Algebraic Number Theory

René Schoof

Dipartimento di Matematica
2^{a} Università di Roma "Tor Vergata"
I-00133 Roma ITALY
Email: schoof@fwi.uva.nl

Abstract. This lecture is part of a series of introductory talks given in El Escorial, Spain in the summer of 1994. The talks were concerned with Wiles' proof of Fermat's Last Theorem. In this lecture we study the Diophantine equations $X^3 = Y^2 + d$ for $d = 1, 19, -18, 61$ and 5. Along the way, we introduce the basic concepts of algebraic number theory.

1. $d = 1$.

In this lecture we study the Diophantine equations

$$X^3 = Y^2 + d, \qquad d \in \mathbf{Z}.$$

The problem is to solve these equations in ordinary integers $X, Y \in \mathbf{Z}$. Even though the problem only involves only ordinary integers in $\mathbf{Z}$, we are naturally led to consider other algebraic numbers. Along the way we introduce various concepts in algebraic number theory. See [1, 2, 3, 4] for more systematic introductions to algebraic number theory.

We begin with the case $d = 1$. In this case we can give a complete answer. Our method relies on arithmetic in the ring of *Gaussian integers* $\mathbf{Z}[i]$, given by

$$\mathbf{Z}[i] = \{a + bi : a, b \in \mathbf{Z}\}.$$

The ring $\mathbf{Z}[i]$ is a subring of the field of complex numbers. It is itself not a field; it is easy to see that the only units of $\mathbf{Z}[i]$ are ± 1 and $\pm i$. The ring $\mathbf{Z}[i]$ is a *unique factorization domain,* i.e., every non-zero element $\alpha \in \mathbf{Z}[i]$ can be written as a product of *irreducible* elements of $\mathbf{Z}[i]$ and, apart from the order and multiplication by the units $\pm 1, \pm i$, this can be done in only one way. This property of the ring $\mathbf{Z}[i]$ is well known; it follows from the fact that $\mathbf{Z}[i]$ is a Euclidean domain which is an easy consequence of the fact that the complex plane $\mathbf{C}$ can be covered by the disks of radius 1 and center $a + bi \in \mathbf{Z}[i]$.

The following lemma is the key ingredient to our method:

lemma 1.1. *Let R be a (commutative) unique factorization domain. Let r be a positive integer and suppose that $\alpha, \beta \in R$ are coprime and satisfy*

$$\alpha\beta = \gamma^r.$$

Then, up to a unit in R^*, both α and β are r-th powers.

Proof. Let

$$\alpha = \pi_1^{a_1} \cdot \ldots \cdot \pi_n^{a_n},$$
$$\beta = {\pi'_1}^{b_1} \cdot \ldots \cdot {\pi'_m}^{b_m}$$

be the factorizations of α into a product of distinct irreducible elements π_i and of β into a product of distinct irreducible elements π'_i respectively. Similarly

$$\gamma = {\pi''_1}^{c_1} \cdot \ldots \cdot {\pi''_k}^{c_k}$$

for distinct irreducible elements π''_i. We now have that

$$\begin{aligned}\gamma^r &= {\pi''_1}^{rc_1} \cdot \ldots \cdot {\pi''_k}^{rc_k}, \\ &= \pi_1^{a_1} \cdot \ldots \cdot \pi_n^{a_n} \cdot {\pi'_1}^{b_1} \cdot \ldots \cdot {\pi'_n}^{b_m}.\end{aligned}$$

Since α and β are coprime, $\pi_i \neq \pi'_j$ for all i and j. Therefore, by the uniqueness of the factorization, each π_i and π'_i is, up to a unit, equal to one of the π''_j, and each exponent a_i and b_i is equal to the corresponding exponent rc_j. This implies that all exponents a_i and b_j are divisible by r and this implies the lemma.

Theorem 1.2. *The only solution $X, Y \in \mathbf{Z}$ of the equation*

$$X^3 = Y^2 + 1$$

is given by $X = 1$ and $Y = 0$.

