11 Some Number Theory

Information about the prime ideals in the ring $\mathbb{Z}[\mathrm{i}]$ of Gaussian integers deepens our knowledge of the integers. After describing these ideals, we showcase a few number-theoretic applications.

11.0 Gaussian Primes

What are the prime ideals in the ring of Gaussian integers? We first identify those positive prime integers that lift to reducible elements in the Gaussian integers.

Proposition 11.0.0. *For any positive prime integer p, the following conditions are equivalent:*

(a) *The integer p is reducible in the ring $\mathbb{Z}[\mathrm{i}]$.*
(b) *There exists integers a and b such that $p = a^2 + b^2$.*
(c) *Either $p = 2$ or $p \equiv 1 \mod 4$.*
(d) *The ring $\mathbb{Z}/\langle p\rangle$ has an element whose square is $[-1]_p$.*
(e) *The polynomial $x^2 + 1$ is reducible in the ring $\mathbb{F}_p[x]$.*
(f) *The ring $\mathbb{F}_p[\mathrm{i}] := \{a + b\,\mathrm{i} \mid a, b \in \mathbb{F}_p \text{ and } \mathrm{i}^2 = -1\}$ is not a field.*

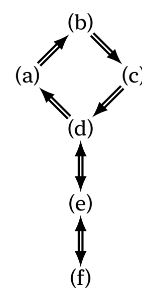

Figure 11.1: Directed graph of implications

Proof. We establish the equivalences by exhibiting a strongly connected directed graph of implications; see Figure 11.1

(a) ⇒ (b): Suppose that p is reducible in the ring $\mathbb{Z}[\mathrm{i}]$. There exist integers a, b, c, and d such that $p = (a + b\,\mathrm{i})(c + d\,\mathrm{i})$ and neither $a + b\,\mathrm{i}$ nor $c + d\,\mathrm{i}$ is a unit. Taking absolute values squared, we obtain $p^2 = (a^2 + b^2)(c^2 + d^2)$. Since p is a prime integer, the ring $\mathbb{Z}$ is a unique factorization domain, and neither $a^2 + b^2$ nor $c^2 + d^2$ is equal to 1, we deduce that $a^2 + b^2 = p = c^2 + d^2$.

(b) ⇒ (c): Observe that $2 = 1^2 + 1^2$. Suppose that p is odd and $p = a^2 + b^2$ for some integers a and b. We may also assume that a is odd and b is even. Since $a = 2\,m + 1$ and $b = 2\,n$ for some integers m and n, we see that $a^2 = 4\,m^2 + 4\,m + 1 \equiv 1 \mod 4$ and $b^2 = 4\,n^2 \equiv 0 \mod 4$. Hence, we have $p = a^2 + b^2 \equiv 1 \mod 4$.

(c) ⇒ (d): Since $[1]_2^2 = [1]_2 = [-1]_2$, we may assume that $p - 1$ is divisible by 4. Consider the product $d := [1]_p[2]_p \cdots [(p-1)/2]_p$. Observe that

$$\begin{aligned} d^2 &= (-1)^{(p-1)/2}\, d^2 \\ &= \big([1]_p\,[2]_p \cdots [(p-1)/2]_p\big)\big([-1]_p\,[-2]_p \cdots [-(p-1)/2]_p\big) \\ &= \big([1]_p\,[2]_p \cdots [(p-1)/2]_p\big)\big([p-1]_p\,[p-2]_p \cdots [p-(p-1)/2]_p\big) \\ &= [1]_p\,[2]_p \cdots [(p-1)/2]_p\,[(p+1)/2]_p \cdots [p-2]_p\,[p-1]_p \\ &= [(p-1)!]_p\,. \end{aligned}$$

The Wilson Theorem 2.3.7 gives $d^2 = [(p-1)!]_p = -1$.

