Solving Diophantine Equations by Factoring in Number Fields

Pezlar Z., J. ASB Soc., 2021, 2(1), 29-34
DOI:10.51337/JASB20211227004

Supporting information

Applications of quadratic residues

Recall a non-zero element $a \in \mathbb{Z}_p$ has an inverse, reason being the set $\{a, 2a, \dots, (p-1)a\}$ reduced modulo p is the set of non-zero residues modulo p, since $ka \equiv \ell a \pmod{p}$ implies $(k-\ell)a$ is zero in $\mathbb{Z}_p$, hence $k = \ell$. In particular, there exists an element $\frac{1}{a} \in \mathbb{Z}_p$ such that $\frac{1}{a} \cdot a = 1$ in $\mathbb{Z}_p$.

Example 1. Let $p \equiv 3 \pmod 4$ be a prime and a, b integers, such that $p \mid a^2 + b^2$. Show that $p \mid a$ and $p \mid b$.

Proof. Assuming p doesn't divide a or b, it doesn't divide either. We are given $a^2 \equiv -b^2 \pmod{p}$ and $p \nmid b$, so multiplying the congruence by $\frac{1}{b^2}$:

$$\left(\frac{a}{b}\right)^2 \equiv -1 \pmod{p}.$$

It follows that -1 is a quadratic residue modulo p. Thus, for $p \equiv 3 \pmod{p}$ we have $1 = \left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$, whereas the last expression is equal to -1, a contradiction. We conclude $p \mid a$ and $p \mid b$. □

Example 2. Solve the equation $x^2 + 4 = y^5$ in integers.

Proof. We are looking for a solution using quadratic residues. With that in mind, notice $5 = \frac{11-1}{2}$, i.e $y^5 \equiv \left(\frac{y}{11}\right) \in \{\pm 1, 0\} \pmod{11}$. For each of these values of y^5 we calculate $x^2 \in \{6, 7, 8\} \pmod{11}$.

Now we show the equation has no integer solutions. It suffices to show none of the three congruences $x^2 \equiv 6, 7, 8 \pmod{11}$ has a solution. This a computation:

$$\left(\frac{6}{11}\right) \equiv 6^5 \equiv -1 \pmod{11},$$
$$\left(\frac{7}{11}\right) \equiv 7^5 \equiv -1 \pmod{11},$$
$$\left(\frac{8}{11}\right) \equiv 8^5 \equiv -1 \pmod{11},$$

so the equation has no solutions. □

We now leave a problem for the reader to try out on their own.

Problem 1. Solve the equation $x^2 + 2 = y^9$ in integers.

Diophantine equations solved via algebraic number theory

Let's look back at Example no. 2., but this time, we will be factoring over the ring of Gaussian integers $\mathbb{Z}[i]$. We will then expand this method further in Problem 3.

Problem 2. Solve the following equation over the integers:

$$x^2 + 4 = y^5. \tag{♠}$$

Proof. Assume (x, y) satisfies the above equation. Firstly, we see x, y have the same parity. If x, y had a common prime divisor p, the equation would imply $p^2 \mid 4$, hence $p = 2$. Then $x = 2x_1$ and $y = 2y_1$ for integers x_1, y_1 and so:

$$x_1^2 + 1 = 8y_1^5,$$

which implies $x_1^2 \equiv -1 \pmod 4$, a contradiction, since -1 is a quadratic non-residue modulo 4. The numbers x, y and therefore coprime, which we will use to prove certain ideals are coprime too.

