THE INTEGERS

TIM SMITS

In a linear algebra course, one develops the theory of linear equations by interpreting them as matrix equations of the form $Ax = b$, which means understanding linear equations is the same as thing as understanding matrices. By abstracting the key properties of Euclidean space and matrices, one comes up with the notions of vector spaces and linear transformations, allowing the theory of linear algebra to work in a more general setting. This is a common theme throughout algebra: start with key examples of objects, and then study general objects that have wanted properties. Before we study rings, our prototypical example will be the integers.

1. The key properties of $\mathbb{Z}$

The set $\mathbb{Z}$ of integers comes with two binary operations, addition $(+)$ and multiplication $(\cdot)$, meaning that for any $a, b \in \mathbb{Z}$ we get well-defined integers $a + b$ and $a \cdot b$. We will take the construction of the integers and the formal definition of these operations for granted, but these operations satisfy the following properties for any $a, b, c \in \mathbb{Z}$:

1. (*Commutativity*) $a + b = b + a$ and $ab = ba$.
2. (*Associativity*) $a + (b + c) = (a + b) + c$ and $a(bc) = (ab)c$.
3. (*Distributivity*) $a(b + c) = ab + ac$.
4. (*Zero*) There exists $0 \in \mathbb{Z}$ such that $a + 0 = a$.
5. (*Negatives*) There exists $-a \in \mathbb{Z}$ such that $a + (-a) = 0$.
6. (*One*) There exists $1 \in \mathbb{Z}$ such that $a \cdot 1 = a$.

More compactly, addition and multiplication are both associative and commutative, multiplication distributes over addition, and there are special elements 0 and 1 that don't "change" an integer a with respect to the relevant operation. Addition has the extra property that integers have additive inverses. The elements of $\mathbb{Z}$ can also be placed in order. We have a relation $<$ defined by $a < b$ if a and b differ by a positive integer. More formally, this can be stated as follows.

There is a non-empty subset $P \subset \mathbb{Z}$ with the following properties:

1. For any $a, b \in P$, $a + b \in P$.
2. For any $a, b \in P$, $a \cdot b \in P$.
3. $0 \notin P$.
4. (*Trichotomy*) For all $a \in \mathbb{Z}$, exactly one of the following holds: $a \in P$, $0 \in P$, or $-a \in P$.

This subset P is of course, the positive integers. The ordering of the integers gives rise to a familiar property:

Proposition 1 (Zero product property)**.** *Let $a, b \in \mathbb{Z}$ with $ab = 0$. Then $a = 0$ or $b = 0$.*

Proof. We prove the contrapositive, that if $a \neq 0$ and $b \neq 0$ then $ab \neq 0$. First suppose that $b > 0$. Since multiplication of integers is defined via repeated addition, i.e. $a \cdot b = \underbrace{a + a + \ldots + a}_{b \text{ times}}$, then $ab \geq a$ or $ab \leq a$ depending on the sign of a. If $b < 0$, do the same thing with $(-a)(-b)$. □

The integers are very special, because not only can they be ordered, but they can be *well-ordered*.

Theorem 1.1 (Well-ordering principle)**.** *Let $S \subset \mathbb{Z}^+$ be non-empty. Then S contains a smallest positive element.*

The well-ordering principle will be very important for proving key theorems that hold in the integers. Perhaps surprisingly, the well-ordering principle is equivalent to mathematical induction. We leave the proof in the appendix. The last key property of the integers that we are all familiar with is the notion of *unique factorization*. As we learn in grade school, any positive integer can be factored into prime numbers.

2. Divsibility

In the integers, we can perform division with remainder.

Theorem 2.1 (Division Algorithm)**.** *Let a and b be integers with $b > 0$. Then there exist unique integers q and r such that $a = bq + r$ with $0 \leq r < b$.*

Proof. Let $S = \{a - bq > 0 : q \in \mathbb{Z}\}$. Then S is non-empty: this is clear if $a > 0$, and if $a < 0$, then $a - (a-1)b = a(1-b) + b > 0$. By the well-ordering principle, S contains a smallest positive element, say r, which we can write as $a - bq = r$ for some q. This then gives $a = bq + r$. First we show that $0 \leq r < b$. If $r > b$, then $r = b + (r - b)$, and $(r - b) > 0$. so $a = b(q+1) + (r - b)$ with $0 < r - b < r$. This contradicts the minimality of r, so $0 \leq r < b$. This proves the existence of such q and r, so it remains to show the uniqueness of q and r.

