Fermat's Theorem on Sums of Squares

Mark Sullivan
Advisor: Karl Zimmermann
Union College

Let R be an integral domain equipped with a multiplicative identity element 1.

Definition An element $u \in R$ is a unit in R provided that $\exists v \in R$ such that $uv = 1$.

Suppose that $p \in R$ is neither 0 nor a unit in R.

Definition The element $p \in R$ is prime provided that $\forall a, b \in R$, $p|ab$ implies that $p|a$ or $p|b$.

Definition The element $p \in R$ is irreducible provided that $p = uv$ implies that u is a unit or v is a unit.

The Gaussian Integers:

$$\mathbb{Z}[i] = \{x + yi \in \mathbb{C} | x, y \in \mathbb{Z}\}$$

Norm:

$$N(x + yi) = (x + yi)(x - yi) = x^2 + y^2 \geq 0$$

One can show that the norm serves as an appropriate Euclidean norm; the Gaussian integers are a Euclidean Domain.

One can show that $N(\alpha) = 1$ if and only if α is a unit in the Gaussian integers.

One can show that $\forall \beta, \gamma \in \mathbb{Z}[i],\ N(\beta\gamma) = N(\beta)N(\gamma)$.

Theorem (Fermat) Let $p \in \mathbb{Z}$ be an odd prime number. Then $p \equiv 1(mod\ 4)$ if and only if $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

Proof: $(\Leftarrow)$ Assume that $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

We know that $p \equiv 1(mod\ 4)$ or $p \equiv 3(mod\ 4)$, since p is an odd prime.

For contradiction, let $p \equiv 3(mod\ 4)$.

Then $a^2 + b^2 \equiv 3(mod\ 4)$ for some $a, b \in \mathbb{Z}$.

Thus, either (working modulo 4):

Case 1: One of a^2 and b^2 is congruent to 0; the other is congruent to 3.
Case 2: One of a^2 and b^2 is congruent to 1; the other is congruent to 2.

However, for any $k \in \mathbb{Z}$, if k is odd, then $k^2 \equiv 1(mod\ 4)$, and if k is even, then $k^2 \equiv 0(mod\ 4)$.

Thus, Cases 1 and 2 are both impossible; by contradiction, $p \equiv 1(mod\ 4)$.

Lemma 1 If an odd prime number $p \in \mathbb{Z}$ is such that $p \equiv 1(mod\ 4)$, then p divides $n^2 + 1$ for some $n \in \mathbb{Z}$.

Proof: Let $p \equiv 1(mod\ 4)$.

Then $p - 1$ is divisible by 4.

Then the order of the group of units of the quotient ring, $\left(\mathbb{Z}/_{p\mathbb{Z}}\right)^{\times}$ is divisible by 4.

But $\left(\mathbb{Z}/_{p\mathbb{Z}}\right)^{\times}$ is cyclic, since p is a prime.

Then $\left(\mathbb{Z}/_{p\mathbb{Z}}\right)^{\times}$ contains some cyclic subgroup of order 4.

Thus, $\exists [n] \in \left(\mathbb{Z}/_{p\mathbb{Z}}\right)^{\times}$ such that $o([n]) = 4$.

In that case, $[n]^4 = [1]$, so $n^4 \equiv 1(mod\ p)$, hence $p|n^4 - 1$.

Therefore, $p|(n^2 + 1)(n^2 - 1)$

Since p is prime, $p|n^2 + 1$, meaning $n^2 \equiv -1(mod\ p)$, or $p|n^2 - 1$, meaning $n^2 \equiv 1(mod\ p)$.

This implies that p divides $n^2 - 1$.

Lemma 2 If a prime number $p \in \mathbb{Z}$ is reducible in $\mathbb{Z}[i]$, then $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

Proof: Let p be reducible in $\mathbb{Z}[i]$. Then $\exists \alpha, \beta \in \mathbb{Z}[i]$, neither being units, with $p = \alpha\beta$.

In that case, $N(\alpha)N(\beta) = N(\alpha\beta) = N(p) = p^2$.

Since $\mathbb{Z}$ is a Euclidean Domain, it is a Unique Factorization domain, so this representation $N(\alpha)N(\beta) = p^2$ is unique.

Therefore, either one of $N(\alpha)$ and $N(\beta)$ is equal to 1 and the other is equal to p^2, or else both are equal to p.

Thus, $N(\alpha) = p$.

However, $\alpha = a + bi$ for some $a, b \in \mathbb{Z}$, so $N(\alpha) = a^2 + b^2$.

This indicates that $p = a^2 + b^2$.

Theorem (Fermat) Let $p \in \mathbb{Z}$ be an odd prime number. Then $p \equiv 1(mod\ 4)$ if and only if $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

($\Rightarrow$) Assume $p \equiv 1(mod\ 4)$.

Lemma 1: If an odd prime number $p \in \mathbb{Z}$ is such that $p \equiv 1(mod\ 4)$, then p divides the integer $n^2 + 1$ for some $n \in \mathbb{Z}$.

Then by Lemma 1, $p|n^2 + 1$ for some $n \in \mathbb{Z}$.

Therefore $p|(n + i)(n - i)$ in $\mathbb{Z}[i]$.

Assume for contradiction that p is irreducible in $\mathbb{Z}[i]$.

However, $\mathbb{Z}[i]$ is a Unique Factorization Domain, and so all irreducibles in $\mathbb{Z}[i]$ are also primes in $\mathbb{Z}[i]$, and so p is a prime in $\mathbb{Z}[i]$.

Thus, $p|n + i$ or $p|n - i$ in $\mathbb{Z}[i]$.

But then, for some $x + yi \in \mathbb{Z}[i]$, $n \pm i = (x + yi)p = xp + ypi$

Therefore $yp = \pm 1$.

The contradiction implies that p is reducible in in $\mathbb{Z}[i]$.

Lemma 2: If a prime number $p \in \mathbb{Z}$ is reducible in $\mathbb{Z}[i]$, then $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

Therefore, by Lemma 2, $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

Bibliography

- D. S. Dummit and R. M. Foote, *Abstract Algebra*, 3rd ed., John Wiley and Sons, 2004.