Mathematics 2200H – Mathematical Reasoning
TRENT UNIVERSITY, Fall 2019

Assignment #6
This and that
Due on Friday, 18 October.

Recall that if a and b are natural numbers, then $a \mid b$ means that a is a factor of b, *i.e.* $b = ac$ for some natural number c, and that a natural number $p > 1$ is said to be *prime* if it has no natural number factor other than itself and 1.

1. Suppose p is prime, a, $b \in \mathbb{N}$, and $p \mid ab$. Show that $p \mid a$ or $p \mid b$. *[3]*

SOLUTION. The most common proofs of this proposition rely on the fact that if two natural numbers a and b have a greatest common divisor d, then there are integers x and y such that $ax + by = d$. (This fact, in turn, is obtained by analyzing the Euclidean algorithm for finding a greatest common divisor. Look it up!) Since one of x or y is normally going to be negative here (because d must be $\leq$ both a and b), this approach requires having $\mathbb{Z}$ sorted out first. We'll take an alternate approach that proceeds by induction on the prime p. Let p_k denote the kth prime, so $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, and so on.

Base Step: ($p = p_1 = 2$) Suppose $2 \mid ab$ for some a, $b \in \mathbb{N}$. This means that ab is an even number. Since the product of two odd natural numbers is odd – $(2k + 1)(2n + 1) = 4kn + 2k + 2n + 1 = 2(2kn + k + n) + 1$, it follows that at least one of a or b is even, *i.e.* $2 \mid a$ or $2 \mid b$.

Inductive Hypothesis: ($p = p_i$ for $1 \leq i \leq k$) If $1 \leq i \leq k$, then for all a, $b \in \mathbb{N}$, if $p_i \mid ab$, then $p \mid a$ or $p \mid b$.

Inductive Step: ($p = p_{k+1}$) Assume the Inductive Hypothesis and that $p_{k+1} \mid ab$ for some a, $b \in \mathbb{N}$. Suppose, by way of contradiction, that $p_{k+1} \nmid a$ and $p_{k+1} \nmid b$. Then we can write $a = xp_{k+1} + r$ and $b = yp_{k+1} + s$ for some natural numbers x, y, r, and s with $0 < r < p_{k+1}$ and $0 < s < p_{k+1}$. (x and y are the number of times you can remove p_{k+1} things at a time from a collection of a or b things, respectively, and r and s are the numbers of things left over. Obviously, r and s must be less than p_{k+1}. If r or s were 0, then p_{k+1} would divide a or b, respectively.) Then

$$ab = (xp_{k+1} + r)\,(yp_{k+1} + s) = (xyp_{k+1} + sx + ry)\,p_{k+1} + rs\,,$$

from which it follows that $p_{k+1} \mid rs$, *i.e.* $rs = zp_{k+1}$ for some natural number z. Since $r > 0$ and $s > 0$, we have $rs > 0$, and thus we must have $z > 0$. On the other hand, since $r < p_{k+1}$ and $s < p_{k+1}$, we have $rs < p_{k+1}^2$, from which it follows that $z < p_{k+1}$. Note also that we can't have either $r = 1$ or $s = 1$ since then the other would have to have p_{k+1} divide it, contradicting the fact that both are less than p_{k+1}.

If $z = 1$, then $p_{k+1} = rs$, with both r and s strictly between 1 and p_{k+1}, which contradicts p_{k+1} being a prime number.

If $z > 1$, execute the following process:

i. Pick a prime factor p_i of z. Since $p_i \leq z < p_{k+1}$, we must have $1 \leq i \leq k$.
ii. By the inductive hypothesis, since $p_i \mid xp_{k+1} = rs$, we have $p_i \mid r$ or $p_i \mid s$. If $p_i \mid r$, replace r by r/p_i; if $p_i \nmid r$, replace s by s/p_i. Either way, replace z by z/p_i.
iii. If the new z is 1, halt; otherwise, go back to step i with the new r, s, and z.

Since z decreases with each pass through the process, it does eventually halt. When it does, you have $p_{k+1} = rs$, with both r and s less than p_{k+1}. (The original r and s were already less than p_{k+1} and the process makes any replacements no larger . . .) This brings us back to the case $z = 1$ and the contradiction to p_{k+1} being prime.

Since assuming that $p_{k+1} \mid ab$ for some $a, b \in \mathbb{N}$, but $p_{k+1} \nmid a$ and $p_{k+1} \nmid b$, leads to a contradiction, it must be the case that $p_{k+1} \mid ab$ implies that $p_{k+1} \mid a$ or $p_{k+1} \mid b$. $\square$

2. Show that there are infinitely many prime numbers. *[2]*

SOLUTION. Suppose, by way of contradiction, that there were only finitely many prime numbers, say p_1, p_2, $p_3, \ldots, p_n$. Let $q = p_1 p_2 p_3 \cdots p_n + 1$. Since each p_i divides the product $p_1 p_2 p_3 \cdots p_n$ but does not divide 1, no p_i can divide q. On the other hand, if $q = rs$ for some natural numbers r, $s > 1$, we could keep factoring r and/or s into smaller and smaller numbers until we encountered prime factors. Such prime factors would have to divide q as well, which we just showed was impossible. It follows that q cannot have any factors smaller than itself except for 1, *i.e.* q is prime. This contradicts the assumption that our finite list of all the prime numbers actually included all the prime numbers.