Suppose that $a = bq + r$ and $a = bq' + r'$ with $0 \leq r < b$ and $0 \leq r' < b$. Without loss of generality, suppose that $r \leq r'$. Then from $bq + r = bq' + r'$ we get $b(q - q') = (r' - r)$. This says $(r' - r)$ is a multiple of b, and since $0 \leq r' - r < b$ this says $r' - r = 0$, i.e. $r = r'$. It's then immediate that $q = q'$ so uniqueness follows. □

The division algorithm can be extended to all integers in the following form:

Theorem 2.2 (Extended division algorithm)**.** *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then there exist unique integers q, r such that $a = bq + r$ and $0 \leq r < |b|$.*

Proof. Exercise. □

Definition 2.3. We say for integers a, b that a **divides** b if there is an integer k such that $b = ak$, and write this as $a \mid b$.

Example 2.4. We have $2 \mid 10$, because $102 \cdot 5$, $(-7) \mid 49$, because $49 = (-7) \cdot (-7)$, and $5 \mid 0$ because $0 = 5 \cdot 0$. Clearly $\pm 1 \mid n$ for any integer n, however, $0 \nmid n$ for any non-zero integer n, because there is no integer k with $0 \cdot k = n$.

From the definition of divisibility, we have the following basic properties:

Proposition 2. *Let $a, b, c \in \mathbb{Z}$.*

1. *If $a \mid b$ then $a \mid b\ell$ for any $\ell \in \mathbb{Z}$.*
2. *If $a \mid b$ and $b \mid c$, then $a \mid c$.*
3. *If $a \mid b$ and $a \mid c$ then $a \mid bx + cy$ for any $x, y \in \mathbb{Z}$.*
4. *If $a \mid b$ for $b \neq 0$, then $|a| \leq |b|$.*

Proof. These follow more or less immediately from the definition and are left as an exercise. □

Definition 2.5. The **greatest common divisior** of two integers a and b is the largest positive integer d such that:

1. $d \mid a$ and $d \mid b$
2. If $c \mid a$ and $c \mid b$, then $c \leq d$.

We write $\gcd(a, b)$ or (a, b) to denote the greatest common divisor. If $(a, b) = 1$, we say that a and b are **relatively prime**.

If d is any divisor of an integer a, then property 4 above says there are only finitely many possibilities for d, so it makes sense to speak of a greatest one. If $a = 0$, then obviously all integers are divisors of a, so $(0, a) = |a|$. Note that $(0, 0)$ is therefore undefined.

Example 2.6. The greatest common divisor of $a = 315$ and $b = 195$ is $d = 15$, which is easily found by factoring.

The greatest common divisor of two integers a and b has the important property that it's an integer linear combination of a and b:

Theorem 2.7 (Bezout's lemma)**.** *Let $a, b \in \mathbb{Z}$ and set $d = \gcd(a, b)$. Then there exist integers x and y such that $ax + by = d$.*

Proof. Let $S = \{ax + by > 0 : x, y \in \mathbb{Z}\}$, the set of all integer linear combinations of a and b that are positive. Notice that S is non-empty, because either a or $-a$ is positive and $a \in S$. By the well-ordering principle, S has a least positive element, say d', so there are integers x and y such that $ax + by = d'$. We will show that $d = d'$.

