

## NUMBER SYSTEMS

Number theory is the study of the integers. We denote the set of integers by  $\mathbb{Z}$ :

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

The integers have two operations defined on them, addition and multiplication, which are commutative ( $a + b = b + a$ ,  $ab = ba$ ) and associative ( $a + (b + c) = (a + b) + c$ ,  $a(bc) = (ab)c$ ) and which interact via the distributive law ( $a(b + c) = ab + ac$ ). These operations have neutral elements 0 and 1 respectively (if  $a$  is an integer,  $a + 0 = a$  and  $a \cdot 1 = a$ ). Notice also that each integer can be negated ( $a + (-a) = 0$ ). In modern algebra language, a set having the aforementioned properties is called a *commutative ring*. The two operations in  $\mathbb{Z}$  are not “created equal”, however; while every integer can be negated (for example,  $3 + (-3) = 0$ ), not every integer can be inverted (for example, there is no integer  $a$  such that  $3a = 1$ ). Indeed, the only integers whose reciprocals are also integers are 1 and  $-1$ . In general, an element  $a$  of a commutative ring is called a *unit* if there is an element  $b$  of the ring such that  $ab = 1$ .

The *rational numbers*, denoted by  $\mathbb{Q}$ , are all the ratios of integers:

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z} \text{ and } b \neq 0 \right\}$$

(of course, we consider  $\frac{4}{6}$  and  $\frac{2}{3}$  to be the same element of  $\mathbb{Q}$ ). Notice that, like  $\mathbb{Z}$ ,  $\mathbb{Q}$  is a commutative ring, but that any nonzero element of  $\mathbb{Q}$  can be inverted (if  $\frac{a}{b} \in \mathbb{Q}$  and  $a \neq 0$ , then certainly  $\frac{b}{a} \in \mathbb{Q}$  also). Commutative rings having this additional property are called *fields*.

Another field you are familiar with is the real numbers, which we will denote by  $\mathbb{R}$ . Notice that  $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ . We know how  $\mathbb{Z}$  sits in  $\mathbb{R}$  (imagine a number line with the integers marked off). You may have thought less about how  $\mathbb{Q}$  sits in  $\mathbb{R}$ .

**Proposition 1.** *Between any two real numbers, there is a rational number.*

*Proof.* Let  $a, b \in \mathbb{R}$ ,  $a < b$ . We can find a positive integer  $n$  such that  $\frac{1}{n} < b - a$ . Then at least one of the rational numbers

$$\left\{ \dots, \frac{-2}{n}, \frac{-1}{n}, 0, \frac{1}{n}, \frac{2}{n}, \dots \right\}$$

lies between  $a$  and  $b$ . □

Because of Proposition 1, we say that  $\mathbb{Q}$  is *dense* in  $\mathbb{R}$ . However, not all real numbers are rational; a real number which is not rational is called *irrational*.

**Proposition 2.** *e is irrational.*

*Proof.* Suppose that  $e$  were rational. Then  $e = a/b$  for some positive integers  $a$  and  $b$ . It follows that the number  $\alpha$  defined by

$$\alpha = b! \left( e - 1 - \frac{1}{1!} - \frac{1}{2!} - \frac{1}{3!} - \cdots - \frac{1}{b!} \right)$$

is an integer (imagine multiplying the  $b!$  through), and since  $e$  is defined by

$$e = \sum_{n=0}^{\infty} \frac{1}{n!},$$

$\alpha$  is positive. But the definition of  $e$ , along with the formula for the sum of a convergent geometric series, gives that

$$\begin{aligned} \alpha &= b! \left( \frac{1}{(b+1)!} + \frac{1}{(b+2)!} + \cdots \right) = \frac{1}{b+1} + \frac{1}{(b+1)(b+2)} + \cdots \\ &< \frac{1}{b+1} + \frac{1}{(b+1)^2} + \cdots = \frac{\frac{1}{b+1}}{1 - \frac{1}{b+1}} = \frac{1}{b} \leq 1. \end{aligned}$$

We find that  $\alpha < 1$ , a contradiction since  $\alpha$  is a positive integer.  $\square$

Note that  $e$  is an infinite sum of positive rational numbers; as such, it is the limit of an increasing sequence of rational numbers (namely, the sequence of partial sums), yet  $e$  itself is not rational. Indeed,  $\mathbb{R}$  has the property that every increasing sequence of rational numbers is either unbounded or converges to an element of  $\mathbb{R}$ . In fact,  $\mathbb{R}$  is the smallest such field, in the sense that any other field having this property contains  $\mathbb{R}$ .

