The Integers

The set of integers is

\[ \mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots \} \].

It is defined by various axioms. First there are the algebraic axioms.

**Algebra Axioms**

0) **uniqueness:** if \( a = a', b = b' \) in \( \mathbb{Z} \) implies \( a + b = a' + b' \)

1) **closure:** \( a, b \in \mathbb{Z} \) implies \( a + b, a - b, a \cdot b \in \mathbb{Z} \)

2) **commutative laws:** \( a + b = b + a, \ a \cdot b = b \cdot a \)

3) **associative laws:** \( a + (b + c) = (a + b) + c; \ a \cdot (b \cdot c) = (a \cdot b) \cdot c \)

4) **distributive law:** \( a \cdot (b + c) = a \cdot b + a \cdot c \)

5) **zero:** \( 0 + a = a \)

6) **one:** \( 1 \cdot a = a \)

7) **additive inverses exist:** for any integer \( a \), there exists an integer \( -a \) so that

\[ a + (-a) = 0. \]

8) **cancellation:** \( c \neq 0, ca = cb \) implies \( a = b \).

These axioms hold for all \( a, b, c \in \mathbb{Z} \). Later (next week probably) we will say \( \mathbb{Z} \) is a "group" under addition (and next quarter we will say that \( \mathbb{Z} \) is a "ring" - actually an "integral domain"). This quarter our main subject is groups. Next quarter it will be rings.

There is one more important property of the integers. They are ordered. You view them as equally spaced points on the real line.

We say \( a < b \) if \( a \) is to the left of \( b \). There are many properties of this ordering, all of which can be deduced from the following definition.

**Defn.** \( a < b \) means \( b - a \in \mathbb{Z}^+ = \) the positive integers = \( \{1, 2, 3, 4, \ldots \} \).

The set of positive integers \( \mathbb{Z}^+ \) satisfies the following axioms.

**Ordering Axioms**

1) **addition:** \( a, b \in \mathbb{Z}^+ \) implies \( a + b \in \mathbb{Z}^+ \)

2) **multiplication:** \( a, b \in \mathbb{Z}^+ \) implies \( a \cdot b \in \mathbb{Z}^+ \)

3) **trichotomy:** for any \( a \in \mathbb{Z} \) one and only one of the following alternatives holds:

   i) \( a \in \mathbb{Z}^+ \)

   ii) \( a = 0 \)

   iii) \( -a \in \mathbb{Z}^+ \).

Every other fact about inequalities can be deduced from these 3 axioms and the definition of \( a < b \).
Example 1. Transitive Law.
\[ a < b, b < c \implies a < c. \]
Proof:
\[ c - a = c - b + b - a \quad \text{which is in } \mathbb{Z}^+ \quad \text{by ordering axiom 1 since } c - b \in \mathbb{Z}^+ \quad \text{and} \quad b - a \in \mathbb{Z}^+. \]

Example 2. Multiplying an inequality by a negative number changes \(<\) to \(>\).
\[ a < b, c < 0 \implies ac > bc. \]
Proof:
\[ ac - bc = (a - b)c = (b - a)(-c) \in \mathbb{Z}^+ \quad \text{by ordering axiom 2 since } c < 0 \quad \text{says } -c \in \mathbb{Z}^+. \]

Example 3. \[ a < b \implies a + c < b + c. \]
Proof.
\[ (b + c) - (a + c) = b - a \in \mathbb{Z}^+ \quad \text{by definition.} \]

We have listed about 12 axioms for the integers (9 algebraic and 3 ordering axioms). There is just one left to discuss.

The Well Ordering Principle (or Axiom)
\[ S \subseteq \mathbb{Z}^+ \quad \text{and} \quad S \neq \emptyset \implies S \text{ has a smallest element.} \]
This says that if \( S \) is a non-empty set of positive integers, then there is an element \( a \in S \) such that \( a \leq x \), for all \( x \in S \).

This axiom is perhaps the hardest to believe. It is not true for the real numbers. It is equivalent to mathematical induction.

Examples.
The functions floor and ceiling come about by the well ordering principle.
For any real number \( x \), floor of \( x = \lfloor x \rfloor \) is the largest integer \( \leq x \).

ceiling of \( x = \lceil x \rceil \) is the smallest integer \( \geq x \).

e.g. \[
\lfloor \sqrt{2} \rfloor = 1 \\
\lceil \sqrt{2} \rceil = 2.
\]
(In the old days we only had \( [x] = \lfloor x \rfloor \).)

\([x] \) exists because any set of integers bounded above will have a greatest element just as well ordering implies that any set of integers bounded below will have a least element.