Since $d \mid a$ and $d \mid b$ by definition, $d \mid (ax + by)$ so $d \mid d'$, and therefore $d \leq d'$. To show that $d' \leq d$, we will show that d' divides every element of S. Let $s \in S$, so $s = ax' + by'$ for some $x', y' \in \mathbb{Z}$. By the division algorithm, we can write $s = d'q + r$ for unique q and r with $0 \leq r < d'$. Then $r = s - d'q = ax' + by' - (ax + by)q = a(x' - xq) + b(y' - yq)$. However, $r < d'$ and d' is the smallest positive element of S, so this forces $r = 0$. Therefore, $s = d'q$ so $d' \mid s$ for any $s \in S$. In particular, $a, b \in S$ so $d' \mid a$ and $d' \mid b$, so d' is a common divisor of a and b, so $d' \leq d$ by definition of d. □

Note that we not only proved that the greatest common divisor is an integer linear combination of a and b, but that it's the *smallest positive* integer linear combination of a and b. As a consequence, we get the following important result:

Corollary 2.8. *Let $a, b, c \in \mathbb{Z}$ with $a \mid bc$ and $(a, c) = 1$. Then $a \mid b$.*

Proof. Since $(a, c) = 1$, by Bezout's lemma there are integers x, y such that $ax + cy = 1$. Multiplying by b says $abx + bcy = b$. Since $a \mid bc$, then $a \mid abx + bcy$, i.e. $a \mid b$. □

3. The Euclidean Algorithm

In the example in the previous section, it was very easy to factor the given numbers to compute their greatest common divisior. In general, factoring is a very hard problem.

Example 3.1. Let $a = 1002001$ and $b = 379427895$. Then $a = 7^2 \cdot 11^2 \cdot 13^2$ and $b = 3^4 \cdot 5 \cdot 7 \cdot 11 \cdot 23^3$, so we have $\gcd(a, b) = 7 \cdot 11 = 77$.

This example would already be hard to do by hand, and if the integers are large enough, even a computer will have trouble factoring them. The following algorithm (of Euclid!) is a significantly more efficient way of doing this computation:

Theorem 3.2 (Euclidean algorithm)**.** *Let a, b be non-zero integers. Repeatedly carry out the division algorithm as follows:*

$$\begin{aligned} a &= bq_1 + r_1, \quad 0 \leq r_1 < |b| \\ b &= r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3, \quad 0 \leq r_3 < r_2 \\ &\vdots \end{aligned}$$

The sequence of remainders $r_1, r_2, r_3, \ldots$ is strictly decreasing, and therefore eventually become 0. The last non-zero remainder is the greatest common divisor of a and b.

We omit the proof, but will give a few examples of how to carry out the algorithm.

Example 3.3. Let $a = 75$ and $b = 45$. We have

$$\begin{aligned} 75 &= 45 \cdot 1 + 30 \\ 45 &= 30 \cdot 1 + 15 \\ 30 &= 15 \cdot 2 + 0 \end{aligned}$$

So that $(75, 45) = 15$.

Example 3.4. Let $a = 517$ and $b = 89$. We have

$$\begin{aligned} 517 &= 89 \cdot 5 + 72 \\ 89 &= 72 \cdot 1 + 17 \\ 72 &= 17 \cdot 4 + 4 \\ 17 &= 4 \cdot 4 + 1 \\ 4 &= 4 \cdot 1 + 0 \end{aligned}$$

So that $(517, 89) = 1$.

Example 3.5. Let $a = 379427895$ and $b = 1002001$. We have

$$\begin{aligned}
379427895 &= 1002001 \cdot 378 + 671517 \\
1002001 &= 671517 \cdot 1 + 330484 \\
671517 &= 330484 \cdot 2 + 10549 \\
330484 &= 10549 \cdot 31 + 3465 \\
10549 &= 3465 \cdot 3 + 154 \\
3465 &= 154 \cdot 22 + 77 \\
154 &= 77 \cdot 2 + 0
\end{aligned}$$

So that $(379427895, 1002001) = 77$.

The Euclidean algorithm is not only useful for computing the greatest common divisor; we can use it to tell us *what* integer linear combination of a and b to take to get the greatest common divisor!