Proof. Let $X, Y \in \mathbf{Z}$ be a solution. If X were even, we would have $Y^2 = X^3 - 1 \equiv -1 \pmod 4$ and that is impossible since squares are congruent to 0 or 1 $\pmod 4$. Therefore X is odd. We write, in the ring $\mathbf{Z}[i]$

$$X^3 = (Y + i)(Y - i).$$

A common divisor of $Y + i$ and $Y - i$ divides their difference $2i$ and hence 2. This common divisor also divides the odd number X^3 and hence the gcd of X^3 and 2, which is 1. We conclude that $Y + i$ and $Y - i$ have no common divisor. The ring $\mathbf{Z}[i]$ being a unique factorization domain, we can apply Lemma 1.1: since the product of $Y + i$ and $Y - i$ is a cube, each factor is, *up to a unit,* itself a cube. Since the unit group of $\mathbf{Z}[i]$ has order 4, which is prime to 3, every unit is also a cube. Therefore

$$Y + i = (a + bi)^3$$

for some $a, b \in \mathbf{Z}$. There is an analogous equation involving $Y - i$. Equating real and imaginary parts, we find that

$$Y = a^3 - 3ab^2,$$
$$1 = 3a^2 b - b^3.$$

The second relation says that $b(3a^2 - b^2) = 1$. Therefore $b = 1$ and $3a^2 = -1$ or $b = -1$ and $3a^2 - 1 = -1$. Only the second possibility gives rise to a solution of the equation $X^3 = Y^2 + 1$ viz., $Y = 0$ and $X = 1$ as required.

2. $d = 19$.

In this section we consider the equation $X^3 = Y^2 + d$ for $d = 19$:

$$X^3 = Y^2 + 19.$$

We solve it in a similar way: if X were even, we would have $Y^2 = X^3 - 19 \equiv 0 - 19 \equiv 5 \pmod 8$, but this is impossible, since odd squares are congruent to $1 \pmod 8$. If X were divisible by 19, also Y would be divisible by 19. This implies that $19 = X^3 - Y^2$ is divisble by 19^2, but that is absurd. We conclude that X is divisible by neither 19 or 2.

In the ring $\mathbf{Z}[\sqrt{-19}]$, viewed as a subring of $\mathbf{C}$

$$\mathbf{Z}[\sqrt{-19}] = \{a + b\sqrt{-19} : a, b \in \mathbf{Z}\},$$

we write

$$X^3 = (Y + \sqrt{-19})(Y - \sqrt{-19}).$$

A common divisor $\delta \in \mathbf{Z}[\sqrt{-19}]$ of $Y + \sqrt{-19}$ and $Y - \sqrt{-19}$ divides the difference $2\sqrt{-19}$ and hence $2 \cdot 19$. Since $(Y + \sqrt{-19})(Y - \sqrt{-19}) = Y^2 + 19 = X^3$, we see that δ also divides X^3. Therefore δ divides the gcd of X^3 and $2 \cdot 19$ which is equal to 1. We conclude that the factors $Y + \sqrt{-19}$ and $Y - \sqrt{-19}$ have no common divisor.

A number $x = a + b\sqrt{-19} \in \mathbf{Z}[\sqrt{-19}]$ is a unit if and only if its norm $N(x) = a^2 + 19b^2$ is equal to 1. It is easy to see that the only units of the ring $\mathbf{Z}[\sqrt{-19}]$ are 1 and -1. Since the product $(Y + \sqrt{-19})(Y - \sqrt{-19})$ is a cube, an application of Lemma 1.1 shows that each of the factors $Y + \sqrt{-19}$ and $Y - \sqrt{-19}$ is, up to a sign, itself a cube. Since -1 is itself a cube, this means that

$$Y + \sqrt{-19} = (a + b\sqrt{-19})^3$$

for some $a, b \in \mathbf{Z}$. Taking real and imaginary parts we find

$$\begin{aligned} Y &= a^3 - 3 \cdot 19ab^2, \\ 1 &= 3a^2b - 19b^3. \end{aligned}$$