(d) ⇒ (a): Suppose that a is an integer such that $[a]_p^2 = [-1]_p$. It follows that $a \neq 0$ and p divides $a^2 + 1 = (a + \mathrm{i})(a - \mathrm{i})$. Assuming that the element p is irreducible in $\mathbb{Z}[\mathrm{i}]$, it would follow that p

divides $a + \mathrm{i}$ or $a - \mathrm{i}$. Hence, there would exists integers c and d such that $a + \mathrm{i} = (c + d\,\mathrm{i})\,p$ or $a + \mathrm{i} = (c + d\,\mathrm{i})\,p$. Comparing real and imaginary parts, we would have that $p\,d = \pm 1$, and $p = \pm 1$ which contradicts p being a prime integer. Thus, we conclude that p is reducible in the ring $\mathbb{Z}[\mathrm{i}]$.

(d)⇔(e): Since $\mathbb{F}_p$ is a field, Corollary 4.0.9 shows that the monic quadratic polynomial $x^2 + 1$ is reducible in $\mathbb{F}_p[x]$ if and only if it has a root in $\mathbb{F}_p$. The polynomial $x^2 + 1$ has a root in $\mathbb{F}_p$ if and only if there exists an element in $\mathbb{F}_p$ whose square is -1.

(e)⇔(f): The evaluation map $\varphi\colon \mathbb{F}_p[x] \to \mathbb{F}_p[\mathrm{i}]$ defined by $\varphi(x) = \mathrm{i}$ is a ring homomorphism whose kernel is $\langle x^2 + 1\rangle$. Hence, the First Isomorphism Theorem 6.1.1 establishes that

$$\frac{\mathbb{F}_p[x]}{\langle x^2 + 1\rangle} \cong \mathbb{F}_p[\mathrm{i}]\,.$$

Proposition 9.0.11 shows that the quotient ring $\mathbb{F}_p[x]/\langle x^2 + 1\rangle$ is a field if and only if the element $x^2 + 1$ is irreducible. □

Generalizing Problem 5.2.5, we register the following fact.

Lemma 11.0.1. *Let a and b be coprime integers, and set $m := a^2 + b^2$. The quotient ring $\mathbb{Z}/\langle m\rangle$ is isomorphic to $\mathbb{Z}[\mathrm{i}]/\langle a + b\,\mathrm{i}\rangle$.*

Solution. When $a = 0$ or $b = 0$ (and the other is 1), the assertion is trivial. We may assume that $a\,b \neq 0$. Consider the unique ring homomorphism $\varphi\colon \mathbb{Z} \to \mathbb{Z}[\mathrm{i}]/\langle a + b\,\mathrm{i}\rangle$ defined, for any integer n, by $\varphi(n) = n + \langle a + b\,\mathrm{i}\rangle$; see Problem 5.0.4. We claim that $\mathrm{Ker}(\varphi) = \langle m\rangle$.

⊇: Since $m = a^2 + b^2 = (a - b\,\mathrm{i})(a + b\,\mathrm{i})$ belongs to the ideal $\langle a + b\,\mathrm{i}\rangle$, we have $\mathrm{Ker}(\varphi) \supseteq \langle m\rangle$.

⊆: Suppose that $n \in \mathrm{Ker}(\varphi)$. The definition of φ implies that $n \in \langle a + b\,\mathrm{i}\rangle$. Hence, there exists integers c and d such that $n = (a+b\,\mathrm{i})(c+d\,\mathrm{i}) = (a\,c-b\,d)+(a\,d+b\,c)\,\mathrm{i}$. Comparing real and imaginary parts, we see that $n = a\,c - b\,d$ and $b\,c = -a\,d$. The integers a and b being coprime implies that there are integers j and k such that $c = k\,a$ and $d = j\,b$. As $k\,a\,b = -j\,a\,b$, we see that $k = -j$ and $n = a\,(k\,a) - b(-k\,b) = k\,(a^2 + b^2) = k\,m$, so we obtain $\mathrm{Ker}(\varphi) \subseteq \langle m\rangle$.

