WORKSHEET ON NUMBERS, MATH 215 FALL 18(WHYTE)

We start our study of numbers with the integers:

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

and their subset of natural numbers:

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

For now we will not worry about defining or justifying the most basic properties : we will assume that we know what the integers and natural numbers are, that we know how to add and multiply them, and that rules like commutativity, associativity, and distributivity all hold. The first thing we wish to study is **divisibility**:

Definition 0.1. *Let a and b be two integers. We say that a* **divides** *b if there is an integer q so that $b = aq$. We will use the notation $a|b$ as shorthand for this property.*

Proposition 0.2. *Let a, b, and c be integers. If $a|b$ and $a|c$ then $a|(b+c)$.*

Proposition 0.3. *Let a, b, and c be integers. If $a|b$ then $a|bc$.*

Question 0.4. *Which integers divide zero? Which are divisible by zero?*

Proposition 0.5. *Let a, b, and c be integers. If $a|b$ and $a|c$ then $a|(b-c)$.*

Question 0.6. *Which integers divide one? Which are divisible by one?*

Proposition 0.7. *Let a, b, c, s and t be integers. If $a|b$ and $a|c$ then $a|(sb+tc)$.*

Proposition 0.8. *Let a, b, and c be integers. If $a|b$ and $b|c$ then $a|c$.*

Question 0.9. *Does $2|4$? Does $2|3$? How can you prove your answers?*

As the last question indicates, we are missing some of the basic structure of the integers. The next piece that we want to incorporate is that we can compare integers to see which is bigger. This is what mathematicians call an **ordering**. To be more precise:

Definition 0.10. *An integer n is* **positive** *if and only if $n \in \mathbb{N}$*

Definition 0.11. *For any two integers a and b, we say $a < b$ if and only if $b - a$ is positive.*

We can now prove many of the basic facts we know about comparing integers

Problem 0.12. *Prove the following (you may use that the sum and product of natural numbers are natural numbers)*

(1) If $a < b$ then for any c we have $a + c < b + c$
(2) If $a < b$ and $b < c$ then $a < c$
(3) For any a and b exactly one of the following holds: $a < b$, $b < a$, or $a = b$
(4) If a is positive and b is negative then ab is negative
(5) If a is negative and b is negative then ab is positive
(6) Let a and b be integers with $a < b$, then for all $c > 0$ we have $ac < bc$ and for all $c < 0$ we have $bc < ac$

We can also now establish some facts that get used quite often:

Proposition 0.13. *Let a and b be integers with $ab = 0$ then $a = 0$ or $b = 0$*

Proposition 0.14. *Let a, b, and c be integers with $c \neq 0$ then $ac = bc \implies a = b$*

This almost resolves the question at the end of the last page:

Proposition 0.15. *If q is an integer with $2q = 3$ then $1 < q < 2$.*

To show that there aren't any such q we need one more fact about the integers:

Axiom 0.16. *There are no integers n with $0 < n < 1$.*

Using this you can now show:

Proposition 0.17. *2 does not divide 3*

We now have an almost complete list of axioms for the integers and so can prove most facts we want. What we are missing is an axiom to guarantee that if we start counting we eventually get to every natural number. This can be formulated a number of ways, but we will start with :

Well-ordering Axiom: If S is any non-empty subset of $\mathbb{N}$ then there is a smallest element $s_0 \in S$ (here "smallest" means that for any $s_0 < s$ for all other $s \in S$.)

This may not at first seem to be the same idea as claiming that we eventually reach every element of $\mathbb{N}$ by counting. Here is a more direct translation of that idea"

Proposition 0.18. *Let $A \subset \mathbb{N}$ and suppose that $1 \in A$ and for every $a \in A$ we also have $a + 1 \in A$, then $A = \mathbb{N}$.*

The idea here is that we are assuming $1 \in A$, and applying the second assumption, $1 + 1 = 2$ must also be in A. But then, applying it again, $2 + 1 = 3$ is in A, etc. In other words, the assumptions here say roughly that A contains all the numbers you can reach by counting. The conclusion asserts that this must be all the natural numbers, which is a way of saying that every natural number can be reached by counting. We can prove this from the Well-ordering axiom as follows:

Let S be the set $\mathbb{N} \setminus A$. If S is empty then $A = \mathbb{N}$ as claimed, so we just need to rule out any other possibility. If S is not empty then by the well-ordering axiom there is a smallest $s_0 in S$. What can s_0 be? It can't be 1 since we assumed that 1 is in A, so we must have $s_0 > 1$. Then consider the number $n = s_0 - 1$. Since $s_0 > 1$ we have $n > 0$ so $n \in \mathbb{N}$. We also know that $n < s_0$ so, since s_0 is the smallest element of S, n must not be in S. That means that $n \in A$. But then our assumption says that $n + 1$ is also in A, and $n + 1 = s_0$ so s_0 is in A. That is impossible since s_0 is also known to be in S.

