Chapter 10

The Arithmetic of $\mathbb{Z}[i]$

In this chapter we will briefly discuss number theory in the ring of Gaussian integers. We know it is a unique factorization domain, so primes and irreducibles are the same. Here we will determine all primes, the units, compute some residue classes, etc.

10.1 Units and Primes

Finding all units in $R = \mathbb{Z}[i]$ is easy. Assume that $a + bi$ is a unit; then $(a + bi)(c + di) = 1$, and taking the norm shows that $(a^2 + b^2)(c^2 + d^2) = 1$, which implies that $a^2 + b^2 = 1$. This happens if and only if $a + bi \in \{\pm 1, \pm i\}$.

Proposition 10.1. *We have* $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Now let us determine all the primes in $\mathbb{Z}[i]$. Assume that $a + bi$ is prime. Then $(a+bi) \mid (a+bi)(a-bi) = N(a+bi) = a^2+b^2$. Thus every prime divides a natural number $a^2 + b^2$; writing this number as a product of primes in $\mathbb{N}$ and keeping in mind that $a + bi$ is a prime in $\mathbb{Z}[i]$ we find that $a + bi$ must divide one of the prime factors of $a^2 + b^2$.

Lemma 10.2. *Every prime in* $\mathbb{Z}[i]$ *divides a prime in* $\mathbb{Z}$.

Thus in order to find all primes in $\mathbb{Z}[i]$ we only need to look at factors of primes in $\mathbb{Z}$. Of course primes in $\mathbb{Z}$ need not be prime in $\mathbb{Z}[i]$: for example, we have $5 = (1 + 2i)(1 - 2i)$.

Now assume that a prime $p \in \mathbb{N}$ factors nontrivially in $\mathbb{Z}[i]$; then $p = (a + bi)(c+di)$. Taking norms gives $p^2 = (a^2+b^2)(c^2+d^2)$. Since none of the factors is a unit, we must have $a^2 + b^2 = c^2 + d^2 = p$. Since $a^2 + b^2 \equiv 0, 1, 2 \bmod 4$, primes of the form $p \equiv 3 \bmod 4$ are irreducible in $\mathbb{Z}[i]$, and since $\mathbb{Z}[i]$ is a UFD, they are prime (in algebraic number theory, primes in $\mathbb{Z}$ remaining prime in an extension are called inert).

Next $2 = i^3(1 + i)^2$: thus 2 is a unit times a square (in algebraic number theory, such primes will be called ramified).

Finally, if $p \equiv 1 \bmod 4$, then $(\frac{-1}{p}) = +1$, hence $x^2 \equiv -1 \bmod p$ for some integer x. This implies $p \mid (x^2+1) = (x+i)(x-i)$. Now clearly p does not divide any of the factors since $\frac{x}{p} + \frac{1}{p}i$ is not a Gaussian integer. Thus p divides a product without dividing one of the factors, and this means p is not prime in $\mathbb{Z}$. Since irreducibles are prime, this implies that p must be reducible, i.e., it has a nontrivial factorization. We have seen above that this means that $p = a^2 + b^2$ for $a, b \in \mathbb{Z}$: thus the first supplementary law plus unique factorization in $\mathbb{Z}[i]$ implies Fermat's two-squares theorem!

Note that this proof is a lot more involved than the simple proof we have given before; on the other hand, it is much clearer.

Let us get back to primes $p \equiv 1 \bmod 4$. We have seen that $p = a^2 + b^2 = (a+bi)(a-bi)$. Can it happen that $a+bi$ and $a-bi$ differ only by a unit? If $a+bi = (a-bi)\varepsilon$, then $\varepsilon = \frac{a+bi}{a-bi} = \frac{1}{p}(a+bi)^2 = \frac{1}{p}(a^2-b^2+2abi)$. But this is not a Gaussian integers since $p \nmid 2ab$. Thus $a+bi$ and $a-bi$ are distinct primes (in algebraic number theory, we say that such primes split).

