$x^2+3y^2=p$

math center

Today we do a basic exercise in algebraic number theory while also take note of some results and the chains of logic involved.

Let p be a prime number. We wish to find integral solutions to the equation

$$x^2 + 3y^2 = p. \tag{1}$$

This is the same as

$$\mathrm{Nm}\left(x + \sqrt{-3}y\right) = \left(x + \sqrt{-3}y\right)\left(x - \sqrt{-3}y\right) = p.$$

By considering the norm ($\mathrm{Nm}(p) = p^2$), we see that such a solution exists if and only if p is reducible in $\mathbb{Z}[\sqrt{-3}]$.

Let $K = \mathbb{Q}(\sqrt{-3})$. Its ring of integers is known by the following result:

Proposition 0.1. Let $K = \mathbb{Q}(\sqrt{m})$ for a square-free $m \neq 1$, then the ring of integers and the discriminant are given by

- If $m \equiv 2, 3 \pmod 4$, then $O_K = \mathbb{Z}[\sqrt{m}]$ and $\mathrm{disc}(O_K|\mathbb{Z}) = 4m$.
- If $m \equiv 1 \pmod 4$, then $O_K = \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$ and $\mathrm{disc}(O_K|\mathbb{Z}) = m$.

Proof. In either case, we have

$$D(1, \sqrt{m}) = (O_K : \mathbb{Z}[\sqrt{m}])^2 \,\mathrm{disc}(O_K|\mathbb{Z}),$$

which can be easily computed as

$$D(1, \sqrt{m}) = \begin{vmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\sqrt{m}) \\ \mathrm{Tr}(\sqrt{m}) & \mathrm{Tr}(m) \end{vmatrix} = 4m.$$

So we have $(O_K : \mathbb{Z}[\sqrt{m}]) \in \{1, 2\}$. To conclude the proof, we note that

- Stickelberger's theorem states that $\mathrm{disc}(O_K|\mathbb{Z}) \equiv 0, 1 \pmod 4$, so if $m \equiv 2, 3 \pmod 4$, we must have $(O_K : \mathbb{Z}[\sqrt{m}]) = 2$.
- On the other hand, if $m \equiv 1 \pmod 4$, the polynomial $X^2 - X + \frac{1-m}{4}$ has integral coefficients and has $\frac{1+\sqrt{m}}{2} \notin \mathbb{Z}[\sqrt{m}]$ as a root.

This completes the proof. □

Since $m = -3$, we have the second scenario, and $O_K = \mathbb{Z}[\omega]$ where $\omega^3 = 1$.

Theorem 0.2. Let A be a Dedekind domain with field of fractions K. If the integral closure B of A in a finite separable extension $L|K$ satisfies $B = A[\alpha]$, then the factorization of any prime ideal $\mathfrak{p}$ of A can be determined as follows. Factorize the mininal polynomial f of α into distinct irreducibles $g_i \in A[X]$ modulo $\mathfrak{p}$, i.e.

$$f \equiv \prod_i g_i^{e_i} \pmod{\mathfrak{p}}, \quad e_i > 0.$$

Then we have

$$\mathfrak{p}B = \prod_i (\mathfrak{p}, g_i(\alpha))^{e_i}$$

is the factorization of $\mathfrak{p}B$ into distinct prime ideals.

Proof. $B/\mathfrak{p}B \simeq B \otimes A/\mathfrak{p} \simeq A[X]/(f) \otimes A/\mathfrak{p} \simeq (A/\mathfrak{p})[X]/(\bar{f})$. The ideal $\mathfrak{p}B$ is uniquely determined by this quotient because (a) its prime factors are precisely the prime ideals in the quotient, and (b) the ramification index e of each factor $\mathfrak{P}$ is the largest number such that $\mathfrak{P}^e \neq 0$. □

If we don't have $B = A[\alpha]$, we can still apply this result for some $\mathfrak{p}$ and α. Write

$$\operatorname{disc}(1, \alpha, \cdots, \alpha^{n-1}) = \mathfrak{a} \cdot \operatorname{disc}(B|A).$$

If $\mathfrak{p} \nmid \mathfrak{a}$, then we can invert any element in $\mathfrak{a} \setminus \mathfrak{p}$, or what is the same, localize at $\mathfrak{p}$. Then $B_\mathfrak{p} = A_\mathfrak{p}[\alpha]$, and the same result holds.

1 The solution

Back to the problem. We have $A = \mathbb{Z}$, $\mathfrak{p} = (p)$, $B = \mathbb{Z}[\omega]$. If $p = 2$, we can't apply the previous result, but obviously (1) has no solution. From now on let $p \neq 2$.

