi(a, b) = \{sa + tb \ \mid \ 0 \leqslant s, t \leqslant 1\}.$$

If $a = (a_1, a_2)$ and $b = (b_1, b_2)$, then by considering the cross-product we see that the area of $\Pi(a, b)$ is

$$A(\Pi(a, b)) = \mid \det \begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix} \mid$$

We notice that if $c = (c_1, c_2)$, $d = (d_1, d_2)$ is another basis of L then

$$\begin{bmatrix} c_1 & d_1 \\ c_2 & d_2 \end{bmatrix} = Q \begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix}$$

where Q is the transition matrix from a, b to c, d. As we observed above, $\det Q = \pm 1$, which implies that $A(\Pi(c, d)) = A(\Pi(a, b))$. Thus, $A(\Pi(a, b))$ depends only on the lattice L, but not on the choice of a basis in L, and therefore will be denoted by $\Delta(L)$.

A bounded subset $S \subset \mathbb{R}^2$ is called *convex* if for any $p, q \in S$, the line segment joining p and q lies entirely in S, and *centrally symmetric* if for any $p \in S$, one has $-p \in S$.

Minkowski's Lemma. *Let L be a lattice in $\mathbb{R}^2$, and let S be a convex, centrally symmetric subset of $\mathbb{R}^2$. If $A(S) > 4\Delta(L)$ then S contains a point of L other than zero.*

Proof. Let $U = (1/2)S$. Then $A(U) = (1/4)A(S) > \Delta(L)$. Fix a basis a, b of L and consider the parallelogram $\Pi = \Pi(a, b)$ spanned by a, b. We have $\mathbb{R}^2 = \cup_{z \in L} \Pi + z$, and for $z_1 \neq z_2$, the shifts $\Pi + z_1$ and $\Pi + z_2$ have only boundary points in common. Since U is bounded, one can find a finite collection $z_1, \ldots, z_m$ such that

$$U \subset \bigcup_{i=1}^{m} (\Pi + z_i);$$

then

$$A(U) = \sum_{i=1}^{m} A(U \cap (\Pi + z_i))$$

Let $U_i = (U \cap (\Pi + z_i)) - z_i$. Then $U_i \subset \Pi$ and

$$\sum A(U_i) = \sum_{i=1}^{m} A(U \cap (\Pi + z_i)) = A(U) > A(\Pi).$$

This means that the U_i's must overlap, i.e. there exist $i \neq j$ and $x, y \in S$ such that $(1/2)x + z_i = (1/2)y + z_j$. Then $z = z_j - z_i$ is a nonzero vector in L and

$$z = (1/2)x - (1/2)y \in S$$

because S is convex and z is nothing but the midpoint of the segment that joins $x, -y \in S$. □

Corollary 3. *Any lattice $L \subset \mathbb{R}^2$ contains a nonzero vector α such that*

$$| \alpha |^2 \leqslant 4\Delta(L)/\pi$$

Proof. Let $r > 0$ be a real number such that $r^2 > 4\Delta(L)/\pi$, and let S_r be a circle of radius r with center the origin. Then S is convex, centrally symmetric and $A(S) = \pi r^2 > 4\Delta(L)$. By Minkowski's Lemma, S_r contains a nonzero point of L. Set $r_0 = \sqrt{4\Delta(L)/\pi}$, and suppose that $S_{r_0} \cap L = \{(0, 0)\}$. Pick any $r_1 > r_0$. Then $L \cap S_{r_1}$ is finite, so the fact that $S_{r_0} \cap L = \{(0, 0)\}$ implies that there exists $r_0 < r_2 < r_1$ such that $L \cap S_{r_2} = \{(0, 0)\}$. But this contradicts our earlier conclusion. So, $S_{r_0} \cap L \neq \{(0, 0)\}$, which proves the corollary. □

Let now $L, M \subset \mathbb{R}^2$ be two lattices such that $M \subset L$. By Theorem 12.4.11, there exist bases a, b of L and c, d of M such that $c = \alpha a$ and $d = \beta b$ for some positive integers α, β. Then

$$L/M \simeq \mathbb{Z}/\alpha\mathbb{Z} \times \mathbb{Z}/\beta\mathbb{Z},$$

in particular, $[L : M] = \alpha\beta$. On the other hand,

$$A(\Pi(c, d)) = A(\Pi(\alpha a, \beta b)) = \alpha\beta A(\Pi(a, b)).$$

Thus, we obtain the following.