This proof outline is common : we what to show something is true for all $n \in \mathbb{N}$, so we look at the set of numbers where it fails to hold and try to prove it is empty. If it isn't empty then it has a smallest element s (by well-ordering again). This is the smallest natural number for which our desired statement is false, so it must be true for $s - 1$ (and all other smaller numbers), and we can often use this to contradict things. Here's a more concrete example:

Proposition 0.19. *Let n be a natural number. Either $n = 2q$ for some integer q or $n = 2q + 1$ for some integer q.*

As before, let S be the set of natural numbers which are neither $2q$ for any q nor are $2q + 1$ for any q. Our goal is to show that S is empty. If not,

then it has a smallest element, s_0. Since $1 = 2(0) + 1$ we know that $s_0 > 1$, so $s_0 - 1$ is also a natural number. Since $s_0 - 1 < s_0$ and s_0 is the smallest element of S we must have $s_0 - 1$ not in S. This means that $s_0 - 1$ is either of the form $2q$ or $2q + 1$.

In the first case, $s_0 - 1 = 2q$ we can add one to both sides to get $s_0 = 2q$, which is impossible since $s_0 \in S$.

Similarly, if $s_0 - 1 = 2q + 1$ then $s_0 = 2q + 2 = 2(q + 1)$ so s_0 is twice some integer, which is again impossible since $s_0 \in S$.

The only possibility left is that S is empty, so that no such s_0 exists. □

Alternatively, you can prove such statements via Proposition 0.18. For example, let A be the set of natural numbers which can be written as $2q$ or $2q + 1$ for some integer q. Then since $1 = 2(0) + 1$ we have $1 \in A$ and, if a is in A then either:

$a = 2q$ for some q, so $a + 1 = 2q + 1$ and so $a + 1 \in A$ or
$a = 2q + 1$ for some q, so $a + 1 = 2q + 2 = 2(q + 1)$ so $a + 1 \in A$]

Since, in both cases, we have $a + 1 \in A$ we can apply Proposition 0.18 to conclude $A = \mathbb{N}$. □

Problem 0.20. *Here are a few more things one can prove with these methods, try to write the proof both directly from the well-ordering axiom and via proposition 0.18:*

(1) Every natural number is $3q$, $3q + 1$, or $3q + 2$ for some integer q.
(2) For every natural number n, $n < 2^n$
(3) For all n, $\frac{d}{dx}x^n = nx^{n-1}$ (this assumes you know the product rule and that $\frac{d}{dx}x = 1$

We often want to use these arguments in more general settings: for subsets of the integers, with largest elements rather than smallest, and so on. To state these we start with some definitions:

Definition 0.21. *If S is a subset of $\mathbb{Z}$ then an integer n is a lower bound for S if $n \leq s$ for all $s \in S$. A set which has a lower bound is called bounded from below. Similarly, an integer m is an upper bound for S if $s \leq m$ for all $s \in S$, and a set with an upper bounded is called bounded from above. A set which is both bounded from above and from below is simply called bounded.*

Proposition 0.22. *Here are some basic facts and questions:*

1. *If n is a lower bound for S and $m \leq n$ then m is also a lower bound for S.*
2. *If n is a lower bound for S and $T \subset S$ then n is also a lower bound for T.*
3. *Can you formulate versions of the above for upper bounds?*
4. *The set $\mathbb{N}$ is bounded from below. Is it bounded from above?*
5. *If S is the set of odd integers, is S bounded from above? from below?*

With these terms in mind we can state a more general form of the well ordering principle:

Proposition 0.23. *If S is a non-empty set of integers which is bounded from below then S contains a smallest element. (Hint: shift S into $\mathbb{N}$ by adding something, apply the basic well ordering principle, and then shift back)*

Similarly, we have:

Proposition 0.24. *If S is a non-empty set of integers which is bounded from above then S contains a largest element. (Hint #1: multiply by -1, apply the lower bound version, then multiply by -1 again. Hint #2: For a completely different proof, let T be the set of upper bounds for S and apply the well ordering principle to T)*

These are all the basic rules (called "axioms") that we need to say what the properties of the integers are that distinguish them from all other kinds of numbers. These are listed on the next page. A good exercise is to look back over all the properties we assumed up until this point and make sure you know how they follow from the things listed (the most challenging to deduce is probably that there is no integer between 0 and 1).

