0. Example of non-unique factorization

We denote by $\mathbf{Z}$ the set of integers, $\mathbf{Z} = \{0, 1, -1, 2, -2, 3, -3, \dots\}$. Recall that prime numbers are $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \dots$.

Consider the set of numbers

$$\mathbf{Z}[\sqrt{-5}] = \{a = x + y\sqrt{-5} \mid x, y \in \mathbf{Z}\}.$$

We can add, subtract and multiply these numbers:

$$(x + y\sqrt{-5})(x_1 + y_1\sqrt{-5}) = (xx_1 - 5yy_1) + (xy_1 + yx_1)\sqrt{-5}.$$

We define the *norm* map

$$N\colon \mathbf{Z}[\sqrt{-5}] \to \mathbf{Z},\ N(x + y\sqrt{-5}) = x^2 + 5y^2.$$

The norm map has the following properties:

- $N(a) \in \mathbf{Z}$ (indeed, $x^2 + 5y^2 \in \mathbf{Z}$);
- $N(a) \geq 0$ (indeed, $x^2 + 5y^2 \geq 0$);
- $N(a) = 0$ if and only if $a = 0$ (indeed, if $x^2 + 5y^2 = 0$, then $x = 0$ and $y = 0$);
- $N(ab) = N(a)N(b)$ (indeed, this is true for complex numbers; one can also check immediately that

$$(xx_1 - 5yy_1)^2 + 5(xy_1 + yx_1)^2 = (x^2 + 5y^2)(x_1^2 + 5y_1^2)\ ).$$

Definition 0.1. A number $a \in \mathbf{Z}[\sqrt{-5}]$ is called *invertible*, if there exists $b \in \mathbf{Z}[\sqrt{-5}]$ such that $ab = 1$.

Lemma 0.2. *A number $a \in \mathbf{Z}[\sqrt{-5}]$ is invertible if and only if $a = \pm 1$.*

Proof. Clearly 1 and -1 are invertible. Conversely, assume that $ab = 1$. Then

$$N(ab) = N(1) = 1,$$

hence

$$N(a)N(b) = 1,$$

hence $N(a) = 1$. Write $a = x + y\sqrt{-5}$, then $N(a) = x^2 + 5y^2$. We obtain

$$x^2 + 5y^2 = 1,$$

hence $y = 0$ and $x = \pm 1$. Thus $a = 1$ or $a = -1$. □

Definition 0.3. A number $a = x + y\sqrt{-5}$ is called *irreducible* (in $\mathbf{Z}[\sqrt{-5}]$) if in any decomposition

$$a = bc$$

either b is invertible (i.e $b = \pm 1$) or c is invertible (i.e $c = \pm 1$).

Example 0.4. In $\mathbf{Z}$ the numbers 2 and -2 are irreducible, while 6 and -6 are reducible, $-6 = 2 \cdot (-3)$.

Amazing example 0.5.

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

By the way, in $\mathbf{Z}$ we also have

$$4 \cdot 9 = 6 \cdot 9.$$

But 4, 9, and 6 are reducible, and we obtain

$$2^2 \cdot 3^2 = (2 \cdot 3)(2 \cdot 3)\ -$$

the same decomposition into irreducibles! And for 6 in $\mathbf{Z}$ we have

$$6 = 2 \cdot 3 = (-2)(-3).$$

Here

$$-2 = 2 \cdot (-1), \quad -3 = 3 \cdot (-1),$$

and -1 is invertible. Again we have essentially the same decomposition. But in our Example 0.5 we have two different decompositions. What is amazing is that they are two different decompositions into *irreducibles!*

Claim 0.6. *The four numbers* $2,\ 3,\ 1+\sqrt{-5},\ 1-\sqrt{-5}$ *are irreducible in in* $\mathbf{Z}[\sqrt{-5}]$.

Proof. We prove that 3 is irreducible. Assume that $3 = ab$. Then

$$N(3) = N(ab) = N(a)N(b).$$

But $N(3) = 3^2 + 5 \cdot 0^2 = 9$. Thus

$$N(a)N(b) = 9.$$

It follows that $N(a) = 1, 3, 9$.

If $N(a) = 1$, then a is invertible. If $N(a) = 9$, then $N(b) = 1$ and b is invertible. At last, if $N(a) = 3$, $a = x + y\sqrt{-5}$, then

$$x^2 + 5y^2 = 3,$$

and we obtain that $y = 0$, hence $x^2 = 3$, which is clearly impossible. Thus the case $N(a) = 3$ is impossible. We have proved that 3 is irreducible in $\mathbf{Z}[\sqrt{-5}]$.

We prove that 2 is irreducible. Assume that $2 = ab$. Then

$$N(a)N(b) = 4.$$

Since the equation

$$x^2 + 5y^2 = 2$$

has no solutions in integers $x, y \in \mathbf{Z}$, we conclude that either $N(a) = 1$ or $N(b) = 1$. Thus 2 is irreducible in $\mathbf{Z}[\sqrt{-5}]$.

We prove that the numbers $1 \pm \sqrt{-5}$ are irreducible. Assume that $1 \pm \sqrt{-5} = ab$. Then

$$N(a)N(b) = 6.$$

Since $N(a) \neq 2, 3$, we see that either $N(a) = 1$ or $N(a) = 6$ (then $N(b) = 1$). Thus the numbers $1 \pm \sqrt{-5}$ are irreducible. □

Claim 0.6 shows that in $\mathbf{Z}[\sqrt{-5}]$ the number 6 has two essentially different decompositions into irreducible factors. We see that there is no unique factorization into irreducibles in $\mathbf{Z}[\sqrt{-5}]$.

Now consider the set of Gaussian integers

$$\mathbf{Z}[i] = \{a = x + yi \mid x, y \in \mathbf{Z}\}, \text{ where } i = \sqrt{-1}.$$

What are the invertible elements of $\mathbf{Z}[i]$? We will prove later that $\mathbf{Z}[i]$ has unique factorization into irreducibles and describe the irreducible elements in $\mathbf{Z}[i]$.

We see that it is not evident that even $\mathbf{Z}$ has unique factorization into irreducibles (primes). We will prove this assertion in the next section.