Lemma 3. *If $M \subset L$ are two lattices in $\mathbb{R}^2$. Then*

$$[L : M] = \Delta(M)/\Delta(L)$$

From now on, we will identify $\mathbb{R}^2$ with $\mathbb{C}$. Given any lattice $L \subset \mathbb{C}$ and any nonzero $z \in \mathbb{C}$, then zL is also a lattice. More precisely, if a, b is a $\mathbb{Z}$-basis of L then za, zb is a $\mathbb{Z}$-basis of zL. Furthermore, $\Pi(za, zb) = z\Pi(a, b)$. We can write z as $z = re^{\imath\phi}$, where $r =\mid z \mid$. Then multiplication by $e^{i\phi}$ is the rotation through an angle ϕ, hence does not change areas, while multiplication by r changes areas by a factor of $r^2 =\mid z \mid^2$. This proves the following.

Lemma 4. $\Delta(zL) =\mid z \mid^2 \Delta(L)$

We will now apply the above results to ideals of the ring R of algebraic integers in an imaginary quadratic field $F = \mathbb{Q}\left[\sqrt{d}\right]$, $d < 0$. We can naturally embed F into $\mathbb{C}$. Then, since $R = \mathbb{Z} + \mathbb{Z}\omega$ (Proposition 1), R can be thought of as a lattice in $\mathbb{C} \simeq \mathbb{R}^2$. If $d \equiv 2, 3 (\mathrm{mod}\, 4)$ then $\omega = \sqrt{d}$, and therefore

$$\Delta(R) =\mid \det \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{\mid d \mid} \end{bmatrix} \mid= \sqrt{\mid d \mid}.$$

If $d \equiv 1 (\mathrm{mod}\, 4)$ then $\omega = (1 + \sqrt{d})/2$, so

$$\Delta(R) =\mid \det \begin{bmatrix} 1 & 1/2 \\ 0 & \sqrt{\mid d \mid}/2 \end{bmatrix} \mid= \sqrt{\mid d \mid}/2.$$

Notice that both cases can be described by a single formula: $\Delta(R) = (1/2)\sqrt{\mid D \mid}$, where D is the discriminant. Now, if $I \subset R$ is a nonzero ideal then I is a sublattice of R and it follows from Lemma 3 that

$$\Delta(I) = \Delta(R)[R : I] \tag{5}$$

Furthermore, it follows from Lemma 4 that for any nonzero $z \in F$,

$$\Delta(zI) = N(z)\Delta(I). \tag{6}$$

Proposition 3. *Let $\mu = 2\sqrt{\mid D \mid}/\pi$. Then every ideal class contains an ideal I such that $[R : I] \leqslant \mu$.*

Proof. Let $J \subset R$ be an arbitrary nonzero ideal. Applying Corollary 3, we find a nonzero $\alpha \in J$ such that

$$N(\alpha) =\mid \alpha \mid^2 \leqslant 4\Delta(J)/\pi = 4\Delta(R)[R : J]/\pi = \frac{2\sqrt{\mid D \mid}}{\pi}[R : J] = \mu[R : J]$$

Then $(1/\alpha)J \supset R$ and

$$m = [(1/\alpha)J : R] = \frac{\Delta(R)}{\Delta((1/\alpha)J)} = N(\alpha)\frac{\Delta(R)}{\Delta(I)} = \frac{N(\alpha)}{[R : J]} \leqslant \mu$$

Then $(1/\alpha)J \subset (1/m)R$, and due to $[(1/m)R : R] = [R : mR] = m^2$, we have

$$[(1/m)R : (1/\alpha)J] = \frac{[(1/m)R : R]}{[(1/\alpha)J : R]} = m$$

It follows that

$$[R : (m/\alpha)J] = [(1/m)R : (1/\alpha)J] = m,$$

so the ideal $I = (m/\alpha)J$ is a required ideal that lies in the class of J and satisfies $[R : I] \leqslant \mu$. □

These results lead to the following important

Theorem 2. *Let $\mathcal{C} = \mathcal{C}(R)$ be the ideal class group. Then*

(1) *$\mathcal{C}$ is finite;*
(2) *$\mathcal{C}$ is generated by the classes of the prime ideals P which divide integer primes $p \leqslant [\mu]$.*

Proof. (1): According to Proposition 3, every class of ideals contain an ideal I such that $m = [R : I] \leqslant \mu$. Then $I \supset mR$. By Proposition 10.4.3, there is a bijection between the ideals of R that contain mR and the ideals of R/mR. But the latter ring is finite, namely $\mid R/mR \mid = m^2$, so the number of ideals $I \subset R$ such that $[R : I] = m$ is finite,for every integer $m \geqslant 1$, and the finiteness of $\mathcal{C}$ follows.