Theorem 10.3. *The ring $\mathbb{Z}[i]$ has the following primes:*

- $1+i$*, the prime dividing* 2*;*
- $a+bi$ *and* $a-bi$*, where* $p = a^2+b^2 \equiv 1 \bmod 4$*;*
- *rational primes* $q \equiv 3 \bmod 4$*.*

In particular, $\mathbb{Z}[i]$ has infinitely many primes. We could have proved this also by Euclid's argument.

10.2 Residue Class Systems

Of course we can now define residue classes in $\mathbb{Z}[i]$: we say that $a+bi \equiv c+di \bmod r+si$ if $(r+si) \mid (a-c+(b-d)i)$. If $a+bi$ is a prime, how many residue classes are there?

This is easy for the prime $1+i$: we claim that every Gaussian integer is congruent to 0 or $1 \bmod 1+i$. In fact, $a+bi \equiv a-b \bmod (1+i)$ because $i \equiv -1 \bmod 1+i$. Now we can reduce $a-b \bmod 2$ since 2 is a multiple of $1+i$, and this proves the claim. Moreover, $1 \not\equiv 0 \bmod 1+i$ since 1 is not divisible by $1+i$. Thus $\{0,1\}$ is a complete system of residues modulo $1+i$.

The same trick works for primes $c+di$ with norm $p \equiv 1 \bmod 4$: we have $i \equiv -\frac{c}{d} \bmod c+di$, hence $a+bi \equiv a-b\frac{c}{d} \bmod a+bi$. Thus every Gaussian integer is congruent to some integer modulo $a+bi$. Now we can reduce modulo p (this is a multiple of $a+bi$) and find that every Gaussian integer is congruent to some element $0, 1, \ldots, p-1$ modulo $a+bi$. Moreover, these elements are incongruent modulo $a+bi$: if $r \equiv s \bmod a+bi$ for $0 \le r, s < p$, then $(a+bi) \mid (r-s)$; taking norms gives $p^2 \mid (r-s)^2$, hence $p \mid (r-s)$ and finally $r = s$. Thus $\{0,1,\ldots,p-1\}$ is a complete system of residues modulo the prime $a+bi$ with norm p.

Finally, consider inert primes $q \equiv 3 \bmod 4$. Here we claim that $S = \{r+si : 0 \le r, s < p\}$ is a complete system of residues modulo p (note that this set contains p^2 elements). It is clear that every $a+bi \equiv r+si \bmod p$ for some $r+si \in S$: just reduce a and b modulo p. We only have to show that no two elements in S are congruent modulo p. Assume therefore that $r+si \equiv t+ui \bmod p$ for $0 \le r,s,t,u < p$. Then $p \mid (r-t+(s-u)i)$, i.e., $\frac{r-t}{p} + \frac{s-u}{p} i \in \mathbb{Z}[i]$. This happens if and only if $r \equiv t \bmod p$ and $s \equiv u \bmod p$, which implies $r = t$ and $s = u$.

We have proved:

Proposition 10.4. *The complete system of residues modulo a Gaussian prime $a+bi$ has exactly $N(a+bi) = a^2+b^2$ elements.*

Let us now add a level of abstraction and consider, for a prime $p = a^2+b^2 \equiv 1 \bmod 4$, the map $\lambda : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}[i]/(a+bi) : [r]_p \longmapsto [r]_{a+bi}$. It obviously is a homomorphism because $\lambda([r]_p)\lambda([s]_p) = [r]_{a+bi}[s]_{a+bi} = [rs]_{a+bi} = \lambda([rs]_p)$. From what we have seen above, λ is surjective because every residue class modulo $a+bi$ is represented by one of the integers $0, 1, \ldots p-1$. Is λ injective? Its kernel is $\ker\lambda = \{[r]_p : [r]_{a+bi} = [0]_{a+bi}\}$. Now $r \equiv 0 \bmod a+bi$ implies $p^2 \mid r^2$, hence $p \mid r$, hence $[r]_p = [0]_p$. Thus $\ker\lambda = \{[0]_p\}$, and λ is injective.