From this, we get
The Division Algorithm. \( \forall \) (for any) \( a, b \in \mathbb{Z} \), with \( a > 0 \), \( \exists \) (there exist) unique integers \( r, q \) such that \( 0 \leq r < b \) and \( a = bq + r \).

Here unique means that if there were also \( r', q' \in \mathbb{Z} \) with \( 0 \leq r' < b \) and \( a = bq' + r' \), it would follow that \( r = r' \) and \( q = q' \).

One could prove the algorithm by saying \( q = \lfloor \frac{a}{b} \rfloor \) and \( r = a - qb \). It is an exercise to show that then \( 0 \leq r < b \).

Example. Take \( a = 163 \) and \( b = 10 \). Then
\[
\begin{array}{c|c}
16 & 163 \\
10 & \hline 163 \\
10 & \hline 63 \\
60 & \hline 3 \\
\end{array}
\]
So we find \( q = 16 \) and \( r = 3 \) and \( 163 = 16 \cdot 10 + 3 \).

See Gallian, p. 4 for the abstract proof of the division algorithm. You could get by with fewer axioms (the Peano Postulates) and a really paranoid mathematician would want to construct something satisfying all these axioms. We will just take the existence of the integers for granted.
Divisibility, Primes, Fundamental Theorem of Arithmetic

**Defn.** If \(a, b \in \mathbb{Z}\), \(b \neq 0\), we say \(b\) divides \(a\) and write \(b \mid a\) if \(a = b \cdot m\), for some \(m \in \mathbb{Z}\). And we say that \(b\) is a divisor of \(a\).

**Examples.**

- 2 divides 10
- 2 does not divide 5

**Defn.** If \(p \in \mathbb{Z}\) and \(p > 1\), then we say \(p\) is a prime iff the only divisors of \(p\) are \(\pm 1\) and \(\pm p\).

**Examples.**

To find all the primes \(p \leq 41\), we use the **Sieve of Eratosthenes**. First write down 2, then all the odd integers \(\leq 41\):

\[
\begin{array}{cccccccccccc}
2 & 3 & 5 & 7 & \hat{9} & 11 & 13 & \hat{15} & 17 & 19 & \hat{21} & \\
23 & \hat{25} & 27 & 29 & 31 & \hat{33} & \hat{35} & 37 & 39 & 41 & \\
\end{array}
\]

Decorate every 3rd integer after 3 with a hat \(^\wedge\).
Decorate every 5th integer after 5 with a tilde \(^\sim\).

The **undecorated numbers on our list are the primes which are \(\leq 41\).**

- 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41

Why does this work? If \(n \leq 41\) is not prime, then \(\exists\) a divisor \(d\) of \(n\) such that

\[d \leq \sqrt{41} < 7.\]

Why? Otherwise \(n = ab\) with \(a > \sqrt{41}\) and \(b > \sqrt{41}\) But then \(n = ab > \sqrt{41} \cdot \sqrt{41} = 41\). This contradicts our hypothesis.

This method works to produce small lists of primes. But if you need two large primes for your public key cryptography, you will need a better method of testing primality. These public key codes are supposed to be secure because it is quite difficult to factor large numbers as a product of primes. There is no problem factoring small numbers.

**Example.**

\[48 = 2^4 \cdot 3\]

Here the primes 2, 3 and the exponents 4, 1 are unique. This is a special case of the fundamental theorem of arithmetic.
Theorem. (The Fundamental Theorem of Arithmetic)
Every integer \(n > 1\) can be written uniquely as
\[ n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}, \]
where \(p_1 < p_2 < \cdots < p_r\) are primes and the exponents \(e_j\) are all positive integers.
Here uniqueness means that if also
\[ n = q_1^{f_1} q_2^{f_2} \cdots q_s^{f_s}, \]
where \(q_1 < q_2 < \cdots < q_s\) are primes and the \(f_j\) are all positive integers, then
\[ r = s, \quad q_j = p_j, \quad f_j = e_j, \text{ for all } j. \]

Proof of the Existence of the Factorization. (a proof by contradiction)
Otherwise the set \(S\) below is non-empty:
\[ S = \{ n \in \mathbb{Z} \mid n > 0, \ n \text{ is not a product of primes} \}. \]
By the well ordering principle, \(S\) must have a smallest element. Call that smallest element \(a \in S\).
So \(a\) is not a prime (as a prime is a product of one prime). Therefore \(a = b \cdot c, \) where \(b, c \in \mathbb{Z}^+.\) But then
\[ 0 < b, c < a. \]
To see this, note that if \(b > a\) and \(c \geq 1,\) then \(a = b \cdot c > a \cdot 1 = a,\) and \(a > a.\) Contradiction.
Then \(b\) and \(c\) must be products of primes by the definition of \(a.\) This implies that \(a = b \cdot c\) is also a product of primes, contradicting the definition of \(a.\)
It follows that the set \(S\) must be empty and we have the existence half of the proof of the fundamental theorem of arithmetic.