Now we factor the left hand side of (♠) in $\mathbb{Z}[i]$ as follows:

$$(x + 2i)(x - 2i) = y^5.$$

This, in particular, means the ideals generated by both sides are equal. Theorem **??** then states:

$$(x + 2i)(x - 2i) = \Big((x + 2i)(x - 2i)\Big) = \big(y^5\big) = (y)^5,$$

as an equality of ideals. Now we would like to show the ideals generated by $x+2i$ and $x-2i$ are coprime. Assume, on the contrary, a prime ideal $\mathcal{P}$ diving both $(x + 2i)$ and $(x - 2i)$ exists. Theorems **??**, **??** and the multiplicativity of norms imply:

$$\mathcal{P} \mid (4i) \Rightarrow N(\mathcal{P}) \mid N((4i)) = |N(4i)| = 16.$$

A prime $p \in \mathcal{P}$ satisfies $p^j = N(\mathcal{P}) \mid 16$ for some j, so $p = 2$. On the other hand, $\mathcal{P}$ divides $(x + 2i)$, and so $2 \mid N(\mathcal{P}) \mid N((x + 2i)) = x^2 + 4$. This shows x is even, a contradiction.

The product of coprime ideals $(x + 2i), (x - 2i)$ is a fifth power of the ideal generated by y, therefore theorem **??** says both of them are fifth powers. We arrive at the existence of an ideal $\mathcal{I} \subseteq \mathcal{O}_K$ such that $(x + 2i) = \mathcal{I}^5$.

The command:

```
NumberFieldClassNumber[Sqrt[-1]]
```

in Wolfram Mathematica gives $h_{\mathbb{Q}(i)} = 1$, so $\mathbb{Z}[i]$ has unique factorisation into irreducible elements. Any ideal of $\mathbb{Z}[i]$ is then principal, or $\mathcal{I}$ is generated by some Gaussian integer $a + bi$:

$$(x + 2i) = \mathcal{I}^5 = (a + bi)^5 = \Big((a + bi)^5\Big),$$

which is once again a consequence of **??**. The ring $\mathbb{Z}[i]$ is an integral domain, theorem **??** therefore says the quotient of $x + 2i$ and $(a + bi)^5$ is a unit in $\mathbb{Z}[i]$.

Units $a + bi \in \mathbb{Z}[i]$ are Gaussian integers with:

$$\pm 1 = N(a + bi) = a^2 + b^2,$$

so $(a, b) \in \{(\pm 1, 0), (0, \pm 1)\}$ and the units are only the following: $1, -1, i, -i$. Hence:

$$x + 2i = u(a + bi)^5$$

for some $u \in \{\pm 1, \pm i\}$. We could, without a doubt, go through all four units and find integers solutions, however, we can reduce our workload substantially. Notice any solution (a, b) for x and $u = -1, i, -i$ gives a solution for $u = 1$ with the pairs $(-a, -b), (-b, a)$ and $(b, -a)$ respectively. With no generality lost, we may assume $u = 1$, since every integer x solving the original equation gives rise to a solution (a, b).

Then:

$$x + 2i = (a + bi)^5 = a^5 - 10a^3b^2 + 5ab^4 + i(5a^4b - 10a^2b^3 + b^5).$$

Numbers 1 and i are linearly independent over the rationals, even over $\mathbb{R}$, so the real and imaginary parts of both sides, respectively, must be equal. The imaginary part gives us:

$$2 = 5a^4b - 10a^2b^3 + b^5 = b(5a^4 - 10a^2b^2 + b^4).$$

We have $b \mid 2$, or $b \in \{\pm 1, \pm 2\}$. Any of these cases results in a quadratic equation in a^2 with no integral solutions for a.

No x such that $x + 2i$ is fifth power of a Gaussian integers exists, so the equation (♠) has no integral solutions. ■

We have seen how to prove a equation has no integral solutions and how to work in the ring $\mathbb{Z}\left[\sqrt{d}\right]$, although if the equation had solutions, the last step would simply cough up solutions for a, b and, in turn, for x and y. Now, we will put the ideal class group to work:

Problem 3. Find all integers x, y satisfying:

$$x^2 + 13 = y^3. \tag{♣}$$

Proof. Let (x, y) be a solution. We see x, y are coprime and of a different parity. If y were even, $x^2 \equiv -1 \pmod 4$ would hold, which is nonsense. We are then left with x being even and y odd. Factoring in $\mathbb{Z}\left[\sqrt{-13}\right]$ gives:

