Mathematics 4300 – Foundations of Algebra – Fall 1999

1. First Stop on the Number Tour: The Integers. The integers include the natural numbers, zero and the negatives. We'll recall the basic operations of arithmetic in this section and talk a little about prime numbers.

The Natural Numbers: Let $\mathbf{N}$ denote the set of natural numbers:

$$\mathbf{N} = \{1, 2, 3, 4, 5, ...\}$$

and we will let l, m, n stand for individual natural numbers.

The natural numbers can be pictured as points on a line (actually a ray) evenly spaced, starting at "1" and extending forever to the right:

The natural numbers have the following familiar operations:

Addition. To obtain $m+n$, start at m on the number-ray and move n units to the right. So $m = 1 + 1 + ... + 1$ (repeated m times) and it follows that:

Addition of natural numbers is commutative: $m + n = n + m$ and

Addition of natural numbers is associative: $(l+m)+n = l+(m+n)$.

Multplication. To obtain $m \cdot n$ (which we will usually write as mn), make an array of evenly spaced dots with m rows and n columns. Then mn is the number of objects in the array. Alternatively, $mn = m + m + ... + m$ (repeated n times) which is equal to $(1+...+1)+(1+...+1)+...+(1+...+1)$ with m of the 1's in each parenthesis and n parentheses in all. Then:

Multiplication of natural numbers is commutative: $mn = nm$

(Flip one array on its side to get the other!)

Multiplication of natural numbers is associative: $(lm)n = l(mn)$

(They both count the dots in the same 3-dimensional array!.)

Multiplication and addition distribute: $l(m + n) = lm + ln$

(Put the arrays for lm and ln next to each other to get the array for $l(m+n)$.)

Relations.

$m < n$ if n is to the right of m on the number-ray.
$m > n$ if n is to the left of m on the number-ray.
$m = n$ if m and n represent the same point on the number-ray.

Subtraction. If $m < n$, then $n - m$ is obtained by moving m units to the left of n on the number-ray. We require $m < n$ so that we do not "fall off" the number-ray(!) Thus subtraction is allowed only about half the time.

Division with remainders (or long division): If $m < n$, then there is a "quotient" natural number q with the property that either:

(a) $n = mq$, in which case we say that m **divides** n, (written $m|n$),

or else there is a "remainder" natural number r such that:

(b) $n = mq + r$ and $r < m$.

Moreover, there is only one possible quotient and remainder.

We will prove this later on. For now let's examine the consequences.

Definition: A natural number p is **prime** if $p > 1$, and the only numbers which divide p are 1 and p itself (with quotients p and 1, respectively).

The first few primes: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots.$

Here are a couple of facts about prime numbers.

Fact 1: There are infinitely many primes. (We will prove this!)

Fact 2: The primes spread out as they get larger. For example, there are fewer primes between 101 and 200 than between 1 and 100.

Here is an unsolved problem that shows how little we know about primes.

The Twin Prime Problem: Let's say primes p and q are "twins" if they differ by 2 (e.g. 5 and 7, or 101 and 103). Are there infinitely many twins?

Here's another fact about natural numbers which we will prove.

The Fundamental Theorem of Arithmetic: Every natural number n (greater than 1) has a unique factorization as a product of prime numbers.

Remark: It can take a long time to factor large numbers, even on a fast computer. This fact has been exploited in encryption schemes, which allow you to use your credit card number over the internet (relatively) safely.

The Integers: Let $\mathbf{Z}$ denote the set of integers:

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

i.e. the natural numbers, the "unnatural" 0 and the negative numbers, which we will denote by $-l, -m$ or $-n$. We let a, b, c denote arbitrary integers.

The integers are represented by evenly spaced points on the number **line**.

We (or rather our ancestors) introduce 0 and the negative numbers in order to make subtraction work all of the time. There is a cost involved, as the basic operations have to be constructed on a case-by-case basis. This is the theme for all of our tour of number systems, as we will introduce rational numbers to make (exact) division possible, real numbers in order to include such numbers as π and $\sqrt{2}$, and complex numbers in order to include $\sqrt{-1}$.

Addition. We have to define this in three cases, separately.

(1) $a + 0 = a$ for any integer a.

(2) $a + m$ is the point m units to the right of a.

(3) $a + (-m)$ is the point m units to the left of a

It takes some work (there are many cases to check), but this:

Addition of integers is commutative and associative.

The role of zero merits special recognition.

Zero is the additive identity: $a + 0 = a = 0 + a$ for all integers a.

Additive Inverses (or Negatives). This is defined in cases, too:

(1) $-0 = 0$

(2) $-m = -m$ (looks kind of stupid)

(3) $-(-m) = m$ (two negatives make a positive in mathematics!)

A Little Lemma: $a + (-a) = 0$ always.

Proof: Check the three cases with our definition of addition and inverses. (1) $a = 0$. $0 + (-0) = 0 + 0 = 0$. Check. (2) $a = m$. $m + (-m) = 0$. Check. (3) $a = -m$. $-m + -(-m) = -m + m = 0$. Check. End of proof.

Another Little Lemma: $-(-a) = a$ always.

Proof: Check the three cases for a. (1) $a = 0$. $-(-0) = -0 = 0$. Check. (2) $a = m$. $-(-m) = m$. Check. (3) $a = -m$. $-(-(-m)) = -m$. Check.

Subtraction. $a - b$ is defined to be $a + (-b)$. This is the inverse operation to addition, in the sense that (by our little lemma and the associative law):

$$(a - b) + b = (a + (-b)) + b = a + ((-b) + b) = a + 0 = a$$

This is the bonus we get by going to the integers.

Relations. These are the same as before.
$a < b$ if b is to the right of a on the number-ray.
$a > b$ if b is to the left of a on the number-ray.
$a = b$ if a and b represent the same point on the number-ray.

Multiplication. Again we split into cases:

(1) $a \cdot 0 = 0$ and $0 \cdot a = 0$.

(2) mn still counts the dots in an $m \times n$ array.

(3) $(-m)n = -mn$ and $m(-n) = -mn$.

(4) $(-m)(-n) = mn$.

Again one has to prove the following statements case by case:

Multiplication of integers is commutative: $ab = ba$

Multiplication of integers is associative: $(ab)c = a(bc)$

Multiplication and addition distribute: $a(b + c) = ab + ac$.

One is the multiplicative identity: $a \cdot 1 = a$ for all a.

Division with remainders needs only minor modifications to handle negative numbers, but notice that 0 has the exceptional property that:

$$a \cdot 0 = 0 \text{ for all } a$$

and it follows that:

Every number divides 0, and 0 doesn't divide anything else

and dividing by 0, even with remainders, is not a sensible thing to do. (Why?)

Exercises. Starting with the assumption that addition and multiplication of natural numbers satisfy the commutative, associative and distributive laws, prove the following properties of the integers on a case-by-case basis.

1.1. Addition of integers is commutative.

1.2. Addition of integers is associative.

1.3. Multiplication of integers is commutative.

1.4. Multiplication of integers is associative.

1.5. Addition and multiplication of integers distribute.

1.6. One is the multiplicative identity.

1.7. $a(-b) = -(ab)$ always.

Food for thought: Why is it not sensible to divide by zero with remainders?

More food for thought: How might you prove that there are infinitely many primes assuming the fundamental theorem of arithmetic?