We have seen that $\lambda : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}[i]/(a+bi)$ is an isomorphism: the two residue class systems have the same number of elements, the same structure, and in particular, they are both fields with p elements.

What can we say about the residue class ring $R = \mathbb{Z}[i]/(p)$ for primes $p \equiv 3 \bmod 4$? Let us check that R is a domain, i.e., that it has no zero divisors. In fact, assume that $(a+bi)(c+di) \equiv 0 \bmod p$. Since p is a prime in $\mathbb{Z}[i]$, this implies $p \mid (a+bi)$ or $p \mid (c+di)$, hence $[a+bi]_p = [0]_p$ or $[c+di]_p = [0]_p$, and this shows that R is a domain.

Now we have

Proposition 10.5. *Any domain R with finitely many elements is a field.*

Proof. Let $a \in R$ be nonzero. We need to show that a is a unit, i.e. that there is a $b \in R$ with $ab = 1$. Let $n = \#R$; we claim that $a^{n-1} = 1$ (this is like Fermat's little theorem, and the proof is the same). Write $R \setminus \{0\} = \{a_1 = 1, a_2, \ldots, a_{n-1}\}$. Define elements b_j by $a_j a = b_j$. We claim that the b_j are just the a_j in some order. This will follow if we can show that no two b_j are equal. Assume therefore that $b_j = b_k$; then $a_j a = a_k a$. Since R is a domain, we may cancel (note that $ac = ad$ implies $a(c-d) = 0$, and since R has no zero divisors, this shows that $a = 0$ or $c = d$), and we get $a_j = a_k$.

Next we multiply all the equations $a_1 a = b_1, \ldots, a_{n-1}a = b_{n-1}$; since $\prod a_j = \prod b_j$ we conclude that $a^{n-1} = 1$.

Now we simply put $b = a^{n-2}$ and observe that $ab = 1$. □

We have proved:

Proposition 10.6. *Let $p \equiv 3 \bmod 4$ be prime. Then $\mathbb{Z}[i]/(p)$ is a field with p^2 elements.*

There also exist finite fields with p^2 elements for primes $p \equiv 1 \bmod 4$, but these cannot be constructed as residue class fields in $\mathbb{Z}[i]$.

Quadratic Reciprocity

Now pick a prime $\pi = a + bi \equiv 1 \bmod 2$; note that this means that a is odd and b is even. We have

Proposition 10.7 (Fermat's Little Theorem)**.** *For any element α coprime to π we have $\alpha^{N\pi-1} \equiv 1 \bmod \pi$.*

The proof is analogous to the one in $\mathbb{Z}$: enumerate the $N\pi - 1$ elements α_i in $(Z[i]/\pi\mathbb{Z}[i])^\times$, then multiply them by α and show that the products $\beta_i \equiv \alpha\alpha_i \bmod \pi$ are just the α_i in some order. Then multiply etc.

As an example, let us compute $(1+i)^{N\pi-1} \bmod \pi$ for $\pi = 1 + 2i$. Then $N\pi = 5$ and $(1+i)^4 = (2i)^2 = -4 \equiv 1 \bmod 5$, hence modulo π.

Since $\pi \equiv 1 \bmod 2$ we find that $N\pi = a^2 + b^2 \equiv 1 \bmod 4$. Thus

$$0 \equiv \alpha^{N\pi-1} - 1 = \big(\alpha^{\frac{N\pi-1}{2}} - 1\big)\big(\alpha^{\frac{N\pi-1}{2}} + 1\big) \bmod \pi,$$

hence $\alpha^{\frac{N\pi-1}{2}} \equiv \pm 1 \bmod \pi$ since π is prime. We now define the quadratic Legendre symbol $[\frac{\alpha}{\pi}] = \pm 1$ in $\mathbb{Z}[i]$ by

$$\Big[\frac{\alpha}{\pi}\Big] \equiv \alpha^{\frac{N\pi-1}{2}} \bmod \pi.$$

As an example, let us compute $[\frac{1+i}{1+2i}]$. We find $(1+i)^{(N\pi-1)/2} = (1+i)^2 = 2i \equiv -1 \bmod \pi$, hence $[\frac{1+i}{1+2i}] = -1$.