it is easy to see that already the second equation $b(3a^2 - 19b^2) = 1$ has no solutions $a, b \in \mathbf{Z}$. As in the previous example one would now like to conclude that the original equation $X^3 = Y^2 + 19$ has no solutions either, but this is *not true at all,* as is shown by the following equality:

$$7^3 = 18^2 + 19.$$

What went wrong? The problem is, that one can only apply Lemma 1.1 if the ring under consideration admits unique factorization. The ring $\mathbf{Z}[\sqrt{-19}]$ does not have this property:

$$\begin{aligned} 35 &= 5 \cdot 7, \\ &= (4 + \sqrt{-19})(4 - \sqrt{-19}), \end{aligned}$$

are two distinct factorizations of the number 35 in the ring $\mathbf{Z}[\sqrt{-19}]$. We check that the factors are irreducible elements. The norm map

$$N : \mathbf{Z}[\sqrt{-19}] \longrightarrow \mathbf{Z}$$

given by $N(a + b\sqrt{-19}) = a^2 + 19b^2$, is multiplicative. We have $N(5) = 25$, $N(7) = 49$ and $N(4 \pm \sqrt{-19}) = 4^2 + 19 = 35$. If any of these numbers were not irreducible in the ring $\mathbf{Z}[\sqrt{-19}]$, there would be elements in this ring of norm 5 or 7. Since the equations $a^2+19b^2 = 5$ and $a^2+19b^2 = 7$ have no solutions $a, b \in \mathbf{Z}$, there are no such elements. We conclude that the number 35 admits two genuinely distinct factorizations into irreducible elements. Therefore the ring $\mathbf{Z}[\sqrt{-19}]$ is not a unique factorization domain.

In this first example it is rather easy to get around the problem. The ring $\mathbf{Z}[\sqrt{-19}]$ is in some sense too small.

Definition. Let F be a number field. The *ring of integers O_F of F* is the integral closure of $\mathbf{Z}$ in F. In other words

$$O_F = \{x \in F : \ f(x) = 0 \text{ for some monic } f \in \mathbf{Z}[X]\}.$$

The ring $\mathbf{Z}[\sqrt{-19}]$ is *not* the ring of integers of the number field $F = \mathbf{Q}(\sqrt{-19})$. In general, for quadratic number fields the rings of integers are as follows.

Proposition 2.2. *Let $d \neq 1$ be a squarefree integer. Then the ring of integers of $\mathbf{Q}(\sqrt{d})$ is given by*

$$\begin{array}{ll} \mathbf{Z}[\sqrt{d}] & \text{if } d \equiv 2 \text{ or } 3 \pmod 4; \\ \mathbf{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \pmod 4; \end{array}$$

For instance, the ring of integers of $F = \mathbf{Q}(\sqrt{-19})$ is

$$O_F = \mathbf{Z}[\frac{1+\sqrt{-19}}{2}] = \{\frac{a+b\sqrt{-19}}{2} : a, b \in \mathbf{Z},\ a \equiv b \pmod 2\}$$

which contains $\mathbf{Z}[\sqrt{-19}]$ as a subring of index 2. The ring O_F is not Euclidean, but using techniques from algebraic number theory, it can be shown that O_F is a unique factorization domain. Applying Lemma 1.1, we can solve the Diophantine equation as follows:

Theorem 2.3. *The only solutions in integers $X, Y \in \mathbf{Z}$ of the equation*

$$X^3 = Y^2 + 19$$

are $X = 7$ and $Y = \pm 18$.