Example 3.6. Let $a = 517$ and $b = 89$. We have

$$\begin{aligned}
517 &= 89 \cdot 5 + 72 \\
89 &= 72 \cdot 1 + 17 \\
72 &= 17 \cdot 4 + 4 \\
17 &= 4 \cdot 4 + 1
\end{aligned}$$

Which tells us that $(517, 89) = 1$. We now back substitute to solve for 1 in terms of the previous lines. We have

$$\begin{aligned}
1 &= 17 - 4 \cdot 4 \\
&= 17 - 4 \cdot (72 - 17 \cdot 4) = 17 \cdot 17 - 4 \cdot 72 \\
&= 17 \cdot (89 - 72 \cdot 1) - 4 \cdot 72 = 89 \cdot 17 - 72 \cdot 21 \\
&= 89 \cdot 17 - (517 - 89 \cdot 5) \cdot 21 = 89 \cdot 122 - 517 \cdot 21
\end{aligned}$$

This says the integers we are looking for in Bezout's lemma are $x = -21$ and $y = 122$.

4. Unique factorization

Definition 4.1. An integer $p > 1$ is called **prime** if the only positive divisors of p are 1 and p.

The sequence of prime numbers starts off as $2, 3, 5, 7, 11, \ldots$. Primes are the "building blocks" of the integers, in the sense that all integers are constructed from primes.

Prime numbers have the following property:

Proposition 3. *Let $p > 1$. Then p is prime if and only if for any integers a, b, $p \mid ab \implies p \mid a$ or $p \mid b$.*

Proof. First, suppose that p is prime. Let $p \mid ab$, and suppose that $p \nmid a$. Then $(a, p) = 1$ by definition of p being prime, so by Bezout's lemma, there are integers x, y with $px + ay = 1$. Multiplying by b says $pbx + aby = b$, and since $p \mid ab$, we have $p \mid pbx + aby$, so $p \mid b$.

Conversely, suppose that $p > 1$ is an integer with the property that $p \mid ab \implies p \mid a$ or $p \mid b$. Let d be a positive divisor of p. Then we can write $p = dk$ for some positive integer k.

Certainly, $p \mid p$, so $p \mid dk$ means that $p \mid d$ or $p \mid k$. However, since $1 \leq d, k \leq p$, the only way this is possible is if $d = 1$ or $d = p$, so that the only positive divisors of p are 1 and p. □

This property will be the key to proving unique factorization.

Theorem 4.2 (Fundamental theorem of arithmetic)**.** *Let $n > 1$ be an integer. Then there exist unique primes $p_1, \ldots, p_k$ and unique positive integers $e_1, \ldots, e_k$ such that $n = p_1^{e_1} \cdots p_k^{e_k}$. That is, every integer has a unique factorization (up to order of factors) into a product of primes.*

Proof. There are two parts to the proof. First, we show that we can write every integer $n > 1$ as *some* product of prime numbers, and then we will show that such a choice of primes are *unique*. Both of these statements will be proven using strong induction.

Existence:

Note that $n = 2$ is a prime. Now suppose for some k that the integers $2, 3, \ldots, k$ can be written as a product of primes. Consider the integer $k + 1$: if it is prime, we are done. Otherwise, $k + 1$ is not prime, so by definition it has a non-trivial positive divisor. Write $k + 1 = ab$ for some integers a and b. Necessarily, $1 < a, b < k + 1$, so in particular a and b are integers between 2 and k. By induction hypothesis, both a and b can be written as a product of primes, and therefore $k+1$ is a product of primes as well. By induction, we then see that every integer $n > 1$ is a product of primes.

Uniqueness:

Note that 2 is a prime so it's a product of primes in a unique way. Now suppose that for some k, we have that $2, 3, \ldots, k$ all have a factorization using a unique set of primes. If $k+1$ is prime, again we are done. Otherwise, suppose that we can write $k+1 = p_1 \cdots p_m = q_1 \cdots q_\ell$ for some primes p_i and q_j. Then $p_1 \mid q_1 \cdots q_\ell$, so by inductively applying Euclid's lemma, one finds $p_1 \mid q_j$ for some j, and since q_j are prime, this says $p_1 = q_j$ for some j. By reordering the factors as necessary, assume $p_1 = q_1$. Cancelling p_1 from both sides, we have $a = p_2 \cdots p_m = q_2 \cdots q_\ell$. However, $1 < a < k$ so by assumption, a has unique factorization, i.e. $m = \ell$ and $p_i = q_i$ for all $2 \leq i \leq m$ (after reordering if necessary). Since $k + 1 = ap_1$, and $p_1 = q_1$, this shows $k + 1$ has unique factorization as desired. By induction, every $n > 1$ has unique factorization. Collecting terms of the same prime together shows that n is of the form listed in the statement and the uniqueness of the exponents is immediate. □

