GAUSSIAN INTEGERS

ANAMITRO BISWAS

Email: anamitroappu@gmail.com

See the primes 1 modulo 4: $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$ etc. They turn out to be expressible as $p = x^2 + y^2$ where $x, y \in \mathbb{Z}$. In fact, this is true for all primes $p \in \mathbb{P}$, $p \equiv 1 \mod 4$. For proving this, we need the fact that the Gaussian integers $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ form an Euclidean domain, which implies it is a uniform factorization domain. Given $\alpha, \beta \in \mathbb{Z}[i]$ we need to prove that there exists $\gamma \in \mathbb{Z}[i]$ such that $\left|\frac{\alpha}{\beta} - \gamma\right| < 1$, where $|x + iy| = (x + iy)(x - iy) = x^2 + y^2$ for $x + iy \in \mathbb{Z}[i]$. But $\mathbb{Z}[i]$ forms a lattice in $\mathbb{C}$ with mesh diagonal length $\sqrt{2}$ and so there must be a $\gamma \in \mathbb{Z}[i]$ such that given $\alpha, \beta \in \mathbb{Z}[i]$, $\left|\frac{\alpha}{\beta} - \gamma\right| \leq \frac{1}{2}\sqrt{2} = \frac{1}{\sqrt{2}}$. Now, since the Gaussian integers are a UFD, what we need to prove is that p facts as $(x + iy)(x - iy)$ in $\mathbb{Z}[i]$, and is no more a prime.

Let $p = 4n+1$, $n \in \mathbb{N}$. By Wilson's theorem, $-1 \equiv (p-1) \mod p = [1.2 \ldots .(2n)]\,[(p-1)(p-2)\ldots(p-2n)] \equiv (2n)!\left[(-1)^{2n}(2n)!\right] \mod p = ((2n)!)^2 \equiv -1 \mod p$. Therefore $(2n)!$ is a solution to $x^2 + 1 \equiv 0 \mod p$. Now since $p \in \mathbb{P}$, $2n < p$, $p \nmid x = (2n)!$, i.e., $(x + i)(x - i)$ is divisible by p in $\mathbb{Z}[i]$ but $\frac{x}{p} \pm \frac{i}{p} \notin \mathbb{Z}[i]$, so p is not a prime in $\mathbb{Z}[i]$. Therefore there exist $x_1 + iy + 1, x_1 - iy_1 \in \mathbb{Z}[i]$ such that $p = x_1^+ y_1^2$.

When we study algebraic extension of a ring, the two most important points to cover are characterization of its prime elements and units. Having defined the ring of Gaussian integers, our next objective is to find all its units and primes. Define norm $N : \mathbb{Z}[i] \to \mathbb{Z}^+ \cup \{0\}$; $x + iy \mapsto (x + iy)(x - iy) = x^2 + y^2$. We know that $\alpha \in (\mathbb{Z}[i])^\times \Leftrightarrow N(\alpha) = 1$. For, if α is a unit, we find some $\beta \in \mathbb{Z}[i]$ such that $\alpha\beta = 1 \Rightarrow N(\alpha\beta) = N(1) = 1 \Rightarrow N(\alpha)N(\beta) = 1 \Rightarrow N(\alpha) = 1$. On the other hand, let $\alpha = a + bi$. Then $N(\alpha) = a^2 + b^2 = 1 \Rightarrow$ either $a \in \{\pm 1\}, b = 0$ or $a = 0, b \in \{\pm 1\}$. Therefore the units in $\mathbb{Z}[i]$ are $\{\pm 1, \pm i\}$, all of which have norm 1. So, we have found the units. And we know that $p \in \mathbb{P}$, $p \equiv 1 \mod 4$ are not primes in $\mathbb{Z}[i]$. But, $p \in \mathbb{P}$, $p \equiv 3 \mod 4$ are.

Because, let's say such a p can be factorized into non-units $\alpha\beta$. Then $N(p) = N(\alpha)N(\beta)$, i..e., $p^2 = N(\alpha)N(\beta)$ and since α, β are non-units, $N(\alpha) = N(\beta) = p$. Let $\alpha = a+bi$. Then $N(\alpha) = a^2+b^2 \in \{0 \mod 4, 1 \mod 4\} \to\leftarrow$.

We say that two elements a and b in a ring are *associated* if one can be obtained from the other through multiplication by a unit, and we write as: $a \sim b$. Let π be a prime in $\mathbb{Z}[i]$. Then upto association, π is one of the following:

(1) $\pi = 1 + i$;
(2) $\pi = a + bi$ where $a, b \in \mathbb{Z}$ such that $a^2 + b^2 = p \equiv 1 \mod 4$;
(3) $\pi = p \equiv 3 \mod 4$ where $p \in \mathbb{P}$.

In cases (1) and (2), if $\pi = \alpha\beta$, then $N(\pi) = N(\alpha)N(\beta) = p \in \mathbb{P}$. One of α and β is a unit. In (3), if $\pi = \alpha\beta$ where α, β are non-units, $p^2 = N(\alpha)N(\beta) \Rightarrow N(\alpha) = p$. If $\alpha = a + bi$, then $p = a^2 + b^2 \equiv 1 \mod 4 \to\leftarrow$.

FURTHER READING:

[DF] D. S. Dummit and R. M. Foote, *Abstract Algebra*, Prentice Hall ed. 2 (1991).
[N] J. Neukrich, *Algebraic Number Theory* tr. N. Schappacher, Springer (1999).