Proof. We proceed as before. We write

$$X^3 = (Y + \sqrt{-19})(Y - \sqrt{-19})$$

and we conclude from Lemma 1.1 that each factor is a cube in the ring of integers O_F. In particular

$$\begin{aligned} Y + \sqrt{-19} &= \left(\frac{a + b\sqrt{-19}}{2}\right)^3, \\ &= \frac{a^3 - 3 \cdot 19ab^2}{8} + \frac{3a^2b - 19b^3}{8}\sqrt{-19}. \end{aligned}$$

Equating real and imaginary parts we find that

$$b\frac{3a^2 - 19b^2}{8} = 1.$$

This implies that b divides 8 and that $3a^2 - 19b^2 = 8/b$. This leaves only a few possibilities for b and one easily checks that only $b = 1$ gives rise to the integral solution $a = \pm 3$. This implies that $Y = \pm 18$ and $X = 7$, as required.

3. $d = -18$**.**

The equation $X^3 = Y^2 - 18$ factors as

$$X^3 = (Y - \sqrt{18})(Y + \sqrt{18}).$$

This time the number field $F = \mathbf{Q}(\sqrt{18}) = \mathbf{Q}(\sqrt{2})$ is involved. By Prop.2.2 the ring of integers O_F of F is given by

$$O_F = \mathbf{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbf{Z}\}.$$

It is a Euclidean ring and therefore a unique factorization domain. The gcd of the factors $Y + \sqrt{18} = Y + 3\sqrt{2}$ and $Y - \sqrt{18} = Y - 3\sqrt{2}$ divides $2\sqrt{18} = 6\sqrt{2}$. However, if $\sqrt{2}$ divides the gcd, then 2 divides both X and Y and $Y^2 = X^3 + 18 \equiv 2 \pmod 4$; a contradiction. If 3 divides the gcd, then 3 divides both X and Y and we can write $X = 3X'$ and $Y = 3Y'$. Then $3X'^3 = Y'^2 - 2$ and $Y'^2 \equiv -1 \pmod 3$. This contradiction shows that $Y + 3\sqrt{2}$ and $Y - 3\sqrt{2}$ are coprime in $\mathbf{Z}[\sqrt{2}]$.

A careless application of Lemma 1.1 to the ring $\mathbf{Z}[\sqrt{2}]$ and the equation $X^3 = (Y - \sqrt{18})(Y + \sqrt{18})$, would give us that

$$\begin{aligned} Y + 3\sqrt{2} &= (a + b\sqrt{3})^3, \\ &= (a^3 + 6ab^2) + (3a^2b + 2b^3)\sqrt{2}. \end{aligned}$$

From this one would then deduce that $b(3a^2 + 2b^2) = \pm 1$ and hence that $b = \pm 1$ and $3a^2 = \pm 1 - 2$. Since this equation has no solutions in $\mathbf{Z}$, the original equation would have no solutions in $\mathbf{Z}$ either. But this is clearly false:

$$7^3 = 19^2 + 18.$$

What went wrong this time? This time the unit group of the ring $\mathbf{Z}[\sqrt{2}]$ is rather large and the application of Lemma 1.1. was not quite correct: from the equation one can only deduce that $Y + 3\sqrt{2}$ is a cube, *up to units of the ring* $\mathbf{Z}[\sqrt{2}]$. To understand this complication better, we consider the unit group more closely.

Dirichlet's Unit Theorem gives a complete description of the unit group of the ring of integers of a number field. This result is one of the basic theorems of algebraic number theory. In general, it says the following.

Let F be a number field. By the theorem of the primitive element there exists an element $\alpha \in F$ such that $F = \mathbf{Q}(\alpha)$. Let $f(X) \in \mathbf{Q}[X]$ be the mimimum polynomial of α. We have that

$$f(X) = (X - \alpha_1)(X - \alpha_2) \cdot \ldots \cdot (X - \alpha_n),$$

where the α_j are the zeroes of $f(X)$ in $\mathbf{C}$. The first r_1 zeroes are contained in $\mathbf{R}$ while the remaining $n - r_1$ are not. The latter zeroes come in complex conjugate pairs. There are $2r_2$ of them and we number them in such a way that $(\overline{\alpha_j}) = \alpha_{j+r_2}$ for $r_1 < j \leq r_2$. We have that $n = [F : \mathbf{Q}] = r_1 + 2r_2$.