(2): Again, by Proposition 3, every class in $\mathcal{C}$ is represented by an ideal I such that $m = [R : I] \leqslant \mu$. By Theorem 1, $I = P_1 \cdots P_r$, where the P_i's are prime ideals. On the other hand, $m = p_1 \cdots p_s$ where the p_j's are primes $\leqslant m \leqslant \mu$. For every $i = 1, \ldots, r$, we have

$$m \in mR \subset I \subset P_i,$$

so P_i contains one on the p_j's, completing the proof.

□

4. The equation $y^2 = x^3 - 13$

We will analyze this equation in Theorem 3. Its relies on properties of the ring $R = \mathbb{Z}\left[\sqrt{-13}\right]$; we notice that since $-13 \equiv 3 (\mathrm{mod}\, 4)$, R is precisely the ring of (all) algebraic integers in $F = \mathbb{Q}\left[\sqrt{-13}\right]$.

Lemma 5. *Let $R = \mathbb{Z}\left[\sqrt{-13}\right]$. Then the ideal class group $\mathcal{C}$ of R is cyclic of order 2.*

Proof. We have

$$14 = 2 \cdot 7 = (1 + \sqrt{-13})(1 - \sqrt{-13}) \tag{7}$$

It is easy to see that the elements $2, 7, 1 \pm \sqrt{-13}$ are irreducible in R. Indeed, if, for example,

$$1 + \sqrt{-13} = (a + b\sqrt{-13})(c + d\sqrt{-13}) \text{ where } a, b, c, d \in \mathbb{Z}$$

is a nontrivial factorization (i.e. neither factor is a unit) then by taking the norm we obtain

$$14 = (a^2 + 13b^2)(c^2 + 13d^2)$$

It follows that $a^2 + 13b^2 = 2$ or 7, but neither case is possible with integer a, b. Thus, R is not a unique factorization domain, and therefore $\mid \mathcal{C} \mid > 1$ by Corollary 2. In fact, using (7), one can explicitly construct a non-principal ideal. Namely, set $P = (2, 1 + \sqrt{-13})$. Then $P \neq R$. Indeed, $P = R$ would imply the existence of $u, v \in R$ such that

$$2u + (1 + \sqrt{-13})v = 1$$

Multiplying by $1 - \sqrt{-13}$, we would get

$$2u(1 - \sqrt{-13}) + 14v = 1 - \sqrt{-13},$$

which is a contradiction because 2 does not divide $1 - \sqrt{-13}$ in R. Now, if $P = (s)$ then s is a non-unit that divides 2 and $1 + \sqrt{-13}$. But the latter elements are non-associated irreducibles, so such an s cannot exist. Since $R/(2)$ contains 4 elements, we see that R/P

contains 2 elements; in particular, P is a maximal ideal. Notice that if $\bar{P} = (2, 1-\sqrt{-13})$ is the conjugate ideal then

$$P\bar{P} = (2) \tag{8}$$

Indeed, $P\bar{P}$ is generated by 4, $2(1\pm\sqrt{-13})$ and $14 = (1+\sqrt{-13})(1-\sqrt{-13})$, implying the inclusion $\subset$ in (8). On the other hand, $g.c.d.(4, 14) = 2$, so $2 \in P\bar{P}$, and (8) is established. It follows from (8) and unique factorization for ideals (Theorem 1) that P and $\bar{P}$ are the only prime ideals of R dividing 2.

