The integers

It is necessary to know the axioms (rules or laws of algebra) for working with the integers $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$. Axioms for the natural numbers $1, 2, 3, \ldots$ are given in the text (Biggs) in Sections 4.1 and 4.2. But I prefer that you take a look at a set of axioms for the entire system of integers, e.g.

http://faculty.wwu.edu/curgus/Courses/209_201220/AxiomsZ.pdf

You may also search for “axioms for integers” on the web.

Most of the rules apply to other algebraic systems, e.g. the real numbers. But read about “well-ordering” or the principle of induction, which are special for the integers. The well-ordering principle states that every nonempty set of positive integers has a least element.

Everything we will prove about integers follows from these rules. For example, $2 + 2 = 4$ is a consequence. But you may notice that while 0 and 1 are mentioned in the axioms, there is no mention of 2 or 4. These must be defined before we can even think about $2 + 2 = 4$. The definitions are

$$2 = 1 + 1,$$
$$3 = 2 + 1,$$
$$4 = 3 + 1.$$

Now we can prove $2 + 2 = 4$ using the axioms and the definitions.

$$2 + 2 = 2 + (1 + 1) = (2 + 1) + 1 = 3 + 1 = 4.$$  

The first equality uses the definition of 2. The second equality is by the associative law of addition. The third equality uses the definition of 3, and the fourth uses the definition of 4.

We will not use class time to rigorously prove the addition table up to $9 + 9$ and most other simple things that you already know.

Divisors

Mathematics is written in English, but many words used in mathematics have a specific technical meaning in mathematics. Be careful to distinguish mathematical terms from English words. For example the word “divides” is used in various ways in English (e.g., “she divides the cake into pieces”), but when applied to two integers $a$ and $b$, it has this precise meaning: We say “$a$ divides $b$” if and only if there exists an integer $s$ so that $b = sa.$
Exercise: Which of the following statements are true and which are false?

3 divides 12
3 divides 7
3 divides −15
−3 divides 3
3 divides 0
−7 divides 0
0 divides 3
0 divides 0

Remark: When defining terms, it has (unfortunately?) become common to omit “only if” and say e.g.

a divides b if there exists an integer s so that b = sa. The “only if” is to be understood. Make sure you understand when a term is being defined or whether the term is being used in another kind of statement.

It is common to use a few other expressions to mean the same thing as “a divides b”. These include “b is divisible by a”, “a is a divisor of b”, and “b is a multiple of a”. It is also common to write “a | b” as an abbreviation for “a divides b”.

A positive integer p is said to be prime when p > 1 and the only positive divisors of p are 1 and p. (One may regard −p as prime too, but we won’t worry about this.)

A number of elementary facts about “divides” may be derived from the axioms and the definition of “divides”. These include

**Proposition 1.**

(i) If a | b and b | c, then a | c.

(ii) If a | b and b | a, then b = ±a.

(iii) If d | a and d | b, then for any integers s and t, we have d | (sa + tb).

Here all variables represent integers. We may prove some of these statements in class.

A very important property of the integers is the following.

**Proposition 2.** Let d be a positive integer. Then for any integer a, there are unique integers q and r so that

\[ a = dq + r \quad \text{and} \quad 0 \leq r < d. \]  

Here q may be called the (partial) quotient and r the remainder “when a is divided by d”. (Don’t confuse the use of the word “divided” here with our definition of “divides”. It is easy to see that d divides a if and only if the remainder r in (\*) is zero.)

Exercise: What are q and r in (\*) when a = 17 and d = 5? When a = −17 and d = 5?
We say that \( d \) is a common divisor of integers \( a, b, c, \ldots \) when \( d \) divides all of \( a, b, c, \ldots \).

Remark: With this terminology, Proposition 1(iii) says that any common divisor of \( a \) and \( b \) divides \( sa + tb \) for any integers \( s \) and \( t \), and so any common divisor of \( a \) and \( b \) is a common divisor of \( a, b, \) and \( sa + tb \).

An common divisor \( g \) is a greatest common divisor (GCD) of \( a, b, c, \ldots \) when \( g \) is a multiple of every common divisor \( d \). Exercise: What is the GCD of 140 and 196? Of \( -14 \) and 91? Of 43 and 0? Of 0 and 0?

This is the sophisticated way to define GCD. It could be defined for integers as the numerically greatest common divisor; see Biggs, page 68. But then 0 and 0 would have no GCD. More significantly, the property that the GCD is a multiple of every common divisor is so important that it is good to take it as the definition.

