

Math Circles: Number Theory II

Centre for Education in
Mathematics and Computing

March 2, 2011

1 The Fundamental Theorem of Arithmetic

Recall that the *fundamental theorem of arithmetic* states that every integer has a unique prime factorization.

Exercise 1.1. Factor each of the following integers:

1. 78
2. 96
3. 113
4. 114
5. 16380
6. -6
7. 1
8. 0

Question 1.2. Taking into account the above examples, how would you formulate the fundamental theorem of arithmetic precisely?

Question 1.3. Does the fundamental theorem of arithmetic hold in other number systems?

In order to answer that question, we would have to ask:

Question 1.4. What *are* some number systems other than the integers?

Partial answer. Some examples of number systems might include:

- \mathbb{N} (the *natural numbers*).
- \mathbb{Z} (the *integers*).
- \mathbb{Q} (the *rational numbers*).
- \mathbb{R} (the *real numbers*).
- \mathbb{C} (the *complex numbers*).

- $\mathbb{R}[x]$ (the set of *polynomials* over the real numbers)
- ... and many more.

Note that some of these number systems are more complete than others. For example, subtraction is not well defined in \mathbb{N} (that is, $a - b$ does not always exist: $3 - 5$ is not in \mathbb{N}). Division is not well defined in \mathbb{N} and \mathbb{Z} . (Is it well defined in the others? What about $1/0$?) \square

Question 1.5. What does it mean for unique prime factorization to hold in \mathbb{N} ? In \mathbb{Z} ? In \mathbb{Q} ? In \mathbb{R} ?

To answer this question, we might define a *prime* (in any number system) to be a number whose only divisors are 1 and itself.

In \mathbb{Z} , is 2 a prime? Is 1 a prime? Is -2 a prime? Is -1 a prime? How would you factor -6 without negative primes?

Suppose that we resolve this problem. We have another problem. What is a *divisor*?

Definition 1.6. In any number system, we say that a *divides* b , or that a is a *divisor* of b , if there exists a number k such that $a \times k = b$. If a divides b , then we write $a \mid b$. If not, we write $a \nmid b$.

Exercise 1.7. True or false? In \mathbb{N} ? In \mathbb{Z} ? In \mathbb{R} ?

- $2 \mid 6$
- $2 \mid 9$
- $6 \mid 9$
- $2 \mid 1$
- $2 \mid 0$
- $0 \mid 2$

True or false? In \mathbb{Z} ? In \mathbb{R} ?

- $2 \mid -2$
- $2 \mid -1$
- $-1 \mid 2$
- $-1 \mid -2$

In light of the above examples, how would you define *prime*? How would you define *unique prime factorization*?

2 Unique prime factorization in $\mathbb{Z}[i]$

The *imaginary numbers* are the number system obtained by taking the set

$$\{a + bi : a, b \in R\}$$

where i is defined to be $\sqrt{-1}$, and R is an existing number system. (If you are familiar with imaginary numbers, then you will recognize that the idea is to add a new *imaginary* number $i = \sqrt{-1}$, which does not normally exist in a number system.)

By altering the choice of R , we can create lots of new number systems:

- If we take $R = \mathbb{Z}$, we get $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ (the *Gaussian integers*).
- If we take $R = \mathbb{Q}$, we get $\mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}$ (the *Gaussian rationals*).
- If we take $R = \mathbb{R}$, we get $\mathbb{R}[i] = \{a + bi : a, b \in \mathbb{R}\}$ (the *complex numbers*).

Exercise 2.1. Using our previous definition of prime factorization, find the prime factorizations of the following numbers in $\mathbb{Z}[i]$.

- $3 + 5i$
- $4 + 7i$
- $7 + 11i$

Solution. We can actually get lots of prime factorizations:

$$\begin{aligned} 4 + 7i &= (1 - 2i)(-2 + 3i) = (2 + i)(3 + 2i) \\ 3 + 5i &= (1 + i)(4 + i) = (1 - i)(-1 + 4i) \\ 7 + 11i &= (1 - i)(2 + i)(1 + 4i) = \dots? \quad \square \end{aligned}$$

How did we find these factorizations? The trick is to multiply each number $a + bi$ by its *conjugate* $a - bi$.