The uniqueness of the factorization is a bit harder. We postpone that proof.

Some History. No one worried about proving the uniqueness of the factorization until the 1800’s when it was discovered that there are rings that seem a lot like \(\mathbb{Z}\) but without unique factorization. An example is
\[ \mathbb{Z}[\sqrt{-5}] = \{ x + y\sqrt{-5} \mid x, y \in \mathbb{Z} \}. \]
This was discovered when people sought to prove "Fermat’s Last Theorem" which was written in 1637 in the margin of Fermat’s copy of a book of Diophantus. It says
\[ x^n + y^n \neq z^n, \text{ for } n \geq 3, \ x, y, z \in \mathbb{Z}, \ x \cdot y \cdot z \neq 0. \]
This was recently proved by Andrew Wiles. See Gallian, pp. 317-318.

We will need a few more facts about the integers to prove the uniqueness part of the fundamental theorem of arithmetic.

The Euclidean Algorithm.
Defn. The greatest common divisor \(d\) of 2 integers \(a, b\) is denoted
\[ d = (a, b) = g.c.d.(a, b), \]
where \(d\) is the largest of all the common divisors of \(a\) and \(b.\) This means that
\[ d|a \quad \text{and} \quad d|b \]
and
\[ \text{if } c|a \quad \text{and} \quad c|b, \quad \text{then} \quad c|d. \]

When \((a, b) = 1,\) we say that \(a\) and \(b\) are relatively prime.
Euclid (around 300 B.C.) gave an algorithm to find the g.c.d.
Example.

\((3132, 7200) = ?\)

Euclid says to keep applying the division algorithm as follows.

\[ 7200 = 2 \times 3132 + 936 \]
\[ 3132 = 3 \times 936 + 324 \]
\[ 936 = 2 \times 324 + 288 \]
\[ 324 = 1 \times 288 + 36 \]
\[ 288 = 8 \times 36 + 0 \]

The last non-zero remainder is the greatest common divisor;

\[ 36 = \text{g.c.d.}(3132, 7200). \]

To see this, note that 36 divides 288 by the 5th row of our calculation. And thus 36 divides 324 by the 4th row. It follows that 36 divides 936 by the 3rd row. And then it must divide 3132 by the 2nd row. So 36 is a common divisor of 3132 and 7200, reading the equations from bottom to top.

Next suppose that \( c \) is any common divisor of 3132 and 7200. Then, reading the equations from top to bottom, \( c \) must divide 936 by equation 1. And \( c \) must divide 324 by equation 2. By equation 3, \( c \) must divide 288. Finally, equation 4 says \( c \) must divide 36. Thus we indeed have found the greatest common divisor.

We leave it up to you to read Gallian’s proof of the abstract statement of the Euclidean algorithm (see p. 6).

Next note that you can read the algorithm from bottom to top to find integers \( m, n \) such that

\[ 36 = 3132m + 7200n. \]

Thus

\[ 36 = 3 \times 3132 - 10 \times 7200. \]

So, the general case can be stated as follows.

**Theorem.** Given \( a, b \in \mathbb{Z} \), if \( a \) and \( b \) are non-zero, the greatest common divisor \( d = \text{g.c.d.}(a, b) \) exists and is the smallest positive integer of the form \( d = am + bn \), for \( m, n \in \mathbb{Z} \).

See Gallian, pp. 5-6, for a careful proof.

**Euclid’s Lemma.**

If \( p \) is a prime and \( p \) divides \( ab \), where \( a, b \in \mathbb{Z} \), then either \( p \) divides \( a \) or \( p \) divides \( b \).

**Proof.**

Suppose \( p \) doesn’t divide \( a \). Then

\[ \text{g.c.d.}(p, a) = 1. \]

(Why? Hint. The only positive divisors of \( p \) are \( p \) and 1)

So, by the preceding theorem,

\[ 1 = pm + an, \text{ for some } m, n \in \mathbb{Z}. \]

Multiply by \( b \) to obtain

\[ b = pbm + abn. \]

Since \( p \) divides \( ab \), we know that \( ab = pq \), for some \( q \in \mathbb{Z} \). It follows that

\[ b = p(bm + qn). \]

Thus \( p \) divides \( b \).

**Euclid’s Lemma** will allow us to complete the proof of the fundamental theorem of arithmetic. This is Exercise 23. There are several ways to formulate the proof. One could use the well ordering principle, or the 2nd principle of mathematical induction, as Gallian expects. Let’s postpone the proof until after our discussion of mathematical induction. Instead we turn to something completely different: congruences or modular arithmetic.