We will see more irrational numbers later; indeed, it turns out that the irrationals are much more numerous than the rationals.

Another field that you may have worked with is the field of *complex numbers*  $\mathbb{C}$ :

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\},$$

where  $i = \sqrt{-1}$ . Many of the commutative rings that we study in these notes are contained in  $\mathbb{C}$ .

## DIVISIBILITY

Let us first focus on the integers  $\mathbb{Z}$ , and study their multiplicative structure. We begin by discussing how integers break down into simpler multiplicative parts.

*Definition 3.* If  $a, b \in \mathbb{Z}$  and  $b \neq 0$ , we say that  $b$  divides  $a$  if there is an integer  $c$  such that  $a = bc$ .

We denote “ $b$  divides  $a$ ” by  $b \mid a$ ; synonyms for this that you may be familiar with are “ $b$  is a divisor of  $a$ ”, “ $b$  is a factor of  $a$ ”, “ $a$  is a multiple of  $b$ ” and “ $a$  is divisible by  $b$ ”. If  $b$  is not a divisor of  $a$ , we write  $b \nmid a$ .

*Example 4.*  $3 \mid 12$ ,  $7 \nmid 16$

*Example 5.* The positive divisors of 30 are 1, 2, 3, 5, 6, 10, 15 and 30.

Notice that any nonzero integer  $a$  is a divisor of 0 ( $0 = a \cdot 0$ ) and is divisible by 1 ( $a = 1 \cdot a$ ); a direct consequence of the former statement is the surprisingly useful

**Corollary 6.** *If  $a$  is an integer, and there is a positive integer  $b$  such that  $b \nmid a$ , then  $a \neq 0$ .*

We have only discussed divisibility in  $\mathbb{Z}$ ; notice that the notion of divisibility is trivial in  $\mathbb{Q}$  (i.e. if  $b$  is a nonzero rational number, then  $b$  divides every rational number) since we can invert any nonzero element of  $\mathbb{Q}$ . Indeed, divisibility is a trivial notion in every field. Therefore, when we discuss divisibility, we will mean it in the context of the integers, unless otherwise stated.

**Proposition 7.** *Let  $a, b, c \in \mathbb{Z}$ .*

- (1) *If  $a \mid b$  and  $b \mid c$ , then  $a \mid c$ .*
- (2) *If  $a \mid b$  and  $a \mid c$ , then for any integers  $x$  and  $y$ ,  $a \mid (bx + cy)$ .*

*Proof.* (1) Since  $a \mid b$  and  $b \mid c$ , there are integers  $m$  and  $n$  such that  $b = ma$  and  $c = nb$ . Then  $c = n(ma) = (nm)a$ , so  $a \mid c$ .

(2) Since  $a \mid b$  and  $a \mid c$ , there are integers  $m$  and  $n$  such that  $b = ma$  and  $c = na$ . Then

$$bx + cy = (ma)x + (na)y = (mx + ny)a,$$

so  $a \mid (bx + cy)$ . □

## THE PRIMES

Notice that every integer  $a > 1$  has at least two positive divisors, namely 1 and  $a$ ; these are sometimes called the trivial divisors of  $a$ . If  $d \mid a$  and  $1 < d < a$ ,  $d$  is called a *proper* divisor of  $a$ .

*Definition 8.* An integer  $p > 1$  is called *prime* if its only positive divisors are 1 and  $p$  (i.e., if it has no proper divisors). An integer  $n > 1$  that is not prime is called *composite*.

*Example 9.* The first five prime numbers are 2, 3, 5, 7 and 11.

Prime numbers can be thought of, then, as multiplicatively the simplest positive integers. We now demonstrate their central place in multiplicative number theory.

