Math 4030-001/Foundations of Algebra/Fall 2017

Numbers at the Foundations: The Integers

Next, we consider the **Integers**. This is the set

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

which is ordered, but which does not enjoy well-ordered axiom since, for example, there is no smallest integer. The integers consist of the natural numbers, zero and the negative integers. Proofs and definitions generally treat the three cases separately.

The integers have a *symmetry* that the natural numbers lack, namely:

Definition 5.1. The negation of an integer is defined by:

$$-(n) = -n \text{ for all natural numbers}$$

$$-(0) = 0$$

$$-(-n) = n \text{ for all negative integers}$$

Remark. Two key properties of negation are:

(a) Negation reverses order. If $a \leq b$, then $-a \geq -b$, and

(b) Negating twice returns to the original. That is, $-(-a) = a$.

If we think of the integers evenly spaced on the number line, then negation is the reflection across the origin, which explains (a) and (b).

Notation. We will let the letters $a, b, c, ...$ denote integers, reserving k, l, m, n to stand more specifically for natural numbers.

Definition 5.2. Addition of integers may be defined inductively:

(o) $a + 0 = a$

(i) $a + 1 =$ the integer after a.

$a + (-1) =$ the integer before a

(ii) $(\forall n \in \mathbb{N})$ $a + (n + 1)$ is the number after $a + n$.

$(\forall n \in \mathbb{N})$ $a + (-(n + 1))$ is the number before $a + (-n)$.

From this definition, we can prove by induction that:

Zero is the Additive Identity. That is, $0 + a = 0$ for all integers a.

Proof. (o) $0 + 0 = 0$ by definition.

(i) $0 + 1 = 1$ and $0 + (-1) = -1$ also by definition.

(ii) If $0 + n = n$, then $0 + (n + 1)$ is the number after n, which is $n + 1$ and if $0 + (-n) = -n$, then $0 + (-(n + 1))$ is the number before $-n$, which is $-(n + 1)$. This completes the proof by induction!

Remark. If $n \geq m$ are natural numbers, we may interpret $n + (-m)$ as the number of elements remaining after removing (subtracting) m elements from a set with n elements. In particular, $n + (-n) = 0$.

To prove the associative law, it is useful to think geometrically.

Observation. (a) The function $f(x) = x + n$ shifts all of the integers (on the number line) to the right by n units.

(b) $f(x) = x + (-n)$ shifts the integers to the left by n units.

(c) $f(x) = x + 0$ leaves all the integers in place.

If we know in advance that f is a shift (translation) function, then

$$f(0) = a$$

is the shift (left or right or none), since $0 + a = a$.

Addition of Integers is Associative.

Proof. Let x be a variable and a, b be fixed integers, and:

$$f(x) = x + a, \quad g(x) = x + b$$

Then $(g \circ f)(0) = (0 + a) + b = a + b$ and therefore:

$$(g(f(x)) = (x + a) + b \text{ and } (g \circ f)(x) = x + (a + b)$$

since $(g \circ f)(0) = a + b$. But by the associativity of composition of functions, $g(f(x)) = (g \circ f)(x)$ for every x, so addition is associative.

Remark. In the proof, we assumed that the composition $g \circ f$ of two shift functions is once again a shift function. This is an appeal to geometric intuition that might make some uncomfortable.

Negation Distributes with Addition.

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z}) - (a + b) = (-a) + (-b)$$

Proof. Fix a. We will prove this for all b. It is clearly true for $b = 0$.

(i) Since $a + 1$ is the number after a and $(-a) + (-1)$ is the number before $-a$, it follows that $-(a+1) = (-a)+(-1)$ since negation reverses the ordering. Similarly, $a+(-1)$ is the number before a and $(-a)+1$ is the number after $(-a)$, so $-(a + (-1)) = (-a) + 1 = (-a) + (-(-1))$.

(ii) For all n, if $-(a + n) = (-a) + (-n)$, then $-(a + (n + 1))$ is the number **before** $-(a + n) = (-a) + (-n)$, i.e. it is $(-a) + (-(n + 1))$, and similarly, if $-(a + (-n)) = (-a) + n$, then $-(a + (-(n + 1)))$ is the number **after** $(-a) + n$, i.e. it is $(-a) + (n + 1)$. □

Remark. The order-reversing property of negation was the key to this proof, and it was also the key to proving that 0 is an additive identity.

The Additive Inverse of a is $-a$. That is, $(\forall a \in \mathbb{Z})\ a + (-a) = 0$.