AXIOMS for the Integers:

(1) If a and b are integers then $a+b$ and ab are integers.

(2) For any a and b, $a+b=b+a$ and $ab=ba$.

(3) For any a, b, and c. $a+(b+c)=(a+b)+c$ and $a(bc)=(ab)c$.

(4) For any a,b, and c, $a(b+c)=ab+ac$.

(5) There are integers 0 and 1 so that for any a, $a=a+0=a1$.

(6) For any a there is a b with $a+b=0$.

(7) For any a and b exactly one of the following is true:
- $a=b$
- $a<b$
- $b<a$

(8) If $a<b$ and $b<c$ then $a<c$.

(9) If $a<b$ then for any c, $a+c<b+c$.

(10) If $a>0$ and $b>0$ then $ab>0$.

(11) (Well ordering) If $S\subset\mathbb{Z}$ is non-empty and bounded from below then S contains a smallest element.

Definition 0.25. *Let a and b be integers and let n be a natural number. We say a* **is congruent to** *b* **modulo** *n if $n|(a-b)$. We use the notation $a \equiv b \bmod n$ for this property.*

Problem 0.26. *Decide whether each of the following statements is true and justify your answers:*

- $2 \equiv 93 \bmod 13$
- $27 \equiv 4 \bmod 5$
- $15 \equiv -6 \bmod 7$
- $-3 \equiv -8 \bmod 2$

Proposition 0.27. *If a is an integer and n a natural number then $a \equiv a \bmod n$.*

Proposition 0.28. *Let a and b be integers and n a natural number. If $a \equiv b \bmod n$ then $b \equiv a \bmod n$.*

Proposition 0.29. *Let a, b, and c be integers and n a natural number. If $a \equiv b \bmod n$ and $b \equiv c \bmod n$ then $a \equiv c \bmod n$.*

Proposition 0.30. *Let a, b, and c be integers and n a natural number. If $a \equiv b \bmod n$ then $a + c \equiv b + c \bmod n$.*

Proposition 0.31. *Let a, b, and c be integers and n a natural number. If $a \equiv b \bmod n$ then $ac \equiv bc \bmod n$.*

Proposition 0.32. *Let a, b, and c be integers and n a natural number. If $a \equiv b \bmod n$ and $b \equiv c \bmod n$ then $a \equiv c \bmod n$.*

Proposition 0.33. *Let a and b be integers and n a natural number. If $a \equiv b \bmod n$ then $a^2 \equiv b^2 \bmod n$.*

Proposition 0.34. *Let a and b be integers and n a natural number. If $a \equiv b \bmod n$ then $a^3 \equiv b^3 \bmod n$.*

The last two propositions suggest the following:

Conjecture 0.35. *Let a and b be integers and n and m natural numbers. If $a \equiv b \bmod n$ then $a^m \equiv b^m \bmod n$.*

Do you believe this conjecture? Can you prove it?

Proposition 0.36. *Let a be an integer and b a natural number. There is an integers q and r with $0 \leq r < b$ such that:*

$$a = bq + r$$

Here q is called the **quotient** and r is called the **remainder**. Here's a hint: think about all possible q and $r \geq 0$ that make the equation hold (without the assumption $r < b$) and then use well ordering to find the smallest such r.