In order to prove a quadratic reciprocity law in $\mathbb{Z}[i]$ we collect a few simple properties of these symbols.

Proposition 10.8. *For elements $\alpha, \beta, \pi \in \mathbb{Z}[i]$ with $\pi \equiv 1 \bmod 2$ prime we have*

1. $[\frac{\alpha}{\pi}] = [\frac{\beta}{\pi}]$ *if* $\alpha \equiv \beta \bmod \pi$*;*
2. $[\frac{\alpha\beta}{\pi}] = [\frac{\alpha}{\pi}][\frac{\beta}{\pi}]$*;*
3. $[\frac{\alpha\beta}{\pi}] = +1$ *if* $\alpha \equiv \xi^2 \bmod \pi$*.*

Proof. The first and second follow directly from the definition. Assume now that $\alpha \equiv \xi^2 \bmod \pi$; then $\alpha^{\frac{N\pi-1}{2}} \equiv \xi^{N\pi-1} \equiv 1 \bmod \pi$ by Fermat's Little Theorem. □

We also will use a few results on the quadratic character of certain integers:

Proposition 10.9. *Let $p = a^2 + b^2$ be an odd prime, and suppose that a is odd. Then*

$$\Big(\frac{a}{p}\Big) = 1, \Big(\frac{b}{p}\Big) = \Big(\frac{2}{p}\Big), \text{ and } \Big(\frac{a+b}{p}\Big) = \Big(\frac{2}{a+b}\Big).$$

Proof. Using the quadratic reciprocity law, we get $(\frac{a}{p}) = (\frac{p}{a}) = +1$, because $p = a^2 + b^2 \equiv b^2 \bmod a$. Next the congruence $(a+b)^2 \equiv 2ab \bmod p$ shows that $(\frac{a}{p}) = (\frac{2b}{p})$, and this proves our second claim. Finally $2p = (a+b)^2 + (a-b)^2$ implies that $(\frac{a+b}{p}) = (\frac{p}{a+b}) = (\frac{2}{a+b})$. □

In order to prove the quadratic reciprocity law in $\mathbb{Z}[i]$, we write $\pi = a+bi, \lambda = c+di$; then $\pi \equiv \lambda \equiv 1 \bmod 2$ implies that $a \equiv c \equiv 1 \bmod 2$ and $b \equiv d \equiv 0 \bmod 2$. If $\pi = p \in \mathbb{Z}$ or $\lambda = \ell \in \mathbb{Z}$, the proof follows directly from the relations $\big[\frac{p}{\lambda}\big] = \big(\frac{p}{N\lambda}\big)$ and $\big[\frac{\pi}{\ell}\big] = \big(\frac{N\pi}{\ell}\big)$, which are easy to verify:

Proposition 10.10. *For primes $\pi \in \mathbb{Z}[i]$ and elements $a \in \mathbb{Z}$ coprime to pi we have $[\frac{a}{\pi}] = (\frac{a}{N\pi})$.*

Proof. We have $[\frac{a}{\pi}] \equiv a^{(N\pi-1)/2} \bmod \pi$ and $(\frac{a}{N\pi}) \equiv a^{(N\pi-1)/2} \bmod p$. This implies $[\frac{a}{\pi}] \equiv (\frac{a}{N\pi}) \bmod \pi$. If the symbols were different, then π must divide 2, hence $N\pi$ must divide 4, and this is nonsense since π has odd norm > 1. □

Thus we may assume that $p = N\pi$ and $\ell = N\lambda$ are prime. We find immediately that $ai \equiv b \bmod \pi$ and $ci \equiv d \bmod \lambda$, hence we get

$$\Big[\frac{\pi}{\lambda}\Big] = \Big[\frac{c}{\lambda}\Big]\Big[\frac{ac+bci}{\lambda}\Big] = \Big[\frac{c}{\lambda}\Big]\Big[\frac{ac+bd}{\lambda}\Big].$$