Proof. This is true when $a = 0$ and when $a = n$ (by subtraction). Since negation distributes with addition, we also have:

$$-(n + (-n)) = -0 = 0 \text{ so } (-n) + n = 0$$

since negation distributes with addition. □

Remark. The preposition "the" before "additive inverse" is premature since we only proved uniqueness of additive inverses assuming that addition is commutative and associative. We remedy this below.

Addition is Commutative.

Proof. We already know that $n + m = m + n$ and $0 + a = a + 0$ for all natural numbers m and n and integers a. We can also use the distributive property of negation to conclude that:

$$(-n) + (-m) = -(n + m) = -(m + n) = (-m) + (-n)$$

So addition also commutes when both integers are negative. This leaves the case where one of the integers is positive and the other is negative. Suppose $n \geq m$. Then:

$$n + ((-m) + n) = (n + (-m)) + n = n + (n + (-m))$$

using the associative law and the proven case of the commutative law. Adding $-n$ we then get $(-m) + n = n + (-m)$. We can similarly use $-n$ in the case where $n < m$ to take care of this final case. □

For multiplication, let's first think about the properties we want:

List of Desired Properties for the Multiplication of Integers.

- Multiplication of natural numbers should be repeated addition.
- Multiplication by -1 should be negation.
- Multiplication should be associative and commutative and it should distribute with the addition of integers.

Proposition 5.1. These properties **determine** multiplication.

Proof. The desired properties tell us:

$$m * n = mn \text{ is the product of natural numbers}$$
$$(-m) * n = ((-1) * m) * n = (-1) * (mn) = -mn$$
$$m * (-n) = m * ((-1) * n) = (-1) * (m * n) = -mn$$
$$(-m) * (-n) = ((-1) * (-1)) * (mn) = -(-mn) = mn$$

In fact, this only used the associative and commutative properties. We use the distributive property to determine multiplication by 0:

$$a * 0 = a * (1 + (-1)) = a + (-a) = 0 \quad \square$$

Remark. This multiplication rule now should undergo an examination. Does it actually satisfy all the desired properties? In particular, does it really satisfy all the laws of arithmetic? This can be done with a case by case analysis, using the fact that the multiplication of natural numbers satisfies the laws and that negation distributes with addition.

We have enlarged the natural numbers to the integers and we have extended the addition and multiplication operations. This gives us a (unique) additive identity (0) and (unique) additive inverses ($-a$). The negation operation, which **defines** multiplication by -1, is a symmetry that we can use to define the subtraction operation on integers as:

$$a - b = a + (-b)$$

addition of the additive inverse. Of course, we don't have division....

Division with Remainder. Given $a \in \mathbb{Z}$ and $n \in \mathbb{N}$, there is a unique quotient $q \in \mathbb{Z}$ and remainder $r \in \{0, 1, ..., n-1\}$ so that:

$$a = qn + r$$

Proof. The set of integers:

$$S = \{a + bn \mid b \in \mathbb{Z}\}$$

has neither a maximum nor a minimum, since n can be added to or subtracted from any element of S to get a new element. It follows that:

$$S \cap \mathbb{N} \neq \emptyset$$

and therefore $S \cap \mathbb{N}$ has a unique smallest element $r = a + bn$ with

$$r \in \{1, 2, ..., n\}$$

because otherwise $r - n$ would be a smaller element in R. So either:

(i) $r = a + bn \in \{1, ..., n-1\}$ and then $a = (-b)n + r$ or else

(ii) $r = a + bn = n$, and then $a = (-b+1)n + 0$ □

We are now ready for something new and exciting.

Definition 5.3. Let $m, n \in \mathbb{N}$. Their **greatest common divisor**,

$$\gcd(m, n)$$

is the largest natural number d that divides both m and n. We say that m and n are **relatively prime** if $\gcd(m, n) = 1$.

Remark. Every pair of natural numbers has a gcd, since 1 is a common divisor and every common divisor is no bigger than $\min\{m, n\}$.

In middle school we find gcd's by factorizing m and n and looking for common prime factors, but we haven't yet proven unique factorization of natural numbers into primes, and in any case there is a better way.

Euclid's Algorithm (for finding $\gcd(m, n)$). Assume $m \leq n$.

Loop. Use division with remainder to write:

$$n = qm + r \text{ with } r \in \{0, 1, ..., m-1\}$$

If $r = 0$, STOP. The gcd is m. Otherwise, reset the n and m to:

$$n := m \text{ and } m := r \text{ and REPEAT}$$

Since each remainder generated by the algorithm is smaller than the previous one, there are no infinite loops (well-ordered axiom!).