From the above discussion, (p) splits/ramifies in B if and only if $f(X) = X^2 + 3$ is reducible modulo p. We have the following chain of implications.

$$\begin{aligned}
&(1) \text{ has a solution} \\
\implies &(p) \text{ splits/ramifies in } B \\
\iff &X^2 + 3 \text{ is reducible in } (\mathbb{Z}/(p))[X] \\
\iff &-3 \text{ is a square modulo } p \\
\iff &p \text{ is a square modulo } 3 \qquad (\heartsuit) \\
\iff &p \equiv 0, 1 \pmod 3
\end{aligned}$$

where, in the line (♡), we used the well-known quadratic reciprocity:

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}\cdot 1} = \left(\frac{p}{3}\right).$$

It remains to prove the converse of the first $\implies$. First, note that

Lemma 1.1. $\mathbb{Z}[\omega]$ is a PID.

Proof. It is well known that the number field $\mathbb{Q}[\sqrt{-3}]$ has class number 1. See section 3. □

Hence, if (p) splits/ramifies in B, it must be the principal ideal generated by the product of two irreducibles in B, and hence must take the form

$$(u + v\omega)(u + v\overline{\omega}) = p,$$

where $u, v \in \mathbb{Z}$. Side note: LHS $= u^2 - uv + v^2$.

Finally, we must check that up to a unit $\mathbb{Z}[\omega]^\times = \langle -1, \omega \rangle$, $u + v\omega \overset{!}{\sim} x + y\sqrt{-3}$. Indeed,

- If v is even, there is nothing to prove;
- If u is even and v is odd, $\omega^2(u+v\omega) = v + u\overline{\omega} \in \mathbb{Z}[\sqrt{-3}]$;
- If u, v are both odd, then $\omega(u+v\omega) = \frac{\left((u+v)+(u-v)\sqrt{-3}\right)}{2} \in \mathbb{Z}[\sqrt{-3}]$.

This completes the proof. □

2 Fermat

According to Milne, this result we just proved

$$(1) \text{ has a solution} \iff p \equiv 0, 1 \pmod 3$$

was (probably) proven by Fermat himself. It is unlikely that he took the above approach—and he didn't really need to. We shall now sketch a proof using his method of infinite descent.

Only the $\Longleftarrow$ direction deserves a proof. Also assume that $p > 3$. First, we solve (1) modulo p. This amounts to solving

$$\left(\frac{x}{y}\right)^2 \equiv -3 \pmod p.$$

Even without QR, it is possible to observe that such solution must exist if $p \equiv 1 \pmod 3$. As hinted by the above manipulations, we have

$$\begin{aligned} & (u/v)^3 \equiv 1, \quad u \not\equiv v \pmod p \\ \Longrightarrow\ & u^2 - uv + v^2 \equiv 0 \pmod p \\ \Longrightarrow\ & (2u - v)^2 \equiv -3v^2 \pmod p. \end{aligned}$$

Now, let $x, y \in \mathbb{Z}$, $k \in \mathbb{Z}_{>0}$ be such that

$$x^2 + 3y^2 = kp$$

and k is minimal among all such triples (x, y, k). Let u, v be integers with smallest absolute value which satisfy

$$u \equiv x, \quad v \equiv y \pmod k.$$

Let $u^2 + 3v^2 = k'k$. Clearly, assuming that $k > 1$, we have $k' > 0$.

Note an equivalent formulation of multiplicity of the norm

$$(x^2 + 3y^2)(u^2 + 3v^2) = (xu + 3yv)^2 + 3(xv - yu)^2.$$

Since both $xu + 3yv$ and $xv - yu$ are divisible by k, we have

$$k'p = \left(\frac{xu + 3yv}{k}\right)^2 + 3\left(\frac{xv - yu}{k}\right)^2.$$

However,

$$k'k = u^2 + 3v^2 \le 4\left(\frac{k}{2}\right)^2 = k^2.$$

Thus we have $k' \le k$, and so $k' = k$ by the minimality of k. This is only possible if both $|u| = |v| = k/2 \in \mathbb{Z}$ and $k = p$, which is absurd.

Hence, it must be that $k = 1$. □

3 Appendix: quadratic number fields of class number 1

Suppose that $-d = 1, 2, 3, 7, 11, 19, 43, 67, 163$. It is well-known that $K := \mathbb{Q}[\sqrt{d}]$ has class number $h = 1$, i.e. O_K is a PID. Let's see why this is true.

Of course, we have to start examining each case by finding the ring of integers using Proposition 0.1. We will also need the following result for reducing the number of primes to check into a very managable, finite number.

Definition 3.1. Let K be an degree n extension of $\mathbb{Q}$, and let $2s$ be the number of nonreal complex embeddings $K \hookrightarrow \mathbb{C}$. Then the *Minkowski bound* is given by

$$B_K = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s .$$

Theorem 3.2. Under the same assumptions as above, there exists a representative $\mathfrak{a}$ for each element of the class group $\mathrm{Cl}(K)$, satisfying

$$\mathbb{N}(\mathfrak{a}) = |\mathcal{N}(\mathfrak{a})| \leq B_K \left|\Delta\right|^{\frac{1}{2}} ,$$

where Δ_K is the discriminant of $O_K|\mathbb{Z}$.

