

Lecture 18 (Fermat's Two Square Theorem)

Gaussian Integers and Sums of Two Squares

Recall the Gaussian integers are the subset $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ of \mathbb{C} . They form a subring of \mathbb{C} .

Recall also the norm $Nz = z\bar{z}$ is a multiplicative function from \mathbb{C} to the non-negative reals. For $\alpha \in \mathbb{Z}[i]$, $N\alpha \in \mathbb{N}$.

Proposition 18.1 (Gauss 1832) The Gaussian integers are Euclidean with $d(\alpha) = N\alpha$.

Proof The Gaussian integers are subring of the field \mathbb{C} and contain 1. So they are an integral domain.

(E1) If $\alpha = a + ib \in \mathbb{Z}[i]$, $N\alpha = a^2 + b^2 \in \mathbb{N}$ and for $\alpha \neq 0$, $N\alpha \geq 1$. Hence for α, β non-zero elements of $\mathbb{Z}[i]$, $N(\alpha\beta) = N\alpha N\beta \geq N\alpha$.

(E2) Let $z = x + iy \in \mathbb{C}$. Then we find $u, v \in \mathbb{Z}$ such that $|x - u| \leq \frac{1}{2}$ and $|y - v| \leq \frac{1}{2}$. Hence $w = u + iv \in \mathbb{Z}[i]$ satisfies

$$|z - w| = \sqrt{(x - u)^2 + (y - v)^2} \leq \sqrt{\frac{1}{4} + \frac{1}{4}} = \frac{1}{\sqrt{2}}.$$

Hence given α and a non-zero β in $\mathbb{Z}[i]$ we can find a $\gamma \in \mathbb{Z}[i]$ such that

$$\begin{aligned} \left| \frac{\alpha}{\beta} - \gamma \right| &\leq \frac{1}{\sqrt{2}} \\ \Rightarrow |\alpha - \gamma\beta| &\leq \frac{1}{\sqrt{2}}|\beta| \\ \Rightarrow N(\alpha - \gamma\beta) &\leq \frac{1}{2}N\beta. \end{aligned}$$

Hence $\alpha = \gamma\beta + \rho$ where $\rho = \alpha - \gamma\beta$ satisfies

$$N\rho \leq \frac{1}{2}N\beta < N\beta. \square$$

Corollary In the Gaussian integers are a principal ideal domain. An $\alpha = a + ib \in \mathbb{Z}[i]$ is a unit if and only if $N\alpha = a^2 + b^2 = 1$. \square

Consequences In the Gaussian integers $\mathbb{Z}[i]$ the following hold.

- Irreducibles are prime.
- Non-zero elements are units or a product of prime elements.
- Factorisation into primes is unique up to associates and order of factors.
- The units are $\pm 1, \pm i$.
- Every non-zero α has four associates, $\pm\alpha, \pm i\alpha$.

Lemma 18.2 An $n \in \mathbb{N}$ is a sum of two squares in \mathbb{Z} if and only if $n = N\alpha$ for some $\alpha \in \mathbb{Z}[i]$.

If and both $n, m \in \mathbb{N}$ are the sum of two squares in \mathbb{Z} so is mn .

Proof The first statement follows from $N(a + ib) = a^2 + b^2 \in \mathbb{N}$. Hence the second follows because if $n = N\alpha$ and $m = N\beta$ for $\alpha, \beta \in \mathbb{Z}[i]$ then $nm = N\alpha N\beta = N\gamma$ where $\gamma = \alpha\beta \in \mathbb{Z}[i]$. \square

Recall For a prime p , $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, the field with p elements

Proposition 18.3 Let $p \in \mathbb{N}$ be an odd prime. Then the following are equivalent

- (i) $p \equiv 1 \pmod{4}$.
- (ii) $-1 \in \mathbb{F}_p$ is a square.

Proof For any non-zero y in \mathbb{F}_p , we can form the four term sequence $S(y) : y, -y, y^{-1}, -y^{-1}$.

Given $y \neq 0$, we see each sequence

$$\begin{aligned} S(y) &: y, -y, y^{-1}, -y^{-1}. \\ S(-y) &: -y, y, -y^{-1}, y^{-1}. \\ S(y^{-1}) &: y^{-1}, -y^{-1}, y, -y. \\ S(-y^{-1}) &: -y^{-1}, y^{-1}, -y, y \end{aligned}$$

contains the same terms permuted. So For $y \neq 0$ the distinct sets $P_y = \{y, -y, y^{-1}, -y^{-1}\}$ partition \mathbb{F}_p^\times .

The terms of $S(y)$ are not necessarily distinct. We cannot have $y = -y, y^{-1} = -y^{-1}$ in \mathbb{F}_p because p is odd and $y \neq 0$.

We may have $y = y^{-1}, -y = -y^{-1}$ and this the case if and only if $y = \pm 1$ and $P_y = \{1, -1\}$.

We may also may have $y = -y^{-1}, -y = y^{-1}$. This can happen if and only if $y^2 = -1$, i.e. -1 is a square in \mathbb{F}_p .

Thus we can partition the $p - 1$ into disjoint classes all with four elements except $P_1 = P_{-1} = \{1, -1\}$ with 2 elements and if $-1 = y^2$ in \mathbb{F}_p , $P_y = P_{-y} = \{y, -y\}$ also with two elements.

Thus if -1 is not a square in \mathbb{F}_p , $p - 3 = (p - 1) - 2$ is a multiple of 4 and if -1 is square, $(p - 1)$ is a multiple of 4. \square

Theorem 18.4 (Fermat 1640, Euler 1747) Let p be an odd prime $p \in \mathbb{N}$. The p is a sum of two squares if and only $p \equiv 1 \pmod{4}$.

Proof (Dedekind 1894) Suppose p is a sum of squares in \mathbb{Z} , $p = a^2 + b^2$. Then neither a nor b is 0 modulo p . In \mathbb{F}_p , $a^2 + b^2 \equiv 0 \pmod{p}$ implies $-1 \equiv (a/b)^2 \pmod{p}$, is a square in \mathbb{F}_p .

Conversely suppose -1 is a square in \mathbb{F}_p . Then there is an $x \in \mathbb{Z}$ such that $x^2 + 1$ is divisible by p . In $\mathbb{Z}[i]$, $x^2 + 1 = (x - i)(x + i)$ and $p|(x - i)(x + i)$. But neither of $(x \pm i)/p$ is in $\mathbb{Z}[i]$ because in each case the coefficient of i , $\pm 1/p$, is not in \mathbb{Z} . So p does not divide $x \pm i$ in $\mathbb{Z}[i]$. Hence p is not a prime in the principal ideal domain $\mathbb{Z}[i]$ and in a P.I.D. an element is prime if and only if it is irreducible. Consequently p is reducible in $\mathbb{Z}[i]$. So there is factorisation $p = \alpha\beta$ in $\mathbb{Z}[i]$ with neither factor a unit, which implies that the rational integers $N\alpha$ and $N\beta$ are both greater than 1. Taking norms gives $p^2 = Np = N\alpha N\beta$, which since p is a prime number implies $N\alpha = N\beta = p$. Hence p is a sum of two squares. \square