Day 16

Last day on quadratic rings

$\mathbb{Z}[\sqrt{2}]$ with norm $N(a+b\sqrt{2})$ given by the absolute value of a^2-2b^2.

- units in this ring come from $a^2-2b^2=\pm 1$. Compute $\pm 1+2b^2$ and look for squares. Or notice that $1+\sqrt{2}$ has norm 1 and consider all powers.

- the division algorithm for α and β is found by taking

$$\frac{\alpha}{\beta}=\frac{\alpha\overline{\beta}}{N(\beta)}=\frac{x}{N(\beta)}+\frac{y}{N(\beta)}\sqrt{2}$$

  where x and y are integers. Then choose the closest integers u and v to $x/N(\beta)$ and $y/N(\beta)$ respectively, so we can write

$$\frac{x}{N(\beta)}+\frac{y}{N(\beta)}\sqrt{2}=u+v\sqrt{2}+(r+s\sqrt{2})$$

  where r and s have absolute value at most $1/2$. Therefore the norm of $r+s\sqrt{2}$ is at most $3/4$.

Multiplying the expression for α/β through by β gives

$$\alpha=\beta(u+v\sqrt{2})+(r+s\sqrt{2})N(\beta)$$

and the remainder term has norm at most $3/4N(\beta)$.

- The prime p remains prime in $\mathbb{Z}[\sqrt{2}]$ if x^2-2 is irreducible mod p. This happens when 2 is a quadratic nonresidue mod p. The “supplement” to the law of quadratic reciprocity says this happens when p is not congruent to ± 1 mod 8. So for example 7 is not prime, it satisfies $7=(3-\sqrt{2})(3+\sqrt{2})$ but 11 is prime.

Remark: The ring $\mathbb{Z}[\sqrt{3}]$ is trickier; if you use the approach above you end up with $u+v\sqrt{3}$ with u and v at most $1/2$ in absolute value; but the norm of $1/2+\sqrt{3}/2$ is 1 which does not yield the necessary estimate, at least unless we are a bit more careful. In fact the remainder term is the absolute value of

$$N(\beta)((\frac{x}{N\beta}-u)^2-3(\frac{y}{N\beta}-v)^2).$$

The second term is the absolute value of the difference of two squares $A^2 - 3B^2$, which is at most the maximum of A^2 or $3B^2$ and is therefore at most $3/4$.

Finally we look at the imaginary ring $\mathbb{Z}[\rho]$ where $\rho = e^{2\pi i/3}$. Here there are finitely many units (6) and the key geometric observation is that the integer lattice is "small enough".