Example. To find $\gcd(512, 1000)$, we run the algorithm:

$$\begin{array}{rcrcr} 1000 & = & 1(512) & + & 488 \\ 512 & = & 1(488) & + & 24 \\ 488 & = & 20(24) & + & 8 \\ 24 & = & 3(8) & + & 0 \end{array}$$

STOP. The gcd is 8.

Verification. Euclid's algorithm does actually produce the gcd.

Proof. Any common divisor of n and m also divides r since

$$r = n - qm$$

This is true for every iteration of the loop, so the gcd divides n, m, r and each subsequent remainder r as long as the loop repeats. Thus the gcd divides the number returned by the algorithm.

On the other hand, the number d returned by the algorithm divides both n and m in the last iteration of the loop, which were m and r in the previous iteration, and:

$$n = qm + r$$

from that iteration shows that d divides n as well. Tracing back the loop to the original pair n and m, we see that d divides the original pair of natural numbers. Thus d is a common divisor of m and n and the gcd divides d, so the gcd must **be** the number d. □

Example. In the example above, $\gcd(512, 1000)$ divides:

$$1000,\ 512,\ 24 \text{ and } 8$$

and 8 divides $24,\ 488,\ 512$ and 1000, so 8 is the gcd.

Remark. This algorithm is easy to code and quick to run. A slightly souped up version of it will finish in approximately $\log_2(m)$ steps, which means it can quickly find gcd's of pairs of numbers with many digits. On the other hand, **factoring** such numbers is very slow.

There is also a very important Corollary of Euclid's Algorithm.

Corollary 5.2. If $d = \gcd(m, n)$, then there are $a, b \in \mathbb{Z}$ such that:

$$am + bn = d$$

In particular, if m and n are relatively prime, then $am + bn = 1$.

Proof. Let $m_0 = m$ and $n_0 = n$ (to distinguish them from the redefined values of m and n in the algorithm). We recursively define **two** pairs of integers a_1, b_1, a_2, b_2 in the loop satisfying:

$$a_1 m_0 + b_1 n_0 = n \text{ and } a_2 m_0 + b_2 n_0 = m$$

When the algorithm returns m, we set $a = a_2$ and $b = b_2$.

Initialize: Set $a_1 = 0, b_1 = 1$ and $a_2 = 0, b_2 = 1$. Then:

$$a_1 m_0 + b_1 n_0 = n \text{ and } a_2 m_0 + b_2 n + 0 = m$$

in the first iteration of the loop.

Loop: When we reset n to m and m to $r = n - qm$, then reset

$$a_2 := a_1 - q a_2 \text{ and } b_2 := b_1 - q b_2$$

$$a_1 := \text{ (previous) } a_2, \text{ and } b_1 := \text{ (previous) } b_2$$

to preserve the two equations. □

Example. The earlier example, annotated with a's and b's, gives:

$$\begin{array}{rcrcrrrr} 1000 & = & 1(512) & + & 488 & a_1 = 0 & b_1 = 1 & a_2 = 1 & b_2 = 0 \\ 512 & = & 1(488) & + & 24 & a_1 = 1 & b_1 = 0 & a_2 = -1 & b_2 = 1 \\ 488 & = & 20(24) & + & 8 & a_1 = -1 & b_1 = 1 & a_2 = 2 & b_2 = -1 \\ 24 & = & 3(8) & + & 0 & a_1 = 2 & b_1 = -1 & a_2 = -41 & b_2 = 21 \end{array}$$

STOP. The gcd is 8 and $(-41)(512) + (21)(1000) = 8$.

Exercises. 5.1. The **absolute value** function:

$|\cdot| : \mathbb{Z} \to \mathbb{N} \cup \{0\}$ is defined by $|n| = n$, $|0| = 0$ and $|-n| = n$

(a) Prove that $|a| = |-a|$ for all integers a.

(b) Prove by induction that:

$$|a + n| \leq |a| + n$$

for all natural numbers n. When does equality hold?

5.2. Prove that multiplication of integers is commutative.

5.3. Prove that multiplication of integers is associative.

5.4. Prove that multiplication of integers distributes with addition.

5.5. Find $d = \gcd(m, n)$ and solve $am + bn = d$ for:

(a) $m = 91,\ n = 343$ (b) $m = 101,\ n = 150$