Since $c \in \mathbb{Z}$ and $ac+bd \in \mathbb{Z}$, we find

$$\Big[\frac{c}{\lambda}\Big] = \Big(\frac{c}{\ell}\Big) \text{ and } \left[\frac{ac+bd}{\lambda}\right] = \left(\frac{ac+bd}{\ell}\right).$$

Using Proposition 10.9, we find

$$\Big[\frac{\pi}{\lambda}\Big] = \Big(\frac{ac+bd}{\ell}\Big). \tag{10.1}$$

But now $p\ell = (a^2+b^2)(c^2+d^2) = (ac+bd)^2+(ad-bc)^2 \equiv (ad-bc)^2 \bmod (ac+bd)$ implies $\big(\frac{\ell}{ac+bd}\big) = \big(\frac{p}{ac+bd}\big)$, and applying the quadratic reciprocity law in $\mathbb{Z}$ twice shows that

$$\left(\frac{ac+bd}{\ell}\right) = \left(\frac{\ell}{ac+bd}\right) = \left(\frac{p}{ac+bd}\right) = \left(\frac{ac+bd}{p}\right).$$

The quadratic reciprocity law in $\mathbb{Z}[i]$ follows by symmetry:

$$\Big[\frac{\pi}{\lambda}\Big] = \left(\frac{ac+bd}{\ell}\right) = \left(\frac{ac+bd}{p}\right) = \Big[\frac{\lambda}{\pi}\Big].$$

The supplementary laws follow immediately from (10.1) by putting $a = 0, b = 1$ or $a = b = 1$, and using quadratic reciprocity.

Quartic Reciprocity

Note that $N\pi \equiv 1 \bmod 4$ implies that we have

$$\begin{aligned} 0 &\equiv \alpha^{N\pi-1} - 1 = \big(\alpha^{\frac{N\pi-1}{2}} - 1\big)\big(\alpha^{\frac{N\pi-1}{2}} + 1\big) \\ &\equiv \big(\alpha^{\frac{N\pi-1}{4}} - 1\big)\big(\alpha^{\frac{N\pi-1}{4}} + 1\big)\big(\alpha^{\frac{N\pi-1}{4}} - i\big)\big(\alpha^{\frac{N\pi-1}{4}} + i\big) \bmod \pi, \end{aligned}$$

hence we can define a quartic power residue symbol $[\frac{\alpha}{\pi}]_4 \in \{1, i, -1, -i\}$ by demanding that

$$\left[\frac{\alpha}{\pi}\right]_4 \equiv \alpha^{\frac{N\pi-1}{4}} \bmod \pi.$$

This symbol satisfies the quartic reciprocity law, according to which

$$\left[\frac{\pi}{\lambda}\right]_4 = \left[\frac{\lambda}{\pi}\right]_4 (-1)^{\frac{N\pi-1}{4}\frac{N\lambda-1}{4}}$$

for any two primes $\pi \equiv \lambda \equiv 1 \bmod (2+2i)$. Its proof is much more difficult that that of the quadratic reciprocity law, but is quite easy using Gauss sums, which are objects defined using the theory of finite fields.

10.3 The ring $\mathbb{Z}[\sqrt{-2}]$

The arithmetic of this ring is very similar to that of $\mathbb{Z}[i]$. In particular, it is a UFD. We will now use this fact to prove one of Fermat's claims; the proof itself is due to Euler, who worked with the algebraic integers $a + b\sqrt{-2}$ as if they were natural numbers, not worrying about defining what primes, gcd's etc. are or whether unique factorization holds.

Theorem 10.11. *The diophantine equation* $y2 = x^3 - 2$ *has* $(3, \pm 5)$ *as its only solutions in integers.*

Proof. Write $x^3 = y^2 + 2 = (y + \sqrt{-2}\,)(y + \sqrt{-2}\,)$. Note that y must be odd (otherwise $y^2 + 2 \equiv 2 \bmod 4$, and no cube is $\equiv 2 \bmod 4$). Now let $\delta = \gcd(y + \sqrt{-2}, y + \sqrt{-2}\,)$. Clearly $\delta \mid 2\sqrt{-2}$ (the difference of these values); thus δ is a power of $\sqrt{-2}$. On the other hand, if $\sqrt{-2} \mid (y \pm \sqrt{-2}\,)$, then it divides the product of these factors, which is $x^3 = y^2 + 2$. But x is odd, hence $\sqrt{-2} \nmid \delta$.

