Chapter 16

$\mathbb{Z}[\sqrt{3}]$ and the Lucas-Lehmer test

16.1 The field $\mathbb{Q}(\sqrt{3})$

We have

$$\mathbb{Q}(\sqrt{3}) = \{x + y\sqrt{3} : x, y \in \mathbb{Q}\}.$$

The conjugate and norm of

$$z = x + y\sqrt{3}$$

are

$$\bar{z} = x - y\sqrt{3}, \ \mathcal{N}(z) = z\bar{z} = x^2 - 3y^2.$$

16.2 The ring $\mathbb{Z}[\sqrt{3}]$

Since $3 \not\equiv 1 \bmod 4$,

$$\mathbb{Z}(\mathbb{Q}(\sqrt{3})) = \mathbb{Q}(\sqrt{3}) \cap \bar{\mathbb{Z}} = \{m + n\sqrt{3} : m, n \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{3}].$$

16.3 The units in $\mathbb{Z}[\sqrt{3}]$

Evidently

$$\epsilon = 2 + \sqrt{3}$$

is a unit, since

$$\mathcal{N}(\epsilon) = 2^2 - 3 \cdot 1^2 = 1,$$

Theorem 16.1. *The units in* $\mathbb{Z}[\phi]$ *are the numbers*

$$\pm\epsilon^n \quad (n \in \mathbb{Z}),$$

where

$$\epsilon = 2 + \sqrt{3}.$$

Proof. We have to show that ϵ is the smallest unit > 1.

Suppose $\eta = m + n\sqrt{3}$ is a unit satisfying

$$1 < \eta \leq \epsilon.$$

Since $\mathcal{N}(\eta) = \eta\bar{\eta} = \pm 1$,

$$\bar{\eta} = m - n\sqrt{3} = \pm\eta^{-1} \in (-1, 1).$$

Hence

$$\eta - \bar{\eta} = 2n\sqrt{3} \in (0, 1 + \epsilon),$$

ie

$$0 < n < (3 + \sqrt{3})/2\sqrt{3} < 2.$$

Thus

$$n = 1.$$

But now

$$\begin{aligned} \mathcal{N}(\eta) = \pm 1 &\implies m^2 - 3 = \pm 1 \\ &\implies m = \pm 2. \end{aligned}$$

Since $-2 + \sqrt{3} < 0$, we conclude that $m = 2,\ n = 1$, ie

$$\eta = \epsilon.$$

□

16.4 Unique Factorisation

Theorem 16.2. $\mathbb{Z}[\sqrt{3}]$ *is a Unique Factorisation Domain.*

Proof. We hurry through the argument, which we have already given 3 times, for $\mathbb{Z}, \Gamma$ and $\mathbb{Z}[\phi]$.

Given $z, w \in \mathbb{Z}[\sqrt{3}]$ we write

$$\frac{z}{w} = x + y\sqrt{3} \quad (x, y \in \mathbb{Q}),$$

and choose the nearest integers m, n to x, y, so that

$$|x - m|, |y - m| \leq \frac{1}{2}.$$

Then we set

$$q = m + n\sqrt{3},$$

so that

$$\frac{z}{w} - q = (x - m) + (y - n)\sqrt{3},$$

and

$$\mathcal{N}(\frac{z - qw}{w}) = (x - m)^2 - 3(y - n)^2.$$

Now

$$-\frac{3}{4} \leq \mathcal{N}(\frac{z - qw}{w}) \leq \frac{1}{4}.$$

In particular,

$$|\mathcal{N}(\frac{z - qw}{w})| < 1,$$

ie

$$|\mathcal{N}(z - qw)| < |\mathcal{N}(w)|.$$

This allows the Euclidean Algorithm to be used in $\mathbb{Z}[\sqrt{3}]$, and as a consequence Eulid's Lemma holds, and unique factorisation follows. □