For every j we consider the embeddings

$$\begin{aligned} \varphi_j : F &\hookrightarrow \mathbf{R}, \qquad \text{for } j \leq r_1, \\ \varphi_j : F &\hookrightarrow \mathbf{C}, \qquad \text{for } j > r_1. \end{aligned}$$

given by $\varphi_j(\alpha) = \alpha_j$. Using the embeddings φ_j for $1 \leq j \leq r_1 + r_2$ we define a group homomorphism

$$\Psi : O_F^* \longrightarrow \mathbf{R}^{r_1+r_2}.$$

by

$$\Psi(\varepsilon) = \begin{pmatrix} \log|\varphi_1(\varepsilon)| \\ \vdots \\ \log|\varphi_{r_1+r_2}(\varepsilon)| \end{pmatrix}.$$

Theorem 3.1. *(Dirichlet's Unit Theorem) The kernel of the homomorphism Ψ is finite and is equal to the group of roots of unity contained in F. The image is a lattice in the subspace of $\mathbf{R}^{r_1+r_2}$ of codimension 1 which is given by*

$$\{\begin{pmatrix} x_1 \\ \vdots \\ x_{r_1+r_2} \end{pmatrix} \in \mathbf{R}^{r_1+r_2} : x_1 + \ldots + x_{r_1+r_2} = 0\}.$$

In particular, $\Psi(O_F^*)$ is a free abelian group of rank $r_1 + r_2 - 1$ and there is an isomorphism of groups

$$O_F^* \cong \mathbf{Z}/w\mathbf{Z} \times \mathbf{Z}^{r_1+r_2-1}$$

where w denotes the number of roots of unity contained in F.

For example, for the fields $\mathbf{Q}(i)$ and $\mathbf{Q}(\sqrt{19})$ and, in general, any number field of the form $F = \mathbf{Q}(\sqrt{-d})$ where d is a positive integer, we have that $r_1 = 0$ and $r_2 = 1$. Therefore the rank of the unit group is $r_1 + r_2 - 1 = 0$ and O_F^* is equal to the group of roots of unity in F. For $F = \mathbf{Q}(i)$ this is a group of order 4 and for $\mathbf{Q}(\sqrt{-19})$ this is the group $\{\pm 1\}$. For $\mathbf{Q}(\sqrt{2})$ however, $r_1 = 2$ and $r_2 = 0$ and in this case the rank of O_F^* is equal to 1.

This means that in the ring $\mathbf{Z}[\sqrt{2}]$ there are, apart from the usual units ± 1, infinitely many more units. Indeed, $1 + \sqrt{2}$ is also a unit (with inverse $-1 - \sqrt{2}$) and so are all its powers. Using methods from algebraic number theory one can show that

$$\mathbf{Z}[\sqrt{2}] = \{\pm(1 + \sqrt{2})^k : k \in \mathbf{Z}\} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}.$$

Lemma 1.1 only allows us to conclude that the factor $Y + 3\sqrt{2}$ is a cube *up to units.* Indeed, the non-trivial solution $X = 7$, $Y = 19$ corresponds to the factor $19 + 3\sqrt{3}$ which satisfies

$$19 + 3\sqrt{2} = \left(3 - \sqrt{2}\right)^3 (3 + 2\sqrt{2}).$$

Note that $3 + 2\sqrt{2} = (1 + \sqrt{2})^2$ is a unit. We do not determine all solutions to the Diophantine equation $X^3 = Y^2 + 18$. This problem is related to the problem of determining integral points on elliptic curves and can be solved by means of techniques that belong to the theory of Diophantine approximation.

4. $d = 61$.