With our definition of GCD, it may not be immediately clear that such a GCD exists. However, this will follow from the Euclidean algorithm. BTW, we often speak of the GCD; we have already done this in the exercise above. In fact, if \( d \) is a GCD of \( a \) and \( b \), then \(-g\) is also a GCD, and these are the only GCDs (details omitted). By the GCD, we mean the nonnegative GCD.

It is easy to determine the GCD of two integers \( a \) and \( b \) if we know their factorizations into powers of distinct primes. (We will not prove the existence and uniqueness of prime factorization in this course. See Biggs, Section 8.6.) For example, the GCD of \( 2^5 \cdot 3^2 \cdot 5^3 \cdot 11^8 \) and \( 2^9 \cdot 3^1 \cdot 5^7 \cdot 7^2 \cdot 23^2 \) is \( 2^5 \cdot 3^1 \cdot 5^3 \). But it is not in general easy to factor large integers with 100 or 1000 digits, so factorizing to compute GCDs may not be practical when large numbers are concerned.

Remark: Mathematica can sometimes factor 100 digit integers, but not always. I asked it to generate “pseudo-random” 100 digit integers and factor them. The first time, Mathematica took 0. seconds (it said) to find the five prime factors. The second time, it factored the number in 1.826 seconds (four factors). A third number took 6015.93 seconds (six prime factors this time). The hardest 100 digit numbers to factor are presumably those that are products of two primes with about 50 digits each. You would have to be extremely lucky for Mathematica to factor a 150 or 200 digit number while you wait.

**The Euclidean algorithm**

The term “algorithm” is hard to define precisely, but for our purposes an informal definition is sufficient. An algorithm is a list of rules to be applied sequentially to a set of data (of a certain form) with the goal of finding an answer to a question about the data. The desired answer may be “yes” or “no”, or it may be a number or a formula or just data of some kind. At each step more data may be produced (or the data may be modified). The rules should include a criterion for stopping the procedure, with an answer. (Some
authorities insist that the term algorithm should be used only when the procedure always ends after a finite number of steps. This property is very important to consider, but I won’t include it as part of the definition.)

Examples of algorithms include the methods for addition, multiplication, etc., that we are taught in elementary school. The addition algorithm describes one way to obtain the base 10 representation of the sum of two integers given the base 10 representations of the integers. I was taught an algorithm to extract square roots by hand, to any number of decimal digits, in junior high school. Were you? I was not taught the Euclidean algorithm for finding the GCD of two integers when I was young, but it was routinely taught in arithmetic books of the 19th century, because the GCD is, of course, relevant to reducing fractions to lowest terms.

Given integers \( a_0 > a_1 \geq 0 \), we define a sequence \( a_0, a_1, a_2, \ldots \) recursively. When \( a_{k-1} \) and \( a_k \) have been determined, STOP if \( a_k = 0 \); otherwise let \( a_{k+1} \) be the remainder when \( a_{k-1} \) is divided by \( a_k \).

Some examples:

\[
45, 26, 19, 7, 5, 2, 1, 0 \\
2700, 576, 396, 180, 36, 0 \\
144, 89, 55, 34, 21, 13, 8, 5, 3, 2, 1, 0 \\
45, 33, 12, 9, 3, 0
\]

**Theorem 3.** Apply the Euclidean algorithm to \( a_0 \) and \( a_1 \) and assume \( a_n = 0 \). Then \( a_{n-1} \) is the greatest common divisor of \( a_0 \) and \( a_1 \).

**Proof:** The proof is based on the fact that if we divide \( a \) by \( b \) to find \( a = bq + r \), then the common divisors of \( a \) and \( b \) are exactly the common divisors of \( b \) and \( r \). This is from Proposition 1(iii); see our above remark. Hence \( \text{GCD}(a, b) = \text{GCD}(b, r) \).

Thus, in the Euclidean algorithm,

\[
\text{GCD}(a_0, a_1) = \text{GCD}(a_1, a_2) = \text{GCD}(a_2, a_3) = \ldots = \text{GCD}(a_{n-1}, a_n).
\]

The last expression \( \text{GCD}(a_{n-1}, a_n) = \text{GCD}(a_{n-1}, 0) \) is \( a_{n-1} \). \( \Box \)

How many divisions might be required to find the greatest common divisor of two 1000 digit numbers? Maybe billions and billions? No. 6440 is more than enough.

**Theorem 4.** We have \( a_{i+2} < a_i / 2 \) for all relevant \( i \). Hence the number of divisions required for the Euclidean algorithm to terminate is at most

\[
2 \log_2(a_0) \approx 6.44(\text{number of digits of } a_0).
\]
Exercise: How many divisions are required by the Euclidean algorithm for two successive Fibonacci numbers? The sequence of Fibonacci numbers is

\[ 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, \ldots \]

The sequence begins with two 1s; thereafter each term is the sum of the two preceding terms.