Proof.(sketch). $\mathfrak{a}$ embeds into $\mathbb{R}^{n-2s} \oplus \mathbb{C}^s \simeq \mathbb{R}^n$ as a full lattice. Denote its fundamental parallelopiped as D. We should be able to see that

$$\mu(D) = 2^{-s} \cdot \mathbb{N}\mathfrak{a} \cdot \left|\Delta_K\right|^{\frac{1}{2}} .$$

Then, by Minkowski's theorem, there exists an $\alpha \in \mathfrak{a}$ whose image in $\mathbb{R}^n$ has coordinates controlled by this number. The result then follows from this. □

In our case, we always have a imaginary quadratic field, so $B_K = \frac{1}{2} \cdot \frac{4}{\pi} \leq 0.637$.

3.1 $d = -1$

$O_K = \mathbb{Z}[\sqrt{-1}]$. This is a Euclidean domain.

3.2 $d = -2$

$O_K = \mathbb{Z}[\sqrt{-2}]$ and $\Delta_K = -8$. We only need to consider primes (in $\mathbb{Z}$) that are $\leq B_K \left|\Delta_K\right|^{1/2} \leq 1.81$. There are none, so we have nothing to check.

3.3 $d = -3$

$O_K = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ and $\Delta_K = -3$. As $B_K \left|\Delta_K\right|^{1/2} \leq 1.11$, we have nothing to check.

3.4 $d = -7$

$O_K = \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ and $\Delta_K = -7$. As $B_K \left|\Delta_K\right|^{1/2} \leq 1.69$, we have nothing to check.

3.5 $d = -11$

$O_K = \mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$ and $\Delta_K = -11$. We have $B_K \left|\Delta_K\right|^{1/2} \leq 2.12$.

- $p = 2$. The factorization of p in O_K is equivalent to the factorization of $X^2 - X + 3 \equiv X^2 + X + 1 \pmod 2$, which is clearly irreducible. That is, the prime 2 is inert in O_K.

3.6 $d = -19$

$O_K = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ and $\Delta_K = -19$. We have $B_K \left|\Delta_K\right|^{1/2} \leq 2.78$.

- $p = 2$. $X^2 - X + 5 \equiv X^2 + X + 1 \pmod 2$ is irreducible, so the prime 2 is inert.

3.7 $d = -43$

$O_K = \mathbb{Z}[\frac{1+\sqrt{-43}}{2}]$ and $\Delta_K = -43$. We have $B_K \left|\Delta_K\right|^{1/2} \leq 4.18$.

- $p = 2$. $X^2 - X + 11 \equiv X^2 + X + 1 \pmod 2$ is irreducible, so the prime 2 is inert.
- $p = 3$. $X^2 - X + 11 \equiv X^2 - X - 1 \pmod 3$ is irreducible, so the prime 3 is inert.

3.8 $d = -67$

$O_K = \mathbb{Z}[\frac{1+\sqrt{-67}}{2}]$ and $\Delta_K = -67$. We have $B_K \left|\Delta_K\right|^{1/2} \leq 5.22$.

- $p = 2$. $X^2 - X + 17 \equiv X^2 + X + 1 \pmod 2$ is irreducible, so the prime 2 is inert.
- $p = 3$. $X^2 - X + 17 \equiv X^2 - X - 1 \pmod 3$ is irreducible, so the prime 3 is inert.
- $p = 5$. $X^2 - X + 17 \equiv X^2 - X - 3 \pmod 5$ is irreducible, so the prime 5 is inert.

3.9 $d = -163$

$O_K = \mathbb{Z}[\frac{1+\sqrt{-163}}{2}]$ and $\Delta_K = -163$. We have $B_K \left|\Delta_K\right|^{1/2} \leq 8.14$.

- $p = 2$. $X^2 - X + 41 \equiv X^2 + X + 1 \pmod 2$ is irreducible, so the prime 2 is inert.
- $p = 3$. $X^2 - X + 41 \equiv X^2 - X - 1 \pmod 3$ is irreducible, so the prime 3 is inert.
- $p = 5$. $X^2 - X + 41 \equiv X^2 - X + 1 \pmod 5$ is irreducible, so the prime 5 is inert.
- $p = 7$. $X^2 - X + 41 \equiv X^2 - X - 1 \pmod 7$ is irreducible, so the prime 7 is inert.

Remark 3.3. To prove irreducibility of $X^2 - X + \frac{1-d}{4}$ modulo an *odd* prime p, instead of checking every element of $\mathbb{F}_p$, it is easier to show that Δ_K is not a square modulo p, i.e., that

$$\left(\frac{\Delta_K}{p}\right) = -1.$$

Final remark: In 1952, Heegner proved that this list exhausts all imaginary quadratic number fields with class number 1.

The End

Compiled on 2025/10/14.
Home page