Chapter 15

$Q(\sqrt{5})$ and the golden ratio

15.1 The field $\mathbb{Q}(\sqrt{5})$

Recall that the quadratic field

$$\mathbb{Q}(\sqrt{5}) = \{x + y\sqrt{5} : x, y \in \mathbb{Q}\}.$$

Recall too that the conjugate and norm of

$$z = x + y\sqrt{5}$$

are

$$\bar{z} = x - y\sqrt{5}, \ \mathcal{N}(z) = z\bar{z} = x^2 - 5y^2.$$

We will be particularly interested in one element of this field.

Definition 15.1. *The* golden ratio *is the number*

$$\phi = \frac{1 + \sqrt{5}}{2}.$$

The Greek letter ϕ (phi) is used for this number after the ancient Greek sculptor Phidias, who is said to have used the ratio in his work.

Leonardo da Vinci used ϕ in analysing the human figure.

Evidently

$$\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\phi),$$

ie each element of the field can be written

$$z = x + y\phi \quad (x, y \in \mathbb{Q}).$$

The following results are immediate:

Proposition 15.1. *1.* $\bar{\phi} = \frac{1-\sqrt{5}}{2}$*;*

2. $\phi + \bar{\phi} = 1, \ \phi\bar{\phi} = -1$*;*

3. $\mathcal{N}(x + y\phi) = x^2 + xy - y^2$*;*

4. $\phi, \bar{\phi}$ *are the roots of the equation*

$$x^2 - x - 1 = 0.$$

15.2 The number ring $\mathbb{Z}[\phi]$

As we saw in the last Chapter, since $5 \equiv 1 \bmod 4$ the associated number ring

$$\mathbb{Z}(\mathbb{Q}(\sqrt{5})) = \mathbb{Q}(\sqrt{5}) \cap \bar{\mathbb{Z}}$$

consists of the numbers

$$\frac{m + n\sqrt{5}}{2},$$

where $m \equiv n \bmod 2$, ie m, n are both even or both odd. And we saw that this is equivalent to

Proposition 15.2. *The number ring associated to the quadratic field* $\mathbb{Q}(\sqrt{5})$ *is*

$$\mathbb{Z}[\phi] = \{m + n\phi : m, n \in \mathbb{Z}\}.$$

15.3 Unique Factorisation

Theorem 15.1. *The ring* $\mathbb{Z}[\phi]$ *is a Unique Factorisation Domain.*

Proof. We prove this in exactly the same way that we proved the corresponding result for the gaussian integers Γ.

The only slight difference is that the norm can now be negative, so we must work with $|\mathcal{N}(z)|$.

Lemma 15.1. *Given* $z, w \in \mathbb{Z}[\phi]$ *with* $w \neq 0$ *we can find* $q, r \in \mathbb{Z}[\phi]$ *such that*

$$z = qw + r,$$

with

$$|\mathcal{N}(r)| < |\mathcal{N}(w)|.$$

Proof. Let

$$\frac{z}{w} = x + y\phi,$$

where $x, y \in \mathbb{Q}$. Let m, n be the nearest integers to x, y, so that

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

Set

$$q = m + n\phi.$$

Then

$$\frac{z}{w} - q = (x - m) + (y - n)\phi.$$

Hence

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

It follows that

$$-\frac{1}{2} < \mathcal{N}(\frac{z}{w} - q) < \frac{1}{2},$$

and so

$$\left|\mathcal{N}(\frac{z}{w} - q)\right| \le \frac{1}{2} < 1,$$

ie

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

□

This allows us to apply the euclidean algorithm in $\mathbb{Z}[\phi]$, and establish

Lemma 15.2. *Any two numbers $z, w \in \mathbb{Z}[\phi]$ have a greatest common divisor δ such that*

$$\delta \mid z, w$$

and

$$\delta' \mid z, w \implies \delta' \mid \delta.$$

Also, δ is uniquely defined up to multiplication by a unit.

Moreover, there exists $u, v \in \mathbb{Z}[\phi]$ such that

$$uz + vw = \delta.$$

From this we deduce that irreducibles in $\mathbb{Z}[\phi]$ are primes.

Lemma 15.3. *If $\pi \in \mathbb{Z}[\phi]$ is irreducible and $z, w \in \mathbb{Z}[phi]$ then*

$$\pi \mid zw \implies \pi \mid z \text{ or } \pi \mid w.$$

Now Euclid's Lemma , and Unique Prime Factorisation, follow in the familiar way. □

15.4 The units in $\mathbb{Z}[\phi]$

Theorem 15.2. *The units in $\mathbb{Z}[\phi]$ are the numbers*

$$\pm\phi^n \quad (n \in \mathbb{Z}).$$

Proof. We saw in the last Chapter that any real quadratic field contains an infinity of units, and that the units form the group

$$\{\pm\epsilon^n : n \in \mathbb{Z}\},$$

where ϵ is the smallest unit > 1.