Example 2.2. Factor $3 + 5i$.

Solution. Suppose

$$3 + 5i = (a_1 + a_2i)(b_1 + b_2i)$$

for unknown a_1, a_2, b_1, b_2 . We multiply both sides by their conjugates:

$$\begin{aligned} (3 + 5i)(3 - 5i) &= (a_1 + a_2i)(b_1 + b_2i)(a_1 - a_2i)(b_1 - b_2i) \\ 3^2 + 5^2 &= (a_1^2 + a_2^2)(b_1^2 + b_2^2) \\ 34 &= (a_1^2 + a_2^2)(b_1^2 + b_2^2) \end{aligned}$$

Since $a_1^2 + a_2^2$ must be a non-trivial divisor of 34, we conclude that $a_1^2 + a_2^2$ is equal to either 2 or 17. Without loss of generality, suppose $a_1^2 + a_2^2 = 2$. Then $a_1 = \pm 1$ and $a_2 = \pm 1$. If we guess (for example) $a_1 = a_2 = 1$, then

$$\frac{3 + 5i}{1 + i} = \frac{(3 + 5i)(1 - i)}{(1 + i)(1 - i)} = \frac{3 - 3i + 5i - 5i^2}{2} = \frac{8 + 2i}{2} = 1 + 4i,$$

so it turns out our guess was right, and $3 + 5i = (1 + i)(1 + 4i)$.

If our guess is wrong, then we can convert it into a correct guess by making any one of the following changes:

- Negating a_1 ,
- Negating a_2 ,
- Switching a_1 and a_2 .

(*Why?*) □

Question 2.3. Does unique prime factorization hold in $\mathbb{Z}[i]$?

Exercise 2.4. Factor each of the following numbers in $\mathbb{Z}[i]$:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \dots$$

Solution. The numbers 3, 7, 11, 19, 23 are prime in $\mathbb{Z}[i]$. The others factor as

$$\begin{aligned} 2 &= 1^2 + 1^2 = (1 + i)(1 - i) \\ 5 &= 2^2 + 1^2 = (2 + i)(2 - i) \\ 13 &= 3^2 + 2^2 = (3 + 2i)(3 - 2i) \\ 17 &= 4^2 + 1^2 = (4 + i)(4 - i) \\ 29 &= 5^2 + 2^2 = (5 + 2i)(5 - 2i) \end{aligned} \quad \square$$

Question 2.5. Find a simple rule for determining if a prime p in \mathbb{Z} is a prime in $\mathbb{Z}[i]$. What does this have to do with representations of the form $p = a^2 + b^2$?

Solution. A prime p in \mathbb{Z} is of the form $a^2 + b^2$ if and only if it factors in $\mathbb{Z}[i]$, and if and only if it is not of the form $p = 4k + 3$. (Exercise: Prove this.) \square

Theorem 2.6. *The primes in $\mathbb{Z}[i]$ are:*

1. $\pm 1 \pm i$,
2. $\pm a \pm bi$, where $a^2 + b^2 = p$ is prime in \mathbb{Z} , and p is of the form $4k + 1$,
3. $\pm p, \pm pi$, where p is prime in \mathbb{Z} and of the form $4k + 3$.

3 Unique factorization in $\mathbb{Z}[\sqrt{2}]$

Consider the number system

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}.$$

Exercise 3.1. Factor each of the following numbers in $\mathbb{Z}[\sqrt{2}]$:

- 2
- 3
- 7
- 17
- $3 - \sqrt{2}$
- $5 + 3\sqrt{2}$
- $11 + 2\sqrt{2}$
- $18 - 13\sqrt{2}$

What is the greatest common divisor of $5 + 3\sqrt{2}$ and $3 - \sqrt{2}$? Of $11 + 2\sqrt{2}$ and $18 - 13\sqrt{2}$?