**Proposition 10.** *If a positive integer  $n$  is composite, then the smallest proper divisor of  $n$  is prime.*

*Proof.* Let  $d$  be the smallest proper divisor of  $n$ . If  $d$  had a proper divisor  $m$ , then by Proposition 7 (1),  $m$  would be a proper divisor of  $n$ . But  $m < d$ , so we have a contradiction. Therefore  $d$  has no proper divisors, i.e.,  $d$  is prime.  $\square$

**Theorem 11.** *Every integer  $n > 1$  is a product of prime numbers.*

*Proof.* By induction. Since 2 is prime, the theorem is certainly true for  $n = 2$ . Now suppose it is true for all the integers from 2 up to  $n$ . If  $n + 1$  is prime, the theorem is true for  $n + 1$ . If  $n + 1$  is composite, then by Proposition 10, it has a prime divisor  $p$ . Writing  $n + 1 = mp$ , we see that  $2 \leq m \leq n$ . By the induction hypothesis  $m$  is a product of primes, and therefore so is  $n + 1 = mp$ .  $\square$

*Example 12.*  $84 = 2 \cdot 42 = 2 \cdot 2 \cdot 21 = 2 \cdot 2 \cdot 3 \cdot 7$

We see that the primes are the multiplicative building blocks of  $\mathbb{Z}$ , and therefore it is natural to study them as a distinguished set. One obvious question to ask is “how many primes are there?”

**Theorem 13.** *(Euclid) There are infinitely many prime numbers.*

*Proof.* Let  $S$  be any finite set of prime numbers. Consider the integer

$$n = 1 + \prod_{p \in S} p.$$

If  $n$  is prime, then  $n \notin S$ , since  $n$  is larger than any element of  $S$ . If  $n$  is composite, then by Proposition 10,  $n$  has a prime factor  $q$ . Notice that  $q \notin S$ , for if it were in  $S$ , then it would divide  $n - 1 = \prod_{p \in S} p$ , and then by Proposition 7 it would divide  $n - (n - 1) = 1$ , a contradiction. In any case,  $S$  does not contain all of the primes.  $\square$

Now that we have shown that there are infinitely many primes, let us consider the question of identifying the primes among all the positive

integers. Suppose we start from the very definition of a prime number: an integer  $n > 1$  with no proper divisors. We can immediately see a foolproof way to determine whether a positive integer  $n$  is prime: search for proper divisors of  $n$ ; if we find one,  $n$  is not prime, and if we do not find any,  $n$  is prime. Since a proper divisor  $d$  of  $n$  satisfies  $1 < d < n$ , we know that this algorithm will involve no more than  $n - 2$  steps.

Now that we have an algorithm, let us consider how to make it more efficient. First of all, let us note the obvious fact that the algorithm need not involve  $n - 2$  steps for every  $n$ . Indeed, if we find a proper divisor of  $n$ , we may terminate our algorithm immediately at that point and conclude that  $n$  is not prime. In the extreme case that  $n$  is composite and the first integer we check happens to be a divisor of  $n$ , our algorithm consists of just one step. In general, then, the efficiency of our algorithm will depend partly upon our testing the integers that are most likely to be divisors of  $n$  first. Fortunately this is not difficult to do, because we know that one half of the positive integers are divisible by 2, one third of the positive integers are divisible by 3, and so on. Therefore we should test the integers for divisors of  $n$  in increasing order.

Notice that if  $n$  is not prime and we search in this way, we will automatically find the smallest proper divisor  $d$  of  $n$  first. Recall that, by Proposition 10,  $d$  is prime. We now prove another very important property of  $d$ .

**Proposition 14.** *If  $n$  is composite and  $d$  is the smallest proper divisor of  $n$ , then  $d \leq \sqrt{n}$ .*

*Proof.* Consider the alternative. □

Combining Propositions 10 and 14, we obtain the following

*Algorithm 15.* (for determining whether  $n$  is prime) Search for divisors of  $n$  among the primes  $\leq \sqrt{n}$ , in increasing order beginning with 2. If a divisor is found, we conclude that  $n$  is composite and stop the search. If a divisor is not found, we conclude that  $n$  is prime.

*Example 16.* 113 is prime, because  $\sqrt{113} = 10.63\dots$  and 113 is not divisible by 2, 3, 5 or 7.

Not a bad test; we don't need to check all the integers up to  $n$  for divisors, just those up to  $\sqrt{n}$ , and among these we only need to consider the primes.

There is something about our primality test that may bother you: to use it to test the primality of  $n$ , we need to have a list of the primes

$\leq \sqrt{n}$ . How do we find such a list? It turns out that we have an efficient way to find one, and for this we may thank the ancient Greek Eratosthenes. This process involves many of the ideas we used in deriving Algorithm 15.

*Algorithm 17.* (Sieve of Eratosthenes, for finding all the primes  $\leq m$ ) List the integers from 2 to  $m$ , then apply the following iterative procedure to this list. The integers not eliminated in this process are the primes  $\leq m$ .

(1) Determine the smallest integer  $p$  in the list.