We have seen that $y + \sqrt{-2}$ and $y + \sqrt{-2}$ are coprime and that their product is a cube. Since $\mathbb{Z}[\sqrt{-2}\,]$ is a UFD, this implies that the factors are cubes up to units. Since the only units are ± 1 and since these are cubes, it follows that $y + \sqrt{-2} = (a + b\sqrt{-2}\,)^3$. Comparing real and imaginary parts we find $y = a^3 - 6ab^2$ and $1 = 3a^2b - 2b^3$. The last equation shows $1 = b(3a^2 - 2b^2)$, hence $b = \pm 1$ and therefore $a = \pm 1$. This shows $y = \pm 5$ and finally $x = 3$. $\square$

10.4 The ring $\mathbb{Z}[\sqrt{-5}]$

This ring is not a UFD: we have $2 \cdot 3 = (1 + \sqrt{-5}\,)(1 - \sqrt{-5}\,)$, and all these factors are irreducible. In fact, $3 = (a + b\sqrt{-5}\,)(c + d\sqrt{-5}\,)$ implies $9 = (a^2 + 5b^2)(c^2 + 5d^2)$, which in turn is possible only if $(c, d) = (\pm 1, 0)$ or $(a, b) = (\pm 1, 0)$; thus 3 only has trivial factorizations.

As above we can show that if $x^2 \equiv -5 \bmod p$ is solvable, then p is not prime. But since $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, this does not imply that p is reducible: see the example $p = 3$ above.

Exercises

10.1 Use the Euclidean algorithm to compute $\gcd(7-6i, 3-14*i)$.

10.2 Find the prime factorization of $-3+24i$. (Hint: first factor the norm).

10.3 Find $c \in \{0, 1, \ldots, 16\}$ such that $3+2i \equiv c \bmod 1+4i$.

10.4 Show that for any $\alpha \in \mathbb{Z}[i]$ with odd norm there is a unit $\varepsilon \in \mathbb{Z}[i]^\times$ such that $\alpha\varepsilon = a+bi$ with a odd, b even, and $a+b \equiv 1 \bmod 4$. Show also that this condition is equivalent to $a+bi \equiv 1 \bmod (2+2i)$.

10.5 Use Euclid's argument to show that there are infinitely many primes in $\mathbb{Z}[i]$.

10.6 Show that for primes $p = a^2+b^2$ with b even we have $[\frac{a+bi}{a-bi}] = (\frac{2}{p})$.

10.7 Compute the quartic symbols $[\frac{1+2i}{1+4i}]_4$ and $[\frac{1+4i}{1+2i}]_4$, and check that the quartic reciprocity law holds for these elements.

10.8 Let $R = \mathbb{Z}[\sqrt{m}\,]$ with $m < -1$. Show that $R^\times = \{\pm 1\}$.

10.9 Show that $\mathbb{Z}[\sqrt{2}\,]$ contains infinitely many units.

10.10 Find all the prime elements in $\mathbb{Z}[\sqrt{-2}\,]$.

10.11 Use the ring $\mathbb{Z}[\sqrt{-2}\,]$ to construct finite fields with p^2 elements for primes $p \equiv 5, 7 \bmod 8$.

10.12 Solve the congruence $x^2 \equiv -1 \bmod 41$ and then compute $\gcd(x+i, 41)$ in $\mathbb{Z}[i]$.

10.13 Find infinitely many integers $x, y, z \in \mathbb{Z}$ with $x^2+y^2 = z^3$.

10.14 Solving equations like $y^2 = x^3+c$ is not always as easy as for $c = -2$. Show that solving $y^2 = x^3+1$ in the standard way leads to the new diophantine equation $a^3 - 2b^3 = 1$. How do you think mathematicians solve this last equation?