We next demonstrate that φ is surjective. Since $\gcd(m, b) = 1$, Lemma 2.2.2 establishes that b has a multiplicative inverse in the quotient ring $\mathbb{Z}/\langle m\rangle$. In other words, there exists an integer e such that $[e]_m\,[b]_m = [1]_m$. As $m = a^2 + b^2 = (a + b\,\mathrm{i})(a - b\,\mathrm{i})$, it follows that $\mathrm{i} + \langle a + b\,\mathrm{i}\rangle = (e\,b\,\mathrm{i}) + \langle a + b\,\mathrm{i}\rangle = (-a\,e) + \langle a + b\,\mathrm{i}\rangle$. For some integers c and d, consider the coset $(c + d\,\mathrm{i}) + \langle a + b\,\mathrm{i}\rangle$ in $\mathbb{Z}[\mathrm{i}]/\langle a + b\,\mathrm{i}\rangle$. We see that $(c + d\,\mathrm{i}) + \langle a + b\,\mathrm{i}\rangle = (c - a\,d\,e) + \langle a + b\,\mathrm{i}\rangle$ and φ is surjective.

Finally, the First Isomorphism Theorem 6.1.1 shows that the induced map $\widetilde{\varphi}\colon \mathbb{Z}/\langle m\rangle \to \mathbb{Z}[\mathrm{i}]/\langle a + b\,\mathrm{i}\rangle$ is an isomorphism. □

We now characterize the prime ideals in the Gaussian integers.

Theorem 11.0.2. *Let p be a positive prime integer. When $p = 4\,j + 3$ for some integer j, the element p is irreducible in $\mathbb{Z}[\mathrm{i}]$. When $p = 2$ or $p = 4\,k + 1$ for some integer k, we have $p = (a + b\,\mathrm{i})(a - b\,\mathrm{i})$ in $\mathbb{Z}[\mathrm{i}]$ and both $a + b\,\mathrm{i}$ and $a - b\,\mathrm{i}$ are irreducible in $\mathbb{Z}[\mathrm{i}]$. Conversely, for any irreducible element z in $\mathbb{Z}[\mathrm{i}]$, either $z\,\overline{z}$ is a prime integer or it is the square of a prime integer.*

Proof. Proposition 11.0.0 shows that p is irreducible in the ring $\mathbb{Z}[\mathrm{i}]$ if and only if $p = 4\,j + 3$ for some integer j, and the integer p is a sum of two squares if and only if $p = 2$ or $p = 4\,k + 1$ for some integer k. In the second case, there exists integers a and b such that $p = a^2 + b^2 = (a + b\,\mathrm{i})(a - b\,\mathrm{i})$. Since $|a + b\,\mathrm{i}|^2 = |a - b\,\mathrm{i}|^2 = p$ is irreducible in $\mathbb{Z}$, we conclude that $a + b\,\mathrm{i}$ and $a - b\,\mathrm{i}$ are both irreducible in $\mathbb{Z}[\mathrm{i}]$.

Suppose that, for some integers a and b, the element $a + b\,\mathrm{i}$ is irreducible in the ring $\mathbb{Z}[\mathrm{i}]$. When $a = 0$ or $b = 0$, irreducibility implies that the other integer is a positive prime. In this situation, Proposition 11.0.0 shows that a or $b = -\mathrm{i}\,(a + b\,\mathrm{i})$ has the form $4\,j + 3$ for some integer j. When $a\,b \neq 0$, we may assume that $\gcd(a, b) = 1$, because otherwise $a + b\,\mathrm{i}$ is reducible in $\mathbb{Z}[\mathrm{i}]$. Setting $m := a^2 + b^2$, Lemma 11.0.1 implies that $\mathbb{Z}/\langle m\rangle \cong \mathbb{Z}[\mathrm{i}]/\langle a + b\,\mathrm{i}\rangle$. Proposition 9.0.11 proves that $a + b\,\mathrm{i}$ is irreducible if and only if these quotient rings are fields, and Theorem 2.2.4 establishes that $\mathbb{Z}/\langle m\rangle$ is a field if and only if m is a prime integer. □

11.1 Sums of Two Squares

How is ring theory useful in number theory? As a first answer, we determine which positive integers are the sum of two squares.