Proof: If \( a_{i+1} \leq a_i/2 \), the claim certainly holds, since always \( a_{i+2} < a_{i+1} \). And if \( a_{i+1} > a_i/2 \), then the remainder when \( a_i \) is divided by \( a_{i+1} \) (it will only go in once) is \( a_{i+2} = a_i - a_{i+1} < a_i/2 \).

The Euclidean algorithm is one of the routines built into Mathematica. I asked Mathematica to generate two “pseudo-random” 500 digit numbers and compute their GCD. The answer was given instantly. (It was 1.)

**Theorem 5.** If the greatest common divisor of integers \( a \) and \( b \) is \( d \), then there are integers \( s, t \) so that \( d = sa + tb \).

A proof is provided by the following algorithm (often called the *extended Euclidean algorithm*).

We will assume that \( a \geq b > 0 \), though this is not very important. Write \( a_0 = a \), \( a_1 = b \). Generate a matrix with three columns by starting with the two rows \( x_0 = (a, 1, 0) \) and \( x_1 = (b, 0, 1) \). We will call the rows \( x_i = (a_i, s_i, t_i) \), so \( a_0 = a, a_1 = b \). Once rows \( k - 1 \) and \( k \) have been generated (you can throw the earlier ones away if you wish), let row \( k + 1 \) be generated by subtracting an integer multiple of row \( k \) from row \( k - 1 \) so that the first coordinate is the remainder \( a_{k+1} \) when \( a_{k-1} \) is divided by \( a_k \), unless \( a_k = 0 \), when you should stop.

Here is an example (on the left).

\[
\begin{pmatrix}
45 & 1 & 0 \\
26 & 0 & 1 \\
19 & 1 & -1 \\
7 & -1 & 2 \\
5 & 3 & -5 \\
2 & -4 & 7 \\
1 & 11 & -19 \\
0 & -26 & 45 \\
\end{pmatrix}
\]

\[
\begin{align*}
45 &= (1)[45] + (0)[26] \\
26 &= (0)[45] + (1)[26] \\
19 &= (1)[45] + (-1)[26] \\
7 &= (-1)[45] + (2)[26] \\
5 &= (3)[45] + (-5)[26] \\
2 &= (-4)[45] + (7)[26] \\
1 &= (11)[45] + (-19)[26] \\
0 &= (-26)[45] + (45)[26] \\
\end{align*}
\]

Note that for each \( i = 0, 1, 2, \ldots \), we have \( a_i = s_i a + t_i b \). This is because this relation holds when \( i = 0 \) and \( i = 1 \) and it is carried over to each succeeding row. The equations
corresponding to the rows in our example are given on the right. Since the greatest common
divisor is in the first column, we find the desired relation. In our example, \( 1 = 11 \cdot 45 - 19 \cdot 26 \).

Integers \( a \) and \( b \) are said to be relatively prime when their GCD is 1.

If \( a \) and \( b \) are relatively prime, then a two-pan balance (or scale) and weights of \( a \) units and \( b \) units can be used to weigh out one unit (or any positive integer number of
units) of some commodity. For example, if we have weights of 45 pounds and 26 pounds,
we can put 11 of the 45 pound weights on the left pan and 19 of the 26 pound weights
on the right pan; then pour gold dust into the right pan until the scale balances, in which
case you have exactly one pound of gold.

A related question is, given relatively prime integers \( a \) and \( b \), what integers \( c \) can
be written as \( sa + tb \) with \( s \) and \( t \) nonnegative integers? For example, you may have an
unlimited number of 7 cent and 11 cent postage stamps. What (exact) values of postage
can you make. First class mail is currently 46 cents, and since \( 46 = 5 \cdot 7 + 1 \cdot 11 \), we can
use our stamps without wasting money. But when postage rises to 59 cents, we cannot use
7 cent and 11 cent stamps to (exactly) add up to that amount.

Facts/question: When \( a \) and \( b \) are relatively prime positive integers, any integer \( c \geq \)
\( (a - 1)(b - 1) \) can be written as a nonnegative integer linear combination of \( a \) and \( b \). But
\( (a - 1)(b - 1) - 1 \) cannot be so written. How many of the integers \( c \) with \( 0 \leq c < (a - 1)(b - 1) \)
are nonnegative integer linear combinations of \( a \) and \( b \)? (This material may come up on
the first Problem Set.)