Since assuming otherwise leads to a contradiction, there must be infinitely many prime numbers. $\square$

Recall from class that we defined the set of integers by defining the equivalence relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ by $(a, b) \sim (c, d) \implies a + d = c + b$, and then took the integers to be equivalence classes for this relation, *i.e.* $\mathbb{Z} = \left\{ [(a, b)]_\sim \mid (a, b) \in \mathbb{N} \times \mathbb{N} \right\}$. We then proceeded to define $0_\mathbb{Z} = [(0, 0)]_\sim$, $1_\mathbb{Z} = [(1, 0)]_\sim$, $-[(a, b)]_\sim = [(b, a)]_\sim$, $[(a, b)]_\sim + [(c, d)]_\sim = [(a + c, b + d)]_\sim$, and $[(a, b)]_\sim \cdot [(c, d)]_\sim = [(ac + bd, ad + bc)]_\sim$.

3. Show that $+$ is an associative operation on $\mathbb{Z}$. *[2]*

SOLUTION. Here goes! Suppose $[(a, b)]_\sim$, $[(c, d)]_\sim$, and $[(e, f)]_\sim$ are in $\mathbb{Z}$. Then

$$\begin{aligned}
\big([(a, b)]_\sim + [(c, d)]_\sim\big) + [(e, f)]_\sim &= [(a + c, b + d)]_\sim + [(e, f)]_\sim \\
&= [((a + c) + e, (b + d) + f)]_\sim \\
&= [(a + (c + e), b + (d + f))]_\sim \quad \text{since } + \text{ is associative in } \mathbb{N} \\
&= [(a, b)]_\sim + [(c + e, d + f)] \\
&= [(a, b)]_\sim + \big([(c, d)]_\sim + [(e, f)]_\sim\big) \,,
\end{aligned}$$

as required. Thus $+$ is an associative operation on $\mathbb{Z}$. $\square$

4. Show that $\cdot$ is a well-defined operation on $\mathbb{Z}$. *[3]*

SOLUTION. Suppose $[(a, b)]_\sim = [(a', b')]_\sim$ and $[(c, d)]_\sim = [(c', d')]_\sim$. We need to show that $[(ac + bd, ad + bc)]_\sim = [(a'c' + b'd', a'd' + b'c')]_\sim$, which is, by definition, equivalent to showing that $(ac + bd, ad + bc) \sim (a'c' + b'd', a'd' + b'c')$, *i.e.* that $(ac + bd) + (a'd' + b'c') = (a'c' + b'd') + (ad + bc)$. Considering the hypotheses, we have, by definition, that $[(a, b)]_\sim = [(a', b')]_\sim \iff (a, b) \sim (a', b') \iff a + b' = a' + b$ and $[(c, d)]_\sim = [(c', d')]_\sim \iff (c, d) \sim (c', d') \iff c + d' = c' + d$.

Intuitively, there is an easy argument: $a + b' = a' + b$ and $c + d' = c' + d$ tell us that $a - b = a' - b'$ and $c - d = c' - d'$, so $(ac + bd) - (ad + bc) = (a - b)(c - d) = (a' - b')(c' - d') = (a'c' + b'd') - (a'd' + b'c')$, and thus $(ac + bd) + (a'd' + b'c') = (a'c' + b'd') + (ad + bc)$, as required. The teeny, tiny, problem with this is that we don't really have subtraction as we know it in the natural numbers because they lack negatives. Since finding ways of working around this is pretty hard, solutions that used a little subtraction were given full credit ...

So what can we do? We need to proceed from $a + b' = a' + b$ and $c + d' = c' + d$ to $(ac+bd)+(a'd' + b'c') = (a'c' + b'd')+(ad+bc)$ using only operations and properties available to us in the natural numbers. (No subtraction, no division, no negatives, ...) What we do have to work with are the facts that $+$ and $\cdot$ are both commutative and associative, satisfy the distributive laws, have 0 and 1 respectively as unit elements, and satisfy cancellation laws. The cancellation law for $+$ (*i.e.* $a + b = c + b \implies a = c$), in particular, is necessary to work around the lack of subtraction.

Here goes! If $a + b' = a' + b$ and $c + d' = c' + d$, we then get:

- $ac + b'c = a'c + bc$ (multiply both sides of $a + b' = a' + b$ by c)
- $b'c' + b'd = b'c + b'd'$ (multiply both sides of $c + d' = c' + d$ by b' and switch sides)
- $a'd + bd = ad + b'd$ (multiply both sides of $a + b' = a' + b$ by d and switch sides)
- $a'c + a'd' = a'c' + a'd$ (multiply both sides of $c + d' = c' + d$ by a')

Now add up all the left-hand sides and all the right-hand sides and set them equal:

$$ac + b'c + b'c' + b'd + a'd + bd + a'c + a'd' = a'c + bc + b'c + b'd' + ad + b'd + a'c' + a'd$$

We can now cancel $b'c$, $b'd$, $a'd$, and $a'c$ on both sides to get:

$$ac + b'c' + bd + a'd' = bc + b'd' + ad + a'c'$$

With a little rearranging this is

$$(ac + bd) + \left(a'd' + b'c'\right) = \left(a'c' + b'd'\right) + (ad + bc)\,,$$

which is exactly what is needed to conclude that $(ac + bd, ad + bc) \sim (a'c' + b'd', a'd' + b'c')$, and hence that $[(ac + bd, ad + bc)]_\sim = [(a'c' + b'd', a'd' + b'c')]_\sim$.

Thus multiplication on the integers is well-defined. ■