Lemma 11.1.0. *Let m be a positive integer. When $m = a^2 + b^2$ for coprime integers a and b, every odd prime that divides m may be expressed in the form $4\,j + 1$ for some integer j.*

Proof. Let p be an odd prime that divides m. The integers a and b being coprime means that p cannot divide both of them. We may assume that $\gcd(p, a) = 1$. Division with remainder 1.1.2 implies that there exists integer q and r such that $a = q\,p + r$ and $1 \leqslant r < p$. Theorem 2.2.4 shows that there exists an integer s such that $[r]_p\,[s]_p = [1]_p$. It follows that

$$([s]_p\,[b]_p)^2 = [s]_p^2\,([m]_p - [a]_p^2) = [s]_p^2\,[0]_p - ([s]_p\,[r]_p)^2 = [-1]_p\,.$$

As $\mathbb{Z}/\langle p\rangle$ has an element whose square is $[-1]_p$, Proposition 11.0.0 shows that $p = 2$ or $p = 4\,j + 1$ for some integer j. □

Two-Square Theorem 11.1.1. *An integer greater than one can be written as a sum of two squares if and only if its prime decomposition contains no factor p^e, where the prime p has the form $4\,k + 3$ for some integer k and e is odd.*

Legendre's Three-Square Theorem characterizes those integers that can be written as a sum of three squares, and Lagrange's Four-Square Theorem proves that every integer can be written as a sum of four squares.

Proof. We prove each implication separately.

$\Leftarrow$: Suppose that, in the prime decomposition of the integer n, every prime of the form $4\,k + 3$ appears an even number of times. It follows that $n = r^2 s$ where r and s are integers and every prime appearing in the decomposition of s is either 2 or has the form $4\,j + 1$ for some integer j. By Proposition 11.0.0, every prime factor of s is a sum of two squares. The equation

$$\begin{aligned}(a^2 + b^2)(c^2 + d^2) &= |a - b\,\mathrm{i}|^2\,|c + d\,\mathrm{i}|^2 \\ &= |(a - b\,\mathrm{i})(c + d\,\mathrm{i})|^2 \\ &= |(a\,c + b\,d) + (a\,d - b\,c)\,\mathrm{i}|^2 \\ &= (a\,c + b\,d)^2 + (a\,d - b\,c)^2\end{aligned}$$

implies that s is a sum of two squares. Lastly, the identity $r^2\,(f^2 + g^2) = (r\,f)^2 + (r\,g)^2$ shows that n is also a sum of two squares.

$\Rightarrow$: Suppose that $n = a^2 + b^2$ for some integers a and b, and set $k := \gcd(a, b)$. There exists integers c and d such that $a = k\,c$ and $b = k\,d$, so $n = k^2\,(c^2 + d^2)$ and $\gcd(c, d) = 1$. Lemma 11.1.0 establishes that the only prime divisors of $c^2 + d^2$ are 2 and primes of the form $4\,j + 1$ for some integer j. It follows that a prime p of the form $4\,k + 3$ for some integer k that divides n must also divide k. If p^e is the highest power of p that divides k, then p^{2e} is the power that divides n. □

Lemma 11.1.2. *Let x and y be coprime integers. When x and y have opposite parity, the elements $x + y\,\mathrm{i}$ and $x - y\,\mathrm{i}$ are coprime in $\mathbb{Z}[\mathrm{i}]$.*

Opposite parity means that one integer is odd and the other is even.

Proof. Suppose that $a + b\,\mathrm{i}$ is an irreducible element in $\mathbb{Z}[\mathrm{i}]$ that divides both $x + y\,\mathrm{i}$ and $x - y\,\mathrm{i}$. This irreducible element must divide both $(x + y\,\mathrm{i}) + (x - y\,\mathrm{i}) = 2\,x$ and $(x + y\,\mathrm{i}) - (x - y\,\mathrm{i}) = 2\,y\,\mathrm{i}$. As i is a unit, it follows that $a + b\,\mathrm{i}$ divides $2\,x$ and $2\,y$.