The discriminant of R is $D = -52$, so $[\mu] = \left[2\sqrt{\mid D \mid}/\pi\right]$ is 4, and therefore by Theorem 2(2), $\mathcal{C}$ is generated by prime ideals that divide 2 and 3. Notice that (3) is a prime ideal in R. Indeed,

$$R/(3) \simeq \mathbb{Z}[X]/(X^2+13, 3) \simeq \mathbb{F}_3[X]/(X^2+13).$$

But the polynomial $X^2 + 13 = X^2 + 1$ has no roots in $\mathbb{F}_3$, and therefore is irreducible in $\mathbb{F}_3[X]$. This implies that $R/(3)$ is a field, so (3) is a prime ideal. Thus, $\mathcal{C}$ is generated by the classes of P and $\bar{P}$. However, the class of $\bar{P}$ coincides with the class of P^{-1}, so eventually $\mathcal{C}$ is cyclic with generator P. It remains to show that P has order 2. Clearly, P^2 is generated by

$$4,\ 2(1+\sqrt{-13}),\ -12+2\sqrt{-13}$$

We conclude that $P^2 \subset (2)$, and on the other hand, $4, 14 \in P^2$ implying that $2 = g.c.d.(4, 14) \in P^2$, so that in fact $P^2 = (2)$. □

Theorem 3. *The only integer solutions to the equation*

$$y^2 = x^3 - 13 \tag{9}$$

are $(x, y) = (17, \pm 70)$.

Proof. Let (x, y) be an integer solution of (9). Then

$$(y+\sqrt{-13})(y-\sqrt{-13}) = x^3$$

This relation implies the following equality of principal ideals in $R = \mathbb{Z}\left[\sqrt{-13}\right]$:

$$(y+\sqrt{-13})(y-\sqrt{-13}) = (x)^3 \tag{10}$$

First, we show that the ideals $(y+\sqrt{-13})$ and $(y-\sqrt{-13})$ are relatively prime in R. Indeed, their sum $I = (y+\sqrt{-13}, y-\sqrt{-13})$ contains x^3 and $2y$. It follows from (9) that $d = g.c.d.(x, y)$ divides 13, so d can only be 1 or 13. However, if $d = 13$ then the left-hand side of $y^2 - x^3 = -13$ is divisible by 13^2, while the right-hand side is not. Thus, x and y are relatively prime. In addition x is odd. Indeed, if x is even, then taking (9) modulo 8 we would get $y^2 \equiv 3 (\mathrm{mod}\ 8)$ which is impossible because squares modulo 8 are $0, 1, 4$. It follows that x^3 and $2y$ are also relatively prime, implying $1 \in I$ as required.

Let

$$(y+\sqrt{-13}) = P_1^{\alpha_1}\cdots P_l^{\alpha_l}\ ,\ (y-\sqrt{-13}) = Q_1^{\beta_1}\cdots Q_m^{\beta_m}\ ,\ (x) = R_1^{\gamma_1}\cdots R_n^{\gamma_n}$$

be factorizations as products of prime ideals. Then (10) implies

$$P_1^{\alpha_1}\cdots P_l^{\alpha_l}Q_1^{\beta_1}\cdots Q_m^{\beta_m} = R_1^{3\gamma_1}\cdots R_n^{3\gamma_n} \tag{11}$$

Since the ideals $(y-\sqrt{-13})$ and $(y+\sqrt{-13})$ are relatively prime, we have $P_i \neq Q_j$ for all $i = 1, \ldots, l$ and $j = 1, \ldots, m$, and therefore we derive from (11) that the α_i's and β_j's are all multiples of 3, say $\alpha_i = 3\alpha_i'$. Consider the ideal

$$J = P_1^{\alpha_1'} \cdots P_l^{\alpha_l'}$$

Then by construction $J^3 = (y+\sqrt{-13})$, in particular, J^3 is principal. However, by Lemma 5, the class group of R is cyclic of order 2, which implies that J itself is principal, say $J = (z)$. Then $(y+\sqrt{-13}) = (z^3)$, and therefore

$$y + \sqrt{-13} = \varepsilon z^3 \tag{12}$$

where $\varepsilon \in R$ is a unit. But if $\varepsilon = a+b\sqrt{-13}$ is a unit in R then by Lemma 1, $a^2+13b^2 = 1$, which implies that the unit group of R is $\{\pm 1\}$. So, if $z = u + v\sqrt{-13}$ (where $u, v \in \mathbb{Z}$) then (12) implies

$$y + \sqrt{-13} = \pm(u + v\sqrt{-13})^3 \tag{13}$$

Replacing u, v with $\pm u, \pm v$, we can assume that the sign in (13) is plus. Then $y = u^3 - 39uv^2$ and $1 = (3u^2 - 13v^2)v$. From the last equation we conclude that $3u^2 - 13v^2$ and v must be ± 1. The only possibilities are $u = \pm 2$ and $v = -1$. Then $y = \pm 70$, and $x = 17$.

□