16.5 The primes in $\mathbb{Z}[\sqrt{3}]$

Theorem 16.3. *Suppose $p \in \mathbb{N}$ is a rational prime. Then*

1. *If $p = 2$ or 3 then p ramifies in $\mathbb{Z}[\sqrt{3}]$;*
2. *If $p \equiv \pm 1 \bmod 12$ then p splits into conjugate primes in $\mathbb{Z}[\sqrt{3}]$,*

$$p = \pm\pi\bar{\pi};$$

3. *If $p \equiv \pm 5 \bmod 12$ then p remains prime in $\mathbb{Z}[\sqrt{3}]$.*

Proof. To see that 2 ramifies, note that

$$(1+\sqrt{3})^2 = 2\epsilon,$$

where *epsilon* $= 2+\sqrt{3}$ is a unit. It is evident that $3 = \sqrt{3}^2$ ramifies.

Suppose $p \neq 2, 3$.

If p splits, say

$$p = \pi\pi',$$

then

$$\mathcal{N}(p) = p^2 = \mathcal{N}(\pi)\mathcal{N}(\pi').$$

Hence

$$\mathcal{N}(\pi) = \mathcal{N}(\pi') = \pm p.$$

Thus if $\pi = m + n\sqrt{3}$ then

$$m^2 - 3n^2 = \pm p.$$

In particular,

$$m^2 - 3n^2 \equiv 0 \bmod p.$$

Now

$$n \equiv 0 \bmod p \implies m \equiv 0 \bmod p \implies p \mid \pi,$$

which is impossible, Hence

$$a \equiv mn^{-1} \bmod p$$

satisfies

$$a^2 \equiv 3 \bmod p.$$

It follows that

$$\left(\frac{3}{p}\right) = 1.$$

Now suppose $p \equiv 5 \bmod 12$, ie $p \equiv 1 \bmod 4$, $p \equiv 2 \bmod 3$. By Gauss' Quadratic Reciprocity Law,

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

Similarly, if $p \equiv -5 \bmod 12$, ie $p \equiv 3 \bmod 4$, $p \equiv 1 \bmod 3$, then by Gauss' Quadratic Reciprocity Law,

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

So we see that p does not split in $\mathbb{Z}[\sqrt{3}]$ if $p \equiv \pm 5 \bmod 12$.

On the other hand, it follows in the same way that

$$p \equiv \pm 1 \bmod 12 \implies \left(\frac{3}{p}\right) = 1,$$

in which case we can find a such that

$$a^2 \equiv 3 \bmod p,$$

ie

$$p \mid (a^2 - 3) = (a - \sqrt{3})(a + \sqrt{3}).$$

If now p does *not* split then this implies that

$$p \mid a - \sqrt{3} \text{ or } p \mid a + \sqrt{3}.$$

But both these imply that $p \mid 1$, which is absurd. □

16.6 The Lucas-Lehmer test for Mersenne primality

Theorem 16.4. *If p is prime then*

$$P = 2^p - 1$$

is prime if and only if

$$\epsilon^{2^{p-1}} \equiv -1 \bmod P,$$

where

$$\epsilon = 2 + \sqrt{3}.$$

Proof. Suppose P is prime. Then

$$\epsilon^P \equiv 2^P + (\sqrt{3})^P,$$

since

$$P \mid \binom{r}{P}$$

for $r \neq 0, P$.

But

$$2^P \equiv 2 \bmod P$$

by Fermat's Little Theorem, while

$$(\sqrt{3})^{P-1} = 3^{\frac{P-1}{2}} \equiv \left(\frac{3}{P}\right) \bmod P$$

by Euler's criterion. Thus

$$\epsilon^P \equiv 2 + \left(\frac{3}{P}\right)\sqrt{3}.$$

Now

$$2^p \equiv (-1)^p \equiv -1 \bmod 3 \implies P \equiv 1 \bmod 3,$$

while

$$4 \mid 2^p \implies P \equiv -1 \bmod 4.$$

So by Gauss' Reciprocity,

$$\begin{aligned}\left(\frac{3}{P}\right) &= -\left(\frac{P}{3}\right)\\ &= -\left(\frac{1}{3}\right)\\ &= -1.\end{aligned}$$