(2) If  $p > \sqrt{m}$ , stop. If  $p \leq \sqrt{m}$ , circle it and eliminate all multiples of  $p$ , except for  $p$  itself, from the list and go back to step (1).

*Proof that Algorithm 17 works.* First, it is clear that in the algorithm only composite numbers are eliminated. Let us now show that the circled numbers are all primes. We do this by induction. Clearly 2 is the smallest circled integer, and it is prime. Now suppose that the first  $k$  circled integers are primes. The sieve removed all of the multiples of these  $k$  primes (except themselves); hence the  $(k + 1)$ st circled integer is not divisible by any of the primes that are smaller than it, and is therefore prime itself by Proposition 10. Finally, what about the remaining uncircled numbers? They remain because they are not multiples of any of the circled primes, which as we have seen are all the primes  $\leq \sqrt{m}$ ; by Propositions 10 and 14, then, the remaining numbers are also prime.

## COMMON DIVISORS

Consider the following problem: we wish to tile a rectangular floor that is 12 feet by 18 feet. For ease of cutting, we wish to use tiles that are square, of uniform size, and have integral side length  $s$  (in feet). Given these constraints, we would like to minimize the number of tiles we use (so as to minimize the amount of cutting). How shall we do this? Since we are using tiles of uniform size, it is clear that this is equivalent to finding the largest usable tile. If we use  $m$  rows and  $n$  columns of tiles, then, we have the following relationships:

$$ms = 18 \quad \text{and} \quad ns = 12.$$

These imply that  $s$  is a divisor of both 18 and 12, so the maximal  $s$  is the largest integer that is a divisor of both 18 and 12, namely 6.

*Definition 18.* If  $m$  and  $n$  are nonnegative integers,  $d$  is a *common divisor* of  $m$  and  $n$  if  $d \mid m$  and  $d \mid n$ . If  $m$  and  $n$  are not both zero, the greatest common divisor (gcd) of  $m$  and  $n$  is denoted by  $(m, n)$ .

*Example 19.* The positive divisors of 20 are  $\{1, 2, 4, 5, 10, 20\}$ , and those of 35 are  $\{1, 5, 7, 35\}$ . The common divisors of 20 and 35 are  $\{1, 5\}$ , and so  $(20, 35) = 5$ .

*Example 20.* If  $m$  is a positive integer, then  $(m, 0) = m$ , since  $m$  is the largest divisor of  $m$  and any positive integer divides zero.

We see that computing the gcd of two positive integers can always be done in a straightforward way: list the divisors of each, and find the largest integer that appears in both lists. For large numbers, however, this procedure can become quite unwieldy. For example, 2310 has 32 divisors, and 1092 has 24 divisors; we might hope that there is a quicker way to find  $(2310, 1092)$ . Indeed, Euclid discovered an algorithm for doing this which has not been significantly improved to this date.

*Algorithm 21.* (Division Algorithm) Let  $m$  and  $n$  be positive integers. Then there exist unique integers  $q$  and  $r$  such that

$$n = mq + r$$

and  $0 \leq r < m$ .

*Proof.* Let  $q = \lfloor n/m \rfloor$  (recall that if  $r \in \mathbb{R}$ ,  $\lfloor r \rfloor$  denotes the largest integer that is less than or equal to  $r$ ). Since

$$(n/m) - 1 < \lfloor n/m \rfloor \leq n/m,$$

it follows that

$$0 = n - m(n/m) \leq n - mq < n - m((n/m) - 1) = m,$$

so let  $r = n - mq$ .

For uniqueness, suppose

$$n = mq_1 + r_1 = mq_2 + r_2$$

where  $0 \leq r_1, r_2 < m$ . Without loss we may assume that  $r_1 \leq r_2$ . Subtracting our two expressions for  $n$ , we find that

$$m(q_1 - q_2) = r_2 - r_1.$$

Hence  $m \mid (r_2 - r_1)$ . Since  $0 \leq r_2 - r_1 < m$ , it follows that  $r_2 - r_1 = 0$ , so  $r_2 = r_1$ . Then our last displayed equation gives  $m(q_1 - q_2) = 0$ , and since  $m \neq 0$ , it must be that  $q_1 - q_2 = 0$ , so  $q_1 = q_2$ .  $\square$

*Example 22.* If we divide  $m = 7$  into  $n = 38$ , we get a quotient of  $q = 5$  and a remainder of  $r = 3$ .

