# UNIQUE FACTORIZATION IN EXOTIC NUMBER SYSTEMS

**Exercise 1**. a) Find the smallest positive integer $n$ for which $n^2 + n + 41$ is NOT a prime number. b) Show that for every prime divisor $p$ of $n^2 + n + 41$, we have $\left(\frac{-163}{p}\right) = 1$. (Hint: complete the square.)

The *Gaussian integers* are the set of complex numbers of the form $a+bi$, where $a$ and $b$ are ordinary integers. The set of Gaussian integers is notated $\mathbf{Z}[i]$. It is easy to see that Gaussian integers can be added, subtracted and multiplied to form new Gaussian integers. The *norm* of a Gaussian integer $\alpha = a + bi$ is $N(\alpha) = a^2 + b^2$. We have the rule $N(\alpha\beta) = N(\alpha)N(\beta)$.

**Exercise 2**. a) In the ordinary integers $\mathbf{Z}$, the only elements that have multiplicative inverses which are also integers are 1 and $-1$. These are the *units* of $\mathbf{Z}$. What are the units in $\mathbf{Z}[i]$? b) Let $\alpha$ and $\beta$ be two Gaussian integers. We say $\alpha$ divides $\beta$ if there is a third Gaussian integer $\gamma$ for which $\beta = \alpha\gamma$. Show that if $p$ is a prime integer, and a Gaussian integer $\alpha = a + bi$ divides $p$, then either $\alpha$ is a unit, or else it equals a unit multiple of $p$, or else $a^2 + b^2 = p$.

We say that two Gaussian integers $\alpha, \beta$ are *unit multiples* if there is some unit $u$ for which $\alpha = \beta u$. A Gaussian integer $\pi$ is *prime* if its only divisors are 1, $\pi$, and the unit multiples of those. For instance, $1 + i$, $1 + 2i$ and 3 are primes in $\mathbf{Z}[i]$. But 5 is not a prime in $\mathbf{Z}[i]$ because it factors: $5 = (1 + 2i)(1 - 2i)$. (The units themselves are not considered primes, nor is zero.)

How do you find primes in $\mathbf{Z}[i]$? One observation is that if $\pi = a + bi$ is a Gaussian integer, and $N(\pi) = a^2 + b^2 = p$ is itself a prime integer, then $\pi$ must be a prime. This is because if $\pi = \alpha\beta$, then $p = N(\pi) = N(\alpha)N(\beta)$. Then either $N(\alpha) = 1$ or $N(\beta) = 1$. We conclude that the only divisors of $\pi$ are either units or unit multiples of $\pi$ itself, which means that $\pi$ is prime.

In this situation, when $N(\pi) = p$ is a prime, we say that $\pi$ is a *split* prime.

**Exercise 3**. a) Find all the split primes $\pi$ with $N(\pi) < 20$. If $\pi$ is on your list, don't bother including unit multiples of $\pi$. b) Let $p$ be a prime integer. Suppose that $\pi$ is a prime Gaussian integer that divides $p$. Show that either $\pi$ is a split prime with $N(\pi) = p$, or else $\pi$ is a unit multiple of $p$ itself. In the latter case, we say that $\pi$ is an *inert* prime.

Thus the primes in $\mathbf{Z}[i]$ fall into two categories: The split primes, which are of the form $\pi = a + bi$ with norm $N(\pi) = a^2 + b^2 = p$ equal to an integer prime $p$, and the inert primes, which up to a unit multiple are already integer primes. A natural question is: Which integer primes $p$ are inert primes in $\mathbf{Z}[i]$, and which are norms of split primes?

**Exercise 4**. a) Show that if an odd integer prime $p$ is the sum of two squares, then it is congruent to 1 mod 4. b) Show that if $p$ is the sum of two squares, then it must be the norm of a split prime in $\mathbf{Z}[i]$. c) Show that if $p$ is not the sum of two squares, then it must be an inert prime.

Primes in $\mathbf{Z}[i]$ have the following nice property: if $\pi$ divides a product $\alpha\beta$ of Gaussian integers, then $\pi$ divides $\alpha$ or else $\pi$ divides $\beta$. This is an important property of Gaussian integers. It has the consequence that every Gaussian integer factors as a product of primes in a unique way.

**Exercise 5**. Show that if $p \equiv 1 \pmod 4$, then $p$ is the sum of two squares. Hint: Use the fact that $\left(\frac{-1}{p}\right) = 1$ to show that $p$ divides an integer of the form $n^2 + 1$. But then $n^2 + 1 = (n + i)(n - i)$...

We created the ring $\mathbf{Z}[i]$ by adding the element $i$ to the integers. The element $i$ is special because it is a root of the polynomial $X^2 + 1$. We can create other rings in a similar manner. Let $\mathbf{Z}[\sqrt{-5}]$ be the set of complex numbers of the form $a + b\sqrt{-5}$, where $a$ and $b$ are integers. Define the norm of such a number to be $N(a + b\sqrt{-5}) = a^2 + 5b^2$.

The elements 2 and 3 do not have any proper divisors in $\mathbf{Z}[\sqrt{-5}]$ other than $\pm 1$. Similarly, the elements $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ do not have any proper divisors either. But we have

$$2 \times 3 = 6 = (1 + \sqrt{-5}) \times (1 - \sqrt{-5}).$$

This is problematic because 2 does not divide either of $1 + \sqrt{-5}$ or $1 - \sqrt{-5}$. So $\mathbf{Z}[\sqrt{-5}]$ does not have the unique factorization property that $\mathbf{Z}[i]$ has. A fascinating research problem in number theory is the investigation of which number systems have unique factorization and which do not.

Let $j$ be one of the roots of the polynomial $X^2 + X + 41$, say $j = \frac{-1+\sqrt{-163}}{2}$. It is a surprising result that $\mathbf{Z}[j]$, the set of all complex numbers of the form $a + bj$, has the unique factorization property. In fact 163 is the largest number that has this property, a fact "known" to Gauss but not proved rigorously until 1952.

**Exercise 6**. In this exercise we explain the bizarre behavior of the polynomial $n^2 + n + 41$ discussed in Exercise 1.

a) If $\alpha = a + bj$, we define $N(\alpha)$ to be $\alpha\overline{\alpha}$, where $\overline{\alpha}$ is the complex conjugate of $\alpha$. What is $N(\alpha)$ in terms of $a$ and $b$?

b) Suppose that $\alpha$ belongs to $\mathbf{Z}[j]$. If $N(\alpha) > 1$, show that $N(\alpha) \geq 41$.

c) Let $n$ be an integer, $0 \leq n \leq 39$. Assume for parts c)-e) that $n^2 + n + 41$ is composite. Show that $n^2 + n + 41$ has a prime factor $p$ with $p < 41$.

d) Show that this prime $p$ must not remain a prime in $\mathbf{Z}[j]$. Hint: Assume that it is. Then since $p$ divides $n^2 + n + 41 = (n - j)(n - \overline{j})$, it must divide one of the factors. Derive a contradiction from this.

e) Since $p$ is not prime in $\mathbf{Z}[j]$, we must have $p = N(\pi)$ for some prime $\pi$ of $\mathbf{Z}[j]$. But then by part b), $p > 41$, contradiction. Therefore $n^2 + n + 41$ must be prime for $n = 0, \ldots, 39$.