Thus

$$\epsilon^P \equiv 2 - \sqrt{3} = \bar{\epsilon} = \epsilon^{-1}.$$

Hence

$$\epsilon^{P+1} \equiv 1 \bmod P,$$

ie

$$\epsilon^{2^p} \equiv 1 \bmod P.$$

Consequently,

$$\epsilon^{2^{p-1}} \equiv \pm 1 \bmod P.$$

We need a little trick to determine which of these holds; it is based on the observation that

$$(1+\sqrt{3})^2 = 4 + 2\sqrt{3} = 2\epsilon.$$

As before,

$$\begin{aligned}(1+\sqrt{3})^P &\equiv 1 + 3^{(P-1)/2}\sqrt{3} \bmod P\\ &\equiv 1 - \sqrt{3} \bmod P.\end{aligned}$$

But now

$$(1-\sqrt{3})(1+\sqrt{3}) = -2,$$

and so

$$1 - \sqrt{3} = -2(1 + \sqrt{3})^{-1}.$$

Thus

$$(1 + \sqrt{3})^{P+1} \equiv -2 \bmod P,$$

ie

$$(1 + \sqrt{3})^{2^p} \equiv -2 \bmod P,$$

ie

$$(2\epsilon)^{2^{p-1}} \equiv -2 \bmod P.$$

To deal with the powers of 2, note that by Euler's criterion

$$2^{(P-1)/2} \equiv \left(\frac{2}{P}\right) \bmod P.$$

Recall that

$$\left(\frac{2}{P}\right) = \begin{cases} 1 \text{ if } P \equiv \pm 1 \bmod 8, \\ -1 \text{ if } P \equiv \pm 1 \bmod 8. \end{cases}$$

In this case,

$$P = 2^p - 1 \equiv -1 \bmod 8.$$

Thus

$$2^{(P-1)/2} \equiv 1 \bmod P,$$

and so

$$2^{(P+1)/2} \equiv 2 \bmod P,$$

ie

$$2^{2^{p-1}} \equiv 2 \bmod P.$$

So our previous result simplifies to

$$\epsilon^{2^{p-1}} \equiv -1 \bmod P.$$

This was on the assumption that P is prime. Suppose now that P is not prime, but that the above result holds.

Then P has a prime factor $Q \le \sqrt{P}$. Also

$$\epsilon^{2^{p-1}} \equiv -1 \bmod Q.$$

It follows that the order of $\epsilon \bmod Q$ is 2^p.

But consider the quotient-ring

$$A = \mathbb{Z}[\sqrt{3}]/(Q).$$

This ring contains just Q^2 elements, represented by

$$m + n\sqrt{5} \quad (0 \le m, n < Q).$$

It follows that the group $A^\times$ of invertible elements contains $< Q^2$ elements. Hence any invertible element of A has order $< Q^2$, by Lagrange's Theorem. In particular the order or $\epsilon \bmod P$ is $< Q^2$. Accordingly

$$2^p < Q^2,$$

which is impossible, since

$$Q^2 \le P = 2^p - 1.$$

We conclude that P *is* prime. □

As with the weaker result in the last Chapter, there is a more computer-friendly version of the Theorem, using the fact that

$$\epsilon^{2^{p-1}} \equiv -1 \bmod P$$

can be re-written as

$$\epsilon^{2^{p-2}} + \epsilon^{-2^{p-2}} \equiv 0 \bmod P.$$

Let

$$s_i = \epsilon^{2^i} + \epsilon^{-2^i}$$

Then

$$\begin{aligned} s_i^2 &= \epsilon^{2^{i+1}} + 2 + \epsilon^{2^{-(i+1)}} \\ &= s_{i+1} + 2, \end{aligned}$$

ie

$$s_{i+1} = s_i^2 - 2.$$

Since

$$s_0 = \epsilon + \epsilon^{-1} = 4$$

it follows that $s_i \in \mathbb{N}$ for all i, with the sequence starting $4, 14, 194, \ldots$.

Now we can re-state our result.

Corollary 16.1. *Let the integer sequence s_i be defined recursively by*

$$s_{i+1} = s_i^2 - 2, \; s_0 = 4.$$

Then

$$P = 2^p - 1 \textit{ is prime} \iff P \mid s_{p-2}.$$