This proposition is often called the **division algorithm** because it is tells you exactly what one gets from old fashioned long division of natural numbers - a quotient and a remainder. However there's a subtlety here - the proposition says that q and r exist, but not that they are unique - in other words the division problem might have more than one right answer. Obviously that's not what we expect. Here's how that is phrased precisely (make sure you understand why, then prove it):

Proposition 0.37. *Let b a natural number and q_1, q_2, r_1, r_2 integers with $0 \leq r_1 < b$ and $0 \leq r_2 < b$ such that $q_1 b + r_1 = q_2 b + r_2$ then $q_1 = q_2$ and $r_1 = r_2$.*

In particular, we get the following about congruences:

Proposition 0.38. *For any integer a and natural number n there is exactly one integer b with $0 \leq b < n$ such that $a \equiv b \bmod n$.*

Definition 0.39. *A natural number $n > 1$ is* **prime** *if the only natural numbers m with $m|n$ are $m = 1$ and $m = n$*

Proposition 0.40. *If $n > 1$ is a natural number then there is a prime number p such that $p|n$.*

Proposition 0.41. *Every natural number $n > 1$ can be written as a product of primes:*

$$n = p_1^{k_1} \cdots p_m^{k_m}$$

where $p_1, p_2, \ldots, p_m$ are prime numbers and k_i are natural numbers.

This is the **prime factorization theorem**. It usually also comes with a uniqueness statement. Can you figure out what this should say? It tuns out that the uniqueness is more subtle than it appears, so we will need to develop some other ideas before tackling it. We start with another definition:

Definition 0.42. *Given two integers a and b a* **common divisor** *is an integer d satisfying such that $d|a$ and $d|b$.*

Proposition 0.43. *Show that unless a and b are both zero they have a greatest common divisor (hint: fist prove that if x and y are natural numbers and $x|y$ then $x \leq y$)*

Problem 0.44. *Let n be a natural number. Find the greatest common divisor of n and 0.*

Proposition 0.45. *Let p be a prime number. Show that for any integer a the greatest common divisor of p and a is either p (if $p|a$) or is 1.*

Proposition 0.46. *Let a and b be natural numbers. Write $a = bq + r$ using the division algorithm. Show that the common divisors of a and b are the same as the common divisors of r and b.*

This gives a practical way to compute greatest common divisors: take the larger of a and b and replace it with its remainder when divided by the other, and repeat until one of the numbers is zero.

Problem 0.47. *What is the greatest common divisor of 120 and 168? of 59 and 1016?*

Question 0.48. *Can you show that this process always works?*

There is another surprising way of characterizing the gcd. For two numbers a and b, we think about all the numbers you can get by adding multiples of a and b together. We can imaging this by thinking of a and b as dollar values of bills and then asking what prices can paid with them. For example, if your country only issues a 6 dollar bill and a 14 dollar bill, can you buy something that costs 10 dollars? Yes - you pay with two 14 dollar bills and get three 6 dollar bills back in change. Can you buy something that costs 15 dollars? No - all the bills are worth an even number of dollars so there is no way to get an odd net transaction. Formulated more abstractly:

Let $S(a, b) = \{na + mb : n, m \in \mathbb{Z}\}$.

Proposition 0.49. *If c is a common divisor of a and b then $c|s$ for all $s \in S(a, b)$*

Proposition 0.50. *If $s \in S(a, b)$ then $gcd(a, b)|s$.*

Proposition 0.51. *If $s \in S(a, b)$ then $sx \in S(a, b)$ for all $x \in \mathbb{Z}$*

Proposition 0.52. *If $S(a, b) = \mathbb{Z}$ if and only if $1 \in S$*

Proposition 0.53. *The set $S(0, 0)$ is $\{0\}$. For any other a and b the set $S(a, b)$ is infinite.*

Proposition 0.54. *If $a|b$ then $S(a, b)$ is precisely the set of multiples of a.*

The main fact we are aiming to prove is a more general version of the last statement:

Proposition 0.55. *For any a and b in $\mathbb{Z}$, not both zero, the set $S(a, b)$ is precisely the set of multiples of $gcd(a, b)$.*

Problem 0.56. *Show that proposition 0.55 is equivalent to the statement that $gcd(a, b) \in S(a, b)$.*

The key ingredient in the proof of proposition 0.55 is this:

Proposition 0.57. *Let $s \in S(a,b)$ and write $s = aq + r$ using the division algorithm, then $r \in S(a,b)$ (note that the same works if we divide by b instead of a).*

Using that you can prove:

Proposition 0.58. *If c is the smallest positive element of $S(a,b)$ then c is a common divisor of a and b.*

This is almost enough to finish the proof of proposition 0.55. The only missing piece is to show that this c must be the greatest common divisor, not a smaller one. But using the earlier propositions we know that c must be divisible by $gcd(a,b)$.

Problem 0.59. *Put all of the above together to give a complete proof of Proposition 0.55.*