Question 3.2. Does the equation

$$1 = (3 + 2\sqrt{2})(3 - 2\sqrt{2})$$

represent a prime factorization of 1 in $\mathbb{Z}[\sqrt{2}]$? (!!)

Exercise 3.3. Find some more “factorizations” of 1 in $\mathbb{Z}[\sqrt{2}]$.

Solution. We have

$$\begin{aligned} 1 &= (3 + 2\sqrt{2})^2(3 - 2\sqrt{2})^2 = (17 + 12\sqrt{2})(17 - 12\sqrt{2}) \\ 1 &= (3 + 2\sqrt{2})^3(3 - 2\sqrt{2})^3 = (99 + 70\sqrt{2})(99 - 70\sqrt{2}) \\ &\vdots \end{aligned}$$

and so on. □

Question 3.4. Does the equation

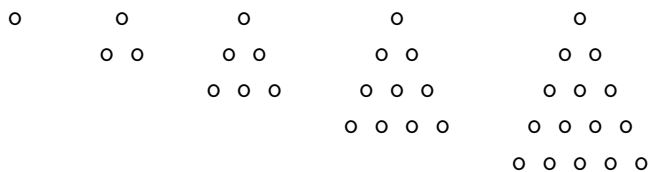
$$17 = (1 - 3\sqrt{2})(1 + 3\sqrt{2}) = (5 + 2\sqrt{2})(5 - 2\sqrt{2})$$

represent two different factorizations of 17 in $\mathbb{Z}[\sqrt{2}]$?

3.1 Squares and triangles

An integer is a *square* if it is equal to a perfect square. The first few squares are: 1, 4, 9, 16, 25, ...

An integer is a *triangle* if it is equal to the number of points in an equilateral triangular lattice. The first few triangles are: 1, 3, 6, 10, 15, ... Here is a picture of these numbers:



Question 3.5. Find all integers which are simultaneously squares and triangles. (For example, 1 and 36 are each simultaneously a square and a triangle.)

Solution. The squares are given by the formula m^2 for $m \in \mathbb{N}$. A formula for the n -th triangular number is

$$\frac{n^2 + n}{2}.$$

(*Why?*) Setting these equal, we find

$$\begin{aligned} m^2 &= \frac{n^2 + n}{2} \\ 2m^2 &= n^2 + n \end{aligned}$$

We then complete the square to obtain

$$\begin{aligned} 2m^2 + \frac{1}{4} &= n^2 + n + \frac{1}{4} \\ 2m^2 + \frac{1}{4} &= \left(n + \frac{1}{2}\right)^2 \\ 8m^2 + 1 &= (2n + 1)^2 \end{aligned}$$

Finally, we substitute $y = 2m$ and $x = 2n + 1$ to get

$$\begin{aligned}2y^2 + 1 &= x^2 \\1 &= x^2 - 2y^2 \\1 &= (x + y\sqrt{2})(x + y\sqrt{2}).\end{aligned}$$

We see that solutions to this problem correspond *exactly* to factorizations of 1 in $\mathbb{Z}[\sqrt{2}]$. Hence we can use our answer to Exercise 3.3 to solve this problem as well. \square

4 Exercises

1. Consider the number system

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}.$$

Does the equation

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

show that unique prime factorization does not hold in $\mathbb{Z}[\sqrt{-5}]$?

2. (A challenge from Fermat to the English mathematicians) Find all integers x, y such that $y^2 = x^3 - 2$. Hint: Use the equation

$$y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2})$$

together with unique prime factorization in $\mathbb{Z}[\sqrt{-2}]$.

3. Make a list of all the divisors of $8 - 2\sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$. Make a list of all the divisors of $1 + 5\sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$. Find the greatest common divisor of $8 - 2\sqrt{-5}$ and $1 + 5\sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$.
4. Find two different factorizations of 6 in $\mathbb{Z}[\sqrt{10}]$. Does unique prime factorization hold in $\mathbb{Z}[\sqrt{10}]$?
5. For which integers d does unique prime factorization hold in $\mathbb{Z}[\sqrt{d}]$?