In this section we discuss the equation

$$X^3 = Y^2 + 61.$$

We have

$$X^3 = (Y + \sqrt{-61})(Y - \sqrt{-61})$$

in the ring $\mathbf{Z}[\sqrt{-61}]$. By Prop.2.2 this ring is actually the ring of integers of the number field $\mathbf{Q}(\sqrt{-61})$. A common divisor of the factors $Y + \sqrt{-61}$ and $Y - \sqrt{-61}$ divides also $2\sqrt{-61}$. If it does not divide $\sqrt{-61}$, then Y is necessarily odd and X must be even. We find that

$$Y^2 = X^3 - 61 \equiv 3 \pmod 8$$

which is impossible. If, on the other hand, the common divisor divides $\sqrt{-61}$, then 61 divides both Y and X. This implies that $61 = X^3 - Y^2$ is divisible by 61. A contradiction. We conclude that the factors are coprime.

By Dirichlet's Unit Theorem 3.1, the only units of the ring $\mathbf{Z}[\sqrt{-61}]$ are ± 1, both of which are cubes. Our final careless application of Lemma 1.1 therefore would give us that

$$\begin{aligned} Y + \sqrt{-61} &= (a + b\sqrt{-61})^3, \\ &= (a^3 - 3 \cdot 61ab^2) + (3a^2b - 61b^3)\sqrt{-61}. \end{aligned}$$

Inspection of the imaginary parts gives us that $1 = b(3a^2 - 61b^2)$. This means that $b = \pm 1$ and that $3a^2 = \pm 1 + 61$ which has no solution in integers. Therefore we would conclude that the equation $X^3 = Y^2 + 61$ has no solutions in integers $X, Y \in \mathbf{Z}$.

However, this is once again false:

$$5^3 = 8^2 + 61.$$

So something went wrong again ... This time the ring $\mathbf{Z}[\sqrt{-61}]$ is the ring of integers of $\mathbf{Q}(\sqrt{-61})$ and the only units are ± 1, but $\mathbf{Z}[\sqrt{-61}]$ does not have the unique factorization property:

$$\begin{aligned} 62 &= (1+\sqrt{-61})(1-\sqrt{-61}), \\ &= 2 \cdot 31. \end{aligned}$$

However, the ring $\mathbf{Z}[\sqrt{-61}]$ still admits unique factorization *of ideals.* In general, for an algebraic number field F, one defines a fractional ideal I as a non-zero O_F-submodule of F. In other words, there exists an $a \in O_F$ such that $aI \subset O_F$ is a non-zero ideal of O_F. Examples of fractional ideals are *principal fractional ideals,* which are given by

$$\{\alpha \cdot x : \alpha \in F\}$$

for any $x \in F^*$. The fractional ideals form a group I_F under ideal multiplication. The fact that the unique factorization property holds for ideals, means that I_F is a free group on the prime ideals of O_F. The principal fractional ideals form a subgroup P_F. The following theorem is one of the basic results of algebraic number theory.

Theorem 4.1. *The group I_F is a free group on the prime ideals of O_F. The quotient group*

$$Cl_F = I_F/P_F$$

is called the ideal class group of F. It is a finite abelian group of order h_F, the *class number of F.*

Clearly, the class group Cl_F is trivial if and only if the ring O_F is a principal ideal ring and one can show that this happens precisely when O_F has the unique factorization property. The class groups of the rings $\mathbf{Q}(i)$, $\mathbf{Q}(\sqrt{-19})$ and $\mathbf{Q}(\sqrt{2})$ are all trivial, but the class group of $\mathbf{Q}(\sqrt{-61})$ is not. Using methods from algebraic number theory, one can show that it has order 6.

From the equation

$$X^3 = (Y+\sqrt{-61})(Y-\sqrt{-61})$$

we can still deduce that $Y+\sqrt{61}$ is the cube *of an ideal.* Indeed, the solution $X = 5$, $Y = 8$ gives rise to the equation

$$5^3 = (8+\sqrt{-61})(8-\sqrt{-61}).$$

and the principal ideal $(8+\sqrt{-61})$ is the cube of the ideal generated by 5 and $3+\sqrt{-61}$.

We do not determine all the solutions of the Diophantine equation $X^3 = Y^2 + 61$, but in the next section we solve a similar equation using Theorem 4.1.