Euclid's algorithm combines the division algorithm with the following

**Proposition 23.** *Let  $m, n$  and  $r$  be as in the division algorithm. Then  $(m, n) = (m, r)$ .*

*Proof.* By definition  $(m, n)$  divides  $m$  and  $n$ , and since  $r = n - mq$ , by Proposition 7 (2),  $(m, n)$  divides  $r$ . Since  $(m, n)$  is a common divisor of  $m$  and  $r$ , we have that  $(m, n) \leq (m, r)$ . On the other hand,  $(m, r)$  divides  $m$  and  $r$ , and since  $n = mq + r$ , Proposition 7 (2) tells us that  $(m, r)$  divides  $n$ . Hence  $(m, r)$  is a common divisor of  $m$  and  $n$ , and therefore  $(m, r) \leq (m, n)$ . We conclude that  $(m, n) = (m, r)$ .  $\square$

*Algorithm 24.* (Euclidean Algorithm) Let  $m$  and  $n$  be positive integers with  $m < n$ . By the division algorithm, we have

$$n = mq_1 + r_1$$

with  $0 \leq r_1 < m$ . If  $r_1 \neq 0$ , we find by the division algorithm

$$m = r_1q_2 + r_2$$

with  $0 \leq r_2 < r_1$ . For  $i \geq 2$ , if  $r_i \neq 0$ , apply the division algorithm to obtain

$$r_{i-1} = r_iq_i + r_{i+1}$$

with  $0 \leq r_{i+1} < r_i$ . In this way we obtain a sequence

$$r_0 = m > r_1 > r_2 > r_3 > \cdots \geq 0.$$

Therefore  $r_k = 0$  for some  $k$ . By Proposition 23,  $(m, n) = (m, r_1) = (r_1, r_2) = \cdots = (r_{k-1}, r_k) = (r_{k-1}, 0) = r_{k-1}$ .

*Example 25.*  $(1092, 2310) = (1092, 126) = (126, 84) = (84, 42) = (42, 0) = 42$

The Euclidean Algorithm is extremely efficient; in fact, it allows us to find the gcd of two integers without factoring either one. As a byproduct of the algorithm, we can write  $(m, n)$  as a linear combination of  $m$  and  $n$ .

**Proposition 26.** *If  $m$  and  $n$  are positive integers, then there exist integers  $a$  and  $b$  such that*

$$(m, n) = am + bn.$$

Notice that, in the notation of Proposition 26, one of the integers  $a$  and  $b$  will be positive, and the other negative.

*Example 27.* Referring back to the previous example, the division that produced the gcd, 42, as remainder tells us that

$$42 = 126 - 84,$$

while the preceding divisions gave us

$$84 = 1092 - 8 \cdot 126 \quad \text{and} \quad 126 = 2310 - 2 \cdot 1092.$$

Then

$$\begin{aligned} 42 &= 126 - (1092 - 8 \cdot 126) = 9 \cdot 126 - 1092 = 9(2310 - 2 \cdot 1092) - 1092 \\ &= 9 \cdot 2310 - 19 \cdot 1092. \end{aligned}$$

**Proposition 28.** *If  $m$  and  $n$  are positive integers, then the set*

$$\{am + bn \mid a, b \in \mathbb{Z}\}$$

*consists of all of the integer multiples of  $(m, n)$ .*

*Proof.* By Proposition 7 (2), every element of the set is a multiple of  $(m, n)$ . And by Proposition 26,  $(m, n)$  is in the set. Therefore any multiple  $d(m, n)$  of  $(m, n)$  is also in the set, for if we write  $(m, n) = am + bn$ , then

$$d(m, n) = d(am + bn) = (da)m + (db)n.$$

□

## UNIQUE FACTORIZATION

We proved earlier (Theorem 11) that every positive integer is a product of primes. Our aim now is to show that the prime factorization of an integer is unique; that is, one always obtains the same prime factors no matter what path one takes to a prime factorization of a number:

$$90 = 3 \cdot 30 = 3 \cdot 3 \cdot 10 = 3 \cdot 3 \cdot 2 \cdot 5$$

$$90 = 5 \cdot 18 = 5 \cdot 2 \cdot 9 = 5 \cdot 2 \cdot 3 \cdot 3$$

We prove one preliminary result.