Assume that $a + b\,\mathrm{i}$ does not divide 2 in $\mathbb{Z}[\mathrm{i}]$. It would follow that $a + b\,\mathrm{i}$ divides x and y. Since x and y are coprime in $\mathbb{Z}$, we would have $a + b\,\mathrm{i} \notin \mathbb{Z}$ and $a + b\,\mathrm{i} \neq a - b\,\mathrm{i}$. Given integers c and d such that $x = (a + b\,\mathrm{i})(c + d\,\mathrm{i})$, conjugation would imply that $x = (a - b\,\mathrm{i})(c - d\,\mathrm{i})$, so the element $a - b\,\mathrm{i}$ would divide x and the product $(a - b\,\mathrm{i})(a + b\,\mathrm{i}) = a^2 + b^2$ would divide x. The analogous argument would show that $a - b\,\mathrm{i}$ and $a^2 + b^2$ divide y. However, this is a contradiction because x and y are coprime integers.

The only other possibility is that $a + b\,\mathrm{i}$ divides 2 in $\mathbb{Z}[\mathrm{i}]$. It follows that $a + b\,\mathrm{i}$ equals $1 + \mathrm{i}$, up to multiplication by a unit. Thus, we have $\frac{x+y\,\mathrm{i}}{1+\mathrm{i}} = \big(\frac{x+y\,\mathrm{i}}{1+\mathrm{i}}\big)\big(\frac{1-\mathrm{i}}{1-\mathrm{i}}\big) = \big(\frac{x+y}{2}\big) - \big(\frac{x-y}{2}\big)\,\mathrm{i}$ is an element in $\mathbb{Z}[\mathrm{i}]$. This happens if and only if x and y have the same parity. Thus, when x and y have opposite parity, the greatest common divisor of $x + y\,\mathrm{i}$ and $x - y\,\mathrm{i}$ in $\mathbb{Z}[\mathrm{i}]$ is a unit. □

As a second answer to our motivating question, we describe the primitive Pythagorean triples.

Proposition 11.1.3. *The integer x, y, and z have no common prime divisor and satisfy the equation $x^2 + y^2 = z^2$ if and only if there exists integers a and b such that $x = a^2 - b^2$, $y = 2\,a\,b$, and $z = a^2 + b^2$.*

Proof. We prove each implication separately.

⇐: Suppose that there exists integers a and b such that $x = a^2 - b^2$, $y = 2\,a\,b$, and $z = a^2 + b^2$. We have

$$\begin{aligned} x^2 + y^2 &= (a^2 - b^2)^2 + (2\,a\,b)^2 \\ &= a^4 - 2\,a^2\,b^2 + b^4 + 4\,a^2\,b^2 \\ &= a^4 + 2\,a^2\,b^2 + b^4 \\ &= (a^2 + b^2)^2 = z^2\,. \end{aligned}$$

⇒: Suppose that $x^2 + y^2 = z^2$ and x, y, and z have no common prime divisor. Any prime that divides two of these integers would also divide the third, so x, y, and z are pairwise coprime. If x and y were both odd, then x^2 and y^2 are congruent to 1 modulo 4. However, this would mean that z^2 is congruent to 2 modulo 4 which is impossible. Hence, the integers x and y have the opposite parity and z is odd. Lemma 11.1.2 proves that $x + y\,\mathrm{i}$ and $x - y\,\mathrm{i}$ are coprime in $\mathbb{Z}[\mathrm{i}]$. As $z^2 = x^2 + y^2 = (x + y\,\mathrm{i})(x - y\,\mathrm{i})$, the ring $\mathbb{Z}[\mathrm{i}]$ of Gaussian integers being a unique factorization domain implies that $x + y\,\mathrm{i}$ is the square of an element in $\mathbb{Z}[\mathrm{i}]$. Hence, there exists integers a and b such that

$$x + y\,\mathrm{i} = (a + b\,\mathrm{i})^2 = (a^2 - b^2) + (2\,a\,b)\,\mathrm{i}\,.$$

We conclude that $x = a^2 - b^2$, $y = 2\,a\,b$, and $z = a^2 + b^2$. □