Thus the theorem will follow if we establish that ϕ is the smallest unit > 1 in $\mathbb{Z}[\phi]$.

Suppose $\eta \in \mathbb{Z}[\phi]$ is a unit with

$$1 < \eta = m + n\phi \leq \phi.$$

Then $m, n > 0$; for if $m < 0$ then $-m + n\phi > m + n\phi$ while if $n < 0$ then $m - n\phi > m + n\phi$, and since all these lie in the foursome $\pm\eta,\ \pm\eta^{-1}$, only one of which can lie in the range $(1, \infty)$. Since no other algebraic integer $m + n\phi$ can lie in the range $(1, \phi]$ the units in $\mathbb{Z}[\phi]$ are

$$\pm\phi^n,$$

with $n \in \mathbb{N}$. □

15.5 The primes in $\mathbb{Z}[\phi]$

Theorem 15.3. *Suppose $p \in \mathbb{N}$ is a rational prime.*

1. *If $p \equiv \pm 1 \bmod 5$ then p splits into distinct conjugate primes in $\mathbb{Z}[\phi]$:*

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

2. *if $p \equiv \pm 2 \bmod 5$ then p remains prime in $\mathbb{Z}[\phi]$.*

Proof. Suppose p splits, say

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

where neither π nor π' is a unit. Then

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

Thus $\pi\bar{\pi'} = \pm p \implies \pi' = \pm\bar{\pi}$. Suppose $\pi = m + n\phi$. Then

$$\mathcal{N}(\pi) = m^2 - mn - n^2 = \pm p.$$

Then $p \mid n \implies p \mid m \implies p^2 \mid p$. Hence $p \nmid n$, and n has an inverse $n' \bmod p$ with $nn' \equiv 1 \bmod p$. Thus

$$((mn')^2 \equiv 5 \bmod p.$$

Hence 5 is a quadratic residue $\bmod p$.

But by Gauss' Law of Quadratic Reciprocit,

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \begin{cases} +1 & \text{if } p \equiv \pm 1 \mod 5 \\ -1 & \text{if } p \equiv \pm 2 \mod 5 \end{cases}$$

(For the quadratic residues mod 5 are $0, 1$ and $4 \equiv -1$.) Thus if $p \equiv \pm 2$ mod 5 then p cannot split in $Z[\phi]$.

Finally, suppose $p \equiv \pm 1 \mod 5$ Then 5 is a quadratic residue mod p, say

$$5 \equiv n^2 \bmod p,$$

where we may suppose that $0 < n < p/2$. Then $p \mid (n + \sqrt{5})(n - \sqrt{5})$, say $p \mid \pi\bar{\pi}$. Hence

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

But $\mathcal{N}(\pi) = \mathcal{N}(\bar{\pi})$, and so

$$p \mid \mathcal{N}(\pi) = \pi\bar{\pi}.$$

Suppose p does not split. Then $p \mid \pi$ or $p \mid \pi'$. In either case,

$$p \mid n \pm \sqrt{5} \implies n \pm \sqrt{5} = p(a + b\phi) \implies 2n \pm 2\phi = p((2a + b) + b\sqrt{5}).$$

Since $\sqrt{5}$ is irrational, it follows that

$$2n = p(2a + b),\ 2 = pb \implies p \mid 2,$$

which is impossible. Hence p must split in $\mathbb{Z}[\phi]$. □

15.6 The weak Lucas-Lehmer test for Mersenne primality

Recall that the Mersenne number

$$M_p = 2^p - 1,$$

where p is a prime.

We give a version of the Lucas-Lehmer test for primality which only works when $p \equiv 3 \bmod 4$. In the next Chapter we shall give a stronger version which works for all primes.

Proposition 15.3. *Suppose the prime* $p \equiv 3 \bmod 4$. *Then*

$$P = 2^p - 1$$

is prime if and only if

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

Proof. Suppose first that P is a prime.

Since $p \equiv 3 \bmod 4$ and $2^4 \equiv 1 \bmod 5$,

$$\begin{aligned} 2^p &\equiv 2^3 \bmod 5 \\ &\equiv 3 \bmod 5. \end{aligned}$$

Hence

$$P = 2^p - 1 \equiv 2 \bmod 5.$$

Now

$$\begin{aligned}\phi^P &= \left(\frac{1+\sqrt{5}}{2}\right)^P \\ &\equiv \frac{1^P + (\sqrt{5})^P}{2^P} \bmod P,\end{aligned}$$

since P divides all the binomial coefficients except the first and last. Thus

$$\phi^P \equiv \frac{1 + 5^{(P-1)/2}\sqrt{5}}{2} \bmod P,$$

since $2^P \equiv 2 \bmod P$ by Fermat's Little Theorem.