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

which can be, due to theorem **??**, expressed as an equality of ideals in $\mathbb{Z}\left[\sqrt{-13}\right]$:

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

The product of the ideals on the left hand side is a third power. We want to once again show these ideals are coprime. Rather, assume a prime ideal $\mathcal{P}$ divides both. The norm being multiplicative and theorem **??** give:

$$\mathcal{P}\mid\left(x\pm\sqrt{-13}\right)\Rightarrow N(\mathcal{P})\mid x^2+13=y^3.$$

In spite of that, theorem **??** states:

$$\mathcal{P}\mid\left(2\sqrt{-13}\right)\Rightarrow N(\mathcal{P})\mid N\left(\left(2\sqrt{-13}\right)\right)=4\cdot 13.$$

We know y is odd a if 13 were to divide y, then x would be divisible by 13 as well, a contradiction. The ideals $\left(x\pm\sqrt{-13}\right)$ are coprime then, so their product is a third power. This means the existence of an ideal $\mathcal{I}\subseteq\mathbb{Z}\left[\sqrt{-13}\right]$ such that $\mathcal{I}^3$ is equal to the ideal $\left(x+\sqrt{-13}\right)$, in particular a principal ideal.

This is the part where the ideal class group shows up. The command:

```
NumberFieldClassNumber[Sqrt[-13]]
```

reveals the class group of $\mathbb{Z}\left[\sqrt{-13}\right]$ as having two elements, the ring does not have unique factorisation. From theorem **??** a square of any ideal of $\mathbb{Z}\left[\sqrt{-13}\right]$ is principal. Since 3 is relatively prime to 2 and the product of principal ideals in principal, the ideal $\mathcal{I}$ is a principal ideal generated by a single element of $\mathbb{Z}\left[\sqrt{-13}\right]$, which is $a+b\sqrt{-13}$ for some integers a,b. Once again, theorem **??** states:

$$\left(x+\sqrt{-13}\right)=\left(a+b\sqrt{-13}\right)^3=\left(\left(a+b\sqrt{-13}\right)^3\right),$$

as an equality of principal ideals in our ring. Theorem **??** states the quotient of $x+\sqrt{-13}$ and $\left(a+b\sqrt{-13}\right)^3$ is a unit in $\mathbb{Z}\left[\sqrt{-13}\right]$, in other words ± 1. Furthermore, a suitable triple (x,a,b) with the unit being -1 gives a triple $(x,-a,-b)$ for the unit being 1. We can without loss of generality assume:

$$x+\sqrt{-13}=\left(a+b\sqrt{-13}\right)^3. \qquad (\diamond)$$

Numbers 1 and $\sqrt{-13}$ are linearly independent over $\mathbb{Q}$ and $\mathbb{R}$, so the real and imaginary parts are equal. Comparing coefficients of $\sqrt{-13}$ bears fruits:

$$b(3a^2-13b^2)=1,$$

since this implies $b\mid 1$ and so $b\in\{\pm 1\}$. We can then easily find all solutions $(a,b)=(\pm 2,-1)$, and the rational part gives of $(\diamond)$ gives $x\in\{\pm 70\}$. The original equation then gives all possible solutions $(\pm 70,17)$. Any other x can not satisfy our equation, so we are done. ■

We solved the two equations by factoring in rings of the type $\mathbb{Z}\left[\sqrt{d}\right]$, however working in rings $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ is not too different from the methods we have shown here and all important differences have been mentioned. The reader can try solving the following equation by factoring in such a ring:

Problem 4. Solve the following equation in integers:

$$x^2 + 11 = y^3,$$

if it is given that the ring $\mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$ is a Dedekind domain.

I wish you a pleasant solving experience!