Note that for any two integers a and b, we can factor them into a common set of primes by allowing the exponents to be 0. This leads to another computation of the greatest common divisor (useful for small integers):

Proposition 4. *Let $a = p_1^{e_1} \cdots p_k^{e_k}$ and $b = p_1^{f_1} \cdots p_k^{f_k}$ be prime factorizations of a and b into a common set of primes. Then $(a, b) = p_1^{\min\{e_1, f_1\}} \cdots p_k^{\min\{e_k, f_k\}}$*

Proof. Let $d = (a, b)$. Then since d divides both a and b, we can write $d = p_1^{t_1} \cdots p_k^{t_k}$ for some non-negative integers t_i where $t_i \leq e_i$ and $t_i \leq f_i$. Therefore, $t_i \leq \min\{e_i, f_i\}$ for all i. It's clear that setting $t_i = \min\{e_i, f_i\}$ for all i gives us a divisor of a and b, which is therefore the greatest common divisor because the size of each exponent has been maximized. □

5. Appendix

The most common statement of mathematical induction may be stated as follows:

Theorem 5.1. *(Principle of Mathematical Induction) For $n \in \mathbb{N}$, let $P(n)$ be a statement such that*

1. *$P(n_0)$ is true for some n_0*
2. *$P(k)$ is true implies $P(k+1)$ is true for all $k \geq n_0$.*

Then $P(n)$ is true for all $n \geq n_0$.

There is also a "stronger" version of induction:

Theorem 5.2. *(Principle of Strong Induction) For $n \in \mathbb{N}$, let $P(n)$ be a statement such that*

1. *$P(n_0)$ is true for some n_0*
2. *$P(n_0), \ldots, P(k)$ is true implies $P(k+1)$ is true for all $k \geq n_0$.*

Then $P(n)$ is true for all $n \geq n_0$.

It's not terribly hard to show that these two forms of induction are equivalent to each other. More interestingly, is that both forms of induction are equivalent to the well-ordering principle!

Theorem 5.3. *The principle of strong induction is equivalent to the well-ordering principle.*

Proof. Suppose that the principle of strong induction holds. Let $S \subset \mathbb{Z}^+$ be a non-empty subset. We wish to show that S has a least positive element. For sake of contradiction, suppose that S does not have a least positive element. Then $1 \notin S$, because 1 is the smallest positive integer. From this we see that $2 \notin S$, because $1 \notin S$ and 2 is the next positive integer after 1. Continuing this train of thought, we see that if $1, 2, \ldots, k \notin S$ for some k, then we must have $k+1 \notin S$. By induction, we must then have $n \notin S$ for all$n \geq 1$, which says that S is empty, a contradiction. Therefore, if we assume strong induction holds, then the well-ordering principle holds.

Now suppose that the well-ordering principle holds, and let P be a statement about integers such that $P(n_0)$ is true for some n_0 and $P(n_0), \ldots, P(k)$ true implies that $P(k+1)$ is true for all $k \geq n_0$. We wish to show that $P(n)$ is true for all $n \geq n_0$. Suppose otherwise, that there is some $m \geq n_0$ such that $P(m)$ is false. Let $S = \{n \in \mathbb{Z}^+ : P(n) \text{ is false}\}$. By assumption S is non-empty, so by the well-ordering principle, S has a smallest positive element, say k. Since $P(n_0)$ is true, we must have that $k > n_0$. Now by definition of k, $P(k-1)$ must be true. Similarly, $P(n_0), P(n_0+1), \ldots, P(k-1)$ must all be true. By strong induction, this then says that $P(k)$ is true, which is a contradiction. Therefore if the well-ordering principle holds, then strong induction holds, so we are done. □

We have shown that induction and the well-ordering principle are equivalent, but we haven't shown that either one of these statements are actually true. In fact, we can't! Any construction of the integers (e.g. the Peano construction) must take either the well-ordering principle or mathematical induction as an axiom.