**Proposition 29.** *If  $p$  is prime and  $p \mid mn$ , then  $p \mid m$  or  $p \mid n$ .*

*Proof.* Since  $p \mid mn$ ,  $mn = pq$ . Suppose  $p \nmid m$ . Then  $(m, p) = 1$ , so by Proposition 26 we can find integers  $a$  and  $b$  such that  $ma + pb = 1$ . Then

$$n = n \cdot 1 = n(ma + pb) = (mn)a + npb = (pq)a + npb = (qa + nb)p,$$

and therefore  $p \mid n$ .  $\square$

**Theorem 30.** *The prime factorization of an integer  $n > 1$  is unique.*

*Proof.* Suppose  $n$  can be written as a product of primes as

$$n = p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_\ell.$$

Then  $p_1 \mid q_1(q_2 \cdots q_\ell)$ , so by Proposition 29, either  $p_1 \mid q_1$  (in which case  $p_1 = q_1$ ), or  $p_1 \mid q_2 \cdots q_\ell$ . In the latter case, by the same argument either  $p_1 = q_2$  or  $p_1 \mid q_3 \cdots q_\ell$ . By exhaustion we find that  $p_1 = q_i$  for some  $1 \leq i \leq \ell$ . Canceling these, we find that

$$p_2 \cdots p_k = \prod_{j=1, j \neq i}^{\ell} q_j.$$

We may apply the same argument to show that  $p_2 = q_j$  for some  $j \neq i$ ; cancelling these and continuing in this fashion, we eventually eliminate all the  $p$ 's, so that the left hand product becomes 1. It follows that at this point, all of the  $q$ 's must have been canceled as well (else the product of the remaining  $q$ 's would be  $> 1$ ). Thus the two factorizations are the same up to ordering.  $\square$

*Definition 31.* If  $m$  is a positive integer and  $p$  is a prime, define  $v_p(m)$  to be the highest power of  $p$  that divides  $m$  (this is a well-defined notion by Theorem 30).

Notice that

$$m = \prod_{p \text{ prime}} p^{v_p(m)},$$

and that  $v_p(m) = 0$  for all but finitely many primes  $p$ .

We worked hard to prove that integers have unique factorizations into primes, a result that is probably quite familiar to you. It may be so familiar to you that the fact seems trivial. Is it? The answer to this question is no, in the following sense: there are number systems very similar to the integers in which factorization into primes is not unique.

*Example 32.* Consider the number system

$$\mathbb{Z}[\sqrt{-6}] = \{a + b\sqrt{-6} \mid a, b \in \mathbb{Z}\}$$

(in fact, this is a commutative ring; note that  $\sqrt{-6} = \sqrt{6}i$  in our usual notation for  $\mathbb{C}$ ). In this number system, 2 and 5 are “primes” in the sense that they have no nontrivial divisors (for example, the only divisors of 2 are  $\pm 1$  and  $\pm 2$ ); indeed, so are  $2 + \sqrt{-6}$  and  $2 - \sqrt{-6}$ . The fact that

$$2 \cdot 5 = 10 = (2 + \sqrt{-6})(2 - \sqrt{-6})$$

shows that we do not have unique factorization in the number system  $\mathbb{Z}[\sqrt{-6}]$ , since 10 has two different factorizations.

Thinking back to the proof of Theorem 30, if we were to try the same technique to prove that  $\mathbb{Z}[\sqrt{-6}]$  has unique factorization, the part that would fail would be the part involving Proposition 29, since the analog of this does not hold in  $\mathbb{Z}[\sqrt{-6}]$ . Our example shows this, for even though 2 has no nontrivial divisors in  $\mathbb{Z}[\sqrt{-6}]$  and it is a divisor of the product  $(2 - \sqrt{-6})(2 + \sqrt{-6})$ , it is clearly not a divisor of either factor.

Unique factorization allows us to prove the irrationality of many real numbers.

**Proposition 33.**  $\sqrt{7}$  is an irrational number.

*Proof.* Suppose  $\sqrt{7}$  were rational. Then

$$\sqrt{7} = \frac{a}{b}$$

for some integers  $a$  and  $b$ . It follows that

$$a^2 = 7b^2.$$

Then  $v_7(a^2) = v_7(7b^2)$ , but  $v_7(a^2) = 2v_7(a)$  is even and  $v_7(7b^2) = 1 + 2v_7(b)$  is odd, a contradiction.  $\square$

The proof of the preceding proposition generalizes easily to prove

**Theorem 34.** *If  $b$  and  $m$  are positive integers, and  $b$  not the  $m$ th power of another integer, then the  $m$ th root of  $b$  is irrational.*

*Example 35.*  $4^{1/3}$ ,  $\sqrt{27}$  are irrational.