But

$$5^{(P-1)/2} \equiv \left(\frac{5}{P}\right),$$

by Euler's criterion. Hence by Gauss' Quadratic Reciprocity Law,

$$\begin{aligned}\left(\frac{5}{P}\right) &= \left(\frac{P}{5}\right) \\ &= -1,\end{aligned}$$

since $P \equiv 2 \bmod 5$. Thus

$$5^{(P-1)/2} \equiv -1 \bmod P,$$

and so

$$\phi^P \equiv \frac{1-\sqrt{5}}{2} \bmod P.$$

But

$$\begin{aligned}\frac{1-\sqrt{5}}{2} &= \bar{\phi} \\ &= -\phi^{-1}.\end{aligned}$$

It follows that

$$\phi^{P+1} \equiv -1 \bmod P,$$

ie

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

Conversely, suppose

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

We must show that P is prime.

The order of ϕ is exactly 2^{p+1}. For

$$\phi^{2^{p+1}} = \left(\phi^{2^p}\right)^2 \equiv 1 \bmod P,$$

so the order divides 2^{p+1}. On the other hand,

$$\phi^{2^p} \not\equiv 1 \bmod P,$$

so the order does not divide 2^p.

Suppose now P is not prime. Since

$$P \equiv 2 \bmod 5,$$

it must have a prime factor

$$Q \equiv \pm 2 \bmod 5.$$

(If all the prime factors of P were $\equiv \pm 1 \bmod 5$ then so would their product be.) Hence Q does not split in $\mathbb{Z}[\phi]$.

Since $Q \mid P$, it follows that

$$\phi^{2^p} \not\equiv 1 \bmod Q;$$

and so, by the argument above, the order of $\phi \bmod Q$ is 2^{p+1}.

We want to apply Fermat's Little Theorem, but we need to be careful since we are working in $\mathbb{Z}[\phi]$ rather than $\mathbb{Z}$.

Lemma 15.4 (Fermat's Little Theorem, extended)**.** *If the rational prime Q does not split in $\mathbb{Z}[\phi]$ then*

$$z^{Q^2-1} \equiv 1 \bmod Q$$

for all $z \in \mathbb{Z}[\phi]$ with $z \not\equiv 0 \bmod Q$.

Proof. The quotient-ring $A = \mathbb{Z}[\phi] \bmod Q$ is a field, by exactly the same argument that $\mathbb{Z} \bmod p$ is a field if p is a prime. For if $z \in A$, $z \neq 0$ then the map

$$w \mapsto zw : A \to A$$

is injective, and so surjective (since A is finite). Hence there is an element z' such that $zz' = 1$, ie z is invertible in A.

Also, A contains just Q^2 elements, represented by

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

Thus the group

$$A^\times = A \setminus 0$$

has order $Q^2 - 1$, and the result follows from Lagrange's Theorem. □

In particular, it follows from this Lemma that

$$\phi^{Q^2-1} \equiv 1 \bmod Q,$$

ie the order of $\phi \bmod Q$ divides $Q^2 - 1$. But we know that the order of $\phi \bmod Q$ is 2^{p+1}. Hence

$$2^{p+1} \mid Q^2 - 1 = (Q-1)(Q+1).$$

But

$$\gcd(Q-1, Q+1) = 2.$$

It follows that either

$$2 \parallel Q-1,\ 2^p \mid Q+1 \text{ or } 2 \parallel Q+1,\ 2^p \mid Q-1.$$

Since $Q \le P = 2^p - 1$, the only possibility is

$$2^p \mid Q+1,$$

ie $Q = P$, and so P is prime. □

This result can be expressed in a different form, more suitable for computation.

Note that

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

can be re-written as

$$\phi^{2^{p-1}} + \phi^{2^{-(p-1)}} \equiv 0 \bmod P.$$

Let

$$t_i = \phi^{2^i} + \phi^{2^{-i}}$$

Then

$$\begin{aligned} t_i^2 &= \phi^{2^{i+1}} + 2 + \phi^{2^{-(i+1)}} \\ &= t_{i+1} + 2, \end{aligned}$$

ie

$$t_{i+1} = t_i^2 - 2.$$

Since

$$t_0 = 2$$

it follows that $t_i \in \mathbb{N}$ for all i.

Now we can re-state our result.

Corollary 15.1. *Let the integer sequence t_i be defined recursively by*

$$t_{i+1} = t_i^2 - 2,\ t_0 = 2.$$

Then

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