Algebraic Number Theory – Lecture 7

Lee Butler

A mathematician, an engineer, and a chemist are staying in adjoining rooms in a hotel. One evening they are downstairs in the bar. The mathematician goes to bed first. The chemist goes next, followed a minute later by the engineer. The chemist notices that in the corridor outside their rooms a rubbish bin is ablaze. There is a bucket of water nearby. The chemist starts concocting a means of generating carbon dioxide in order to create a makeshift extinguisher but before he can do so the engineer arrives, dumps the water on the fire and puts it out. The next morning the chemist and engineer tell the mathematician about the fire. She admits she saw it. They ask her why she didn't put it out. She replies contemptuously "There was a fire and a bucket of water: a solution obviously existed."

1. Exampletastic recappery

So far we've been introduced to algebraic numbers and rings of integers; we've seen ideals and how they uniquely factorise, even when the underlying integers don't; and we've learnt about the embeddings of a number field into the complex numbers. We've only scratched the surface of algebraic number theory, yet I decided it'd be nice to see some number theoretical results that we can already prove. I'll only use results stated or proved in the previous six lectures (as well as standard algebra and number theory).

Theorem 1. *A prime number $p > 2$ is expressible as the sum of two squares if and only if $p \equiv 1 \pmod 4$.*

Proof. To see the condition is necessary just consider the quadratic residues mod 4. For sufficiency we factor the equation

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

over the number field $\mathbb{Q}(i)$ as

$$p = (x + iy)(x - iy).$$

So the question becomes: when does a prime $p \in \mathbb{Z}$ factorise in the ring $\mathbb{Z}[i]$?

Since $-1 \not\equiv 1 \pmod 4$ we know from L4 Thm S3 that $\mathbb{Z}[i]$ is the ring of integers in $\mathbb{Q}(i)$. We'll show that $\mathbb{Z}[i]$ is a Euclidean domain, and hence a unique factorisation domain.

By L3 Thm 1, $[\mathbb{Q}(i):\mathbb{Q}]=2$, and indeed the embeddings $\mathbb{Q}(i)\hookrightarrow\mathbb{C}$ are

$$\sigma_1 : x+iy \mapsto x+iy$$
$$\sigma_2 : x+iy \mapsto x-iy.$$

So the norm of $a+bi\in\mathbb{Q}(i)$ is

$$N(a+bi)=\prod_{j=1}^{2}\sigma_j(a+bi)=a^2+b^2.$$

We'll show $\mathbb{Z}[i]$ is Euclidean with respect to this norm. Let $\alpha,\beta\in\mathbb{Z}[i]$, $\beta\neq 0$. We need to show there exist $\gamma,\rho\in\mathbb{Z}[i]$ such that

$$\alpha=\gamma\beta+\rho, \qquad N(\rho)<N(\beta).$$

That is, we need $\gamma\in\mathbb{Z}[i]$ such that

$$N\left(\frac{\alpha}{\beta}-\gamma\right)<1.$$

Let $\alpha/\beta=u+vi\in\mathbb{Q}(i)$ and let $u',v'\in\mathbb{Z}$ be the closest integers to u and v respectively. So $|u-u'|\leqslant 1/2$, $|v-v'|\leqslant 1/2$, and if $\gamma=u'+v'i$ then

$$\begin{aligned} N\left(\frac{\alpha}{\beta}-\gamma\right) &= N(u-u'+(v-v')i) \\ &= (u-u')^2+(v-v')^2 \\ &\leqslant \frac{1}{2}<1. \end{aligned}$$

So $\mathbb{Z}[i]$ is a Euclidean domain, hence a principal ideal domain, hence a unique factorisation domain. We want to show that if $p\equiv 1 \pmod 4$ then p is not a prime in $\mathbb{Z}[i]$. Having proved this we'll know there are non-units $\alpha,\beta\in\mathbb{Z}[i]$ such that $p=\alpha\beta$. Then

$$N(p)=N(\alpha)N(\beta)$$

i.e.

$$p^2=N(\alpha)N(\beta).$$

Since α,β aren't units we must have $N(\alpha)=N(\beta)=p$. If $\alpha=a+bi$ we'll then have

$$a^2+b^2=p$$

as required.