5. $d = 5$**.**

The equation

$$X^3 = Y^2 + 5$$

gives rise to a factorization

$$X^3 = (Y + \sqrt{-5})(Y - \sqrt{-5})$$

in the ring $\mathbf{Z}[\sqrt{-5}]$. A common divisor of the factors necessarily divides $2\sqrt{-5}$. Since $61 \equiv 5 \pmod 8$, one can use the same arguments as in the previous section to show that any common divisor of $Y + \sqrt{-5}$ and $Y - \sqrt{-5}$ is necessarily a unit.

In order to avoid further "careless" applications of Lemma 1.1, we analyze the ring $\mathbf{Z}[\sqrt{-5}]$ in some detail. Since $x \in \mathbf{Z}[\sqrt{-5}]$ is a unit if and only if $x = a + b\sqrt{-5}$ with $a, b \in \mathbf{Z}$ and $a^2 + 5b^2 = 1$, we see that the only units of $\mathbf{Z}[\sqrt{-5}]$ are ± 1. By Prop.2.2, $\mathbf{Z}[\sqrt{-5}]$ is the ring of integers of $F = \mathbf{Q}(\sqrt{-5})$. This ring is not a principal ideal ring or a unique factorization domain. Indeed,

$$\begin{aligned} 6 &= (1 + \sqrt{-5})(1 - \sqrt{-5}), \\ &= 2 \cdot 3, \end{aligned}$$

which shows that the unique factorization property fails. The ideal

$$(2, 1 + \sqrt{5})$$

is not principal. Indeed, any generator $\alpha = a + b\sqrt{-5}$ (with $a, b \in \mathbf{Z}$) would necessarily have the property that $N(\alpha) = a^2 + 5b^2$ divides 4 and $1^2 + 5 = 6$ and therefore 2. Since α cannot be a unit and since the equation $a^2 + 5b^2 = 2$ has no solutions with $a, b \in \mathbf{Z}$, the ideal cannot be principal.

Using techniques from algebraic number theory, one can show that the class group Cl_F has order 2. This implies that the product of any two non-principal ideals is principal and, in particular, that the square of any ideal is principal. Indeed,

$$(2, 1 + \sqrt{5})^2 = (4, 2 + 2\sqrt{-5}, 6) = (2).$$

Finally we solve the equation:

Theorem 5.1. *The equation*

$$X^3 = Y^2 + 5$$

admits no solutions $X, Y \in \mathbf{Z}$.

Proof. From the discussion above and the uniqueness of ideal factorization we conclude that the ideal

$$(Y + \sqrt{-5})$$

is the cube of a $\mathbf{Z}[\sqrt{-5}]$-ideal I. Therefore the cube of the class of I is trivial in the class group. Since the class group has order 2, which is prime to 3, this means that the class of

I itself is trivial. In other words, I is principal. Since the only units of $\mathbf{Z}[\sqrt{-5}]$ form the group $\{\pm 1\}$ of order 2, we conclude that

$$\begin{aligned} Y + \sqrt{-5} &= (a + b\sqrt{-5})^3, \\ &= (a^3 - 3 \cdot 5ab^2) + (3a^2b - 5b^3)\sqrt{-5}. \end{aligned}$$

This implies that $b(3a^2 - 5b^2) = 1$ and therefore that $b = \pm 1$ and $3a^2 = \pm 1 + 5$. Since this equation has no solution $a \in \mathbf{Z}$, we conclude that there is no solution in integers $X, Y \in \mathbf{Z}$ of the original equation, as required.

Bibliography

[1] Borevič, Z. and Shafarevič, I.: *Number Theory*, Academic Press, London 1966.

[2] Ono, T.: *An introduction to algebraic number theory*, Plenum Press, New York 1990.

[3] Samuel, P.: *Théorie algebrique des nombres*, Hermann, Paris 1971.

[4] Stewart, I.N. and Tall, D.O.: *Algebraic number theory*, Chapman and Hall, London 1987.