So we just have to show that $p=4n+1$ isn't prime in $\mathbb{Z}[i]$ Note first that -1 is a quadratic residue mod p since $p\equiv 1 \pmod 4$. So $-1\equiv x^2 \pmod p$ for some x, hence

$$p \mid x^2+1=(x+i)(x-i).$$

But $\frac{x}{p}\pm\frac{i}{p}\notin\mathbb{Z}[i]$ so p doesn't divide either factor on the right in $\mathbb{Z}[i]$. But in a unique factorisation domain every prime that divides a product must divide one of the factors. Hence p is not a prime in $\mathbb{Z}[i]$, which is what we wanted. $\square$

Lemma 1. *Let $d > 0$ be square-free and $K = \mathbb{Q}(\sqrt{-d})$. The only units in $\mathcal{O}_k$ are:*

$$\begin{cases} \{\pm 1, \pm i\} & \text{if } d = 1 \\ \{\pm 1, \pm\omega, \pm\omega^2\} & \text{if } d = 3 \\ \{\pm 1\} & \text{for all other } d > 0. \end{cases}$$

Proof. Suppose $\alpha = a + b\sqrt{-d}$ is a unit in $\mathcal{O}_k$. So $N(\alpha)N(\beta) = 1$ for some β. From L3 we know $N(\alpha) \in \mathbb{Z}$ and also that $N(a + b\sqrt{-d}) = a^2 + db^2 > 0$, so $N(\alpha) = 1$. Thus we need to solve

$$a^2 + db^2 = 1.$$

If $d = 1$ then $a, b \in \mathbb{Z}$ so we get $a = \pm 1$, $b = 0$ or $a = 0$, $b = \pm 1$, giving the stated units.

If $d = 2$ then $a, b \in \mathbb{Z}$ so the only solutions are $a = \pm 1$ and $b = 0$.

If $d > 3$ then either $a, b \in \mathbb{Z}$ or $a, b \in \frac{1}{2}\mathbb{Z}$. Either way $a = \pm 1$ and $b = 0$ else $a^2 + db^2 \geqslant db^2 > 1$.

If $d = 3$ then $a, b \in \frac{1}{2}\mathbb{Z}$. If $b = 0$ we get $a = \pm 1$, but we could also have $a = A/2$, $b = B/2$ for odd integers A, B. Then

$$A^2 + 3B^2 = 4,$$

which has solutions $A = \pm 1$, $B = \pm 1$. The four combinations of sign give $\pm\omega$ and $\pm\omega^2$. □

While the above result is of mild interest in itself, it does allow us to prove the following surprising result.

Theorem 2. *Only finitely many imaginary quadratic fields are Euclidean.*

Proof. Let $\psi : \mathcal{O}_k \to \mathbb{Z}$ be a norm for $\mathcal{O}_k$. (So for every $a, b \neq 0$ in $\mathcal{O}_k$ there exist $q, r \in \mathcal{O}_k$ such that $a = qb + r$ and $\psi(r) < \psi(b)$.) Let $\alpha \in \mathcal{O}_k$ be a non-unit have minimal nonzero norm and consider the residue classes of $\mathcal{O}_k$ modulo α. Each class can be represented either by 0 or by an element r with $\psi(r) < \psi(\alpha)$, since for any $\beta \in \mathcal{O}_k$ we may write

$$\beta = q\alpha + r \in r + \alpha\mathcal{O}_k$$

with $\psi(r) < \psi(\alpha)$. In particular either $r = 0$ or r is a unit by the choice of α. For $d > 11$ we know the ring of integers of $\mathbb{Q}(\sqrt{-d})$ only has the units ± 1 so for every $\beta \in \mathcal{O}_k$

$$\beta \equiv -1, 0, \text{ or } 1 \pmod{(\alpha)}.$$

Thus $|\mathcal{O}_k/(\alpha)| \leqslant 3$. By L6 Thm 2 we know

$$|\mathcal{O}_k/(\alpha)| = N((\alpha)) = |N(\alpha)|,$$

so $|N(\alpha)| \leqslant 3$. But if $\alpha = a + b\sqrt{d}$ then $N(\alpha) = a^2 + db^2$.

If $d \equiv 1 \pmod 4$ then we need $|a^2 + db^2| \leqslant 3$ with $a, b \in \mathbb{Z}$.

If $d \not\equiv 1 \pmod 4$ then we need $|a^2 + db^2| \leqslant 3$ with $a = A/2, b = B/2$ and $A, B \in \mathbb{Z}$.

The restriction $d > 11$ forces $b = 0$ in all cases leading us solely to the solutions $a = \pm 1$ and thus $|N(\alpha)| = 1$, i.e. the realisation that α is a unit. But this contradicts the non-unityness of α, and so for $d > 11$ the ring of integers of $\mathbb{Q}(\sqrt{-d})$ cannot be Euclidean. □

In fact the only Euclidean imaginary quadratic fields are $\mathbb{Q}(\sqrt{-d})$ for

$$d = 1, 2, 3, 7, 11.$$

It is known which real quadratic fields are norm-Euclidean, i.e. Euclidean using the usual norm. But it is an open problem if there are any real quadratic fields that are Euclidean but not norm-Euclidean.