Mathematics 2200H – Mathematical Reasoning
TRENT UNIVERSITY, Fall 2021

Solutions to Assignment #3
A Little Number Theory
Due on Friday, 1 October.

For this assignment you may assume that basic arithmetic on the integers works in the ways we are familiar with. (We will be showing that it does after we officially define the natural numbers and the integers in class.) You may also assume the following fact:

(↓) *(Descending Chain Condition)* Every strictly decreasing sequence of positive integers is finite.

That is, if you have a sequence of positive integers $a_0 > a_1 > a_2 > \cdots$, then it cannot be infinite. (In fact, it can have at most $|a_0|$ elements. Why?) This fact is surprisingly powerful; it turns out to be equivalent to being able to do induction, which we will see entirely too much of in the course of building up the various common number systems.

1. Suppose that a and b are positive integers with $a < b$. Use (↓) to show that there exist unique integers $c \geq 1$ and $0 \leq r < a$ such that $b = ca + r$. *[3]*

SOLUTION. Since a is positive, *i.e.* $a > 0$, we have that $b > b - a > b - 2a > b - 3a > \cdots$, and because $a < b$, it follows that this strictly decreasing sequence has at least two positive elements, namely b and $b - a$. By the Descending Chain Condition, there are only finitely many positive integers in this strictly decreasing sequence. This means that there is some $n \geq 1$ such that if we subtract a one more time from $b - na$, the result will not be positive, *i.e.* $b - (n+1)a \leq 0$.

Suppose, then, that $b - na$ is the last (and smallest) positive integer in the sequence. There are two cases: either $b - na < a$, *i.e.* $b - (n+1)a < 0$, or $b - na = a$, *i.e.* $b - (n+1)a = 0$. In the first case, let $c = n$ and $r = b - na$, so $b = na + (b - na) = ca + r$, where $c = n \geq 1$ and $0 < b - na = r < a$; in the second case, let $c = n + 1$ and $r = 0$, so $b = (n+1)a + 0 = ca + r$, where $n + 1 \geq 2$ and $0 = r < a$. Either way, we have a $c \geq 1$ and r with $0 \leq r < a$ such that $b = ca + r$.

It remains to show that c and r are unique. Suppose, for the sake of argument that we also have $b = ka + s$ for some integers k and s with $k \geq 1$ and $1 \leq s < a$. We need to show that $c = k$ and $r = s$.

First, suppose $r \geq s$. Then $0 \leq r - s = (b - ca) - (b - ka) = (c - k)a$, so $r - s$ is a multiple of a, while $0 \leq r - s < r < a$, so $0 \leq r - s < a$ as well. The only non-negative multiple of a that is less than a is 0, so $r - s = 0$, *i.e.* $r = s$. A similar argument, with the roles of r and s reversed show that $r = s$ in the case that $r \leq s$.

Second, since we have established that $r = s$, it follows that $b - ca = r = s = b - ka$, from which we can deduce that $ca = ka$. It follows that $(c - k)a = ca - ka = 0$. Since $a > 0$, this is only possible if $c - k = 0$, *i.e.* $c = k$.

Thus c and r must be unique. ■

Recall that an integer a divides an integer b, often written as $a|b$, if $b = ca$ for some integer c, *i.e.* $r = 0$ above. [In the case where a and b are positive, anyway.] The *greatest*

common divisor of two integers a and b, often written as $\gcd(a, b)$ or just (a, b), is the largest positive integer d such that $d|a$ and $d|b$.

2. Use **1** and **(↓)** to show that any two positive integers do have a greatest common divisor. **[5]**

Hint: If you have trouble getting started, look up the Euclidean algorithm.

SOLUTION. Suppose a and b are positive integers. There are three cases:

Case 1. If $a = b$, then a (or you could call it b :-) is the greatest common divisor of a and b, since $a = 1 \cdot b$.

Case 2. If $a < b$, consider the following process* to discover the greatest common divisor d of a and b:

Start. Let $a_0 = a$ and $b_0 = b$. Note that $a_0 = a < b = b_0$.

Step n. Given positive integers $a_n < b_n$ for some $n \geq 0$, the result of **1** tells us that there are unique integers $c_n \geq 0$ and r_n with $0 \leq r_n < a_n$ such that $b_n = c_n a_n + r_n$.

- If $r_n = 0$, then we stop the process with $d = a_n$.
- If $r_n > 0$, let $b_{n+1} = a_n$ and $a_{n+1} = r_n$ and proceed to Step $n + 1$. (Note that in this case $0 < a_{n+1} = r_n < a_n = b_{n+1}$, as required to do Step $n + 1$.)

Since $a = a_0 > a_1 > a_2 > \cdots$ is a descending sequence of positive integers, it must be finite by the Descending Chain Condition, so the process must terminate at Step n for some $n \geq 0$, giving us $d = a_n$ as the candidate for the greatest common divisor.

We need to show that the d produced in this way is indeed the greatest common divisor. First, we show that d divides both $a = a_0$ and $b = b_0$. $d = a_n$ so $d|a_n$ and $b_n = c_n a_n + 0 = c_n d$, so $d|b_n$. Since d divides both $r_{n-1} = a_n$ and $a_{n-1} = b_n$, and $b_{n-1} = c_{n-1}a_{n-1} + r_{n-1}$ it follows that $d|b_{n-1}$ as well. Then, since d divides both $r_{n-2} = a_{n-1}$ and $a_{n-2} = b_{n-1}$, and $b_{n-2} = c_{n-2}a_{n-2} + r_{n-2}$ it follows that $d|b_{n-2}$ as well, and so on. Backtracking like this all the way back to $a = a_0$ and $b = b_0$ tells us that d divides both a and b, so it is a common divisor.

Second, we show that d is the greatest possible common divisor of a and b, which boils down to showing that if an integer e is a common divisor of a and b, then it is also a divisor of d. Since e divides both $a_0 = a$ and $b_0 = b$, it also divides $r_0 = b_0 - c_0 a_0$. Then, since e divides both $b_1 = a_0$ and $a_1 = r_0$, it also divides $r_1 = b_1 - c_1 a_1$; since e divides both $b_2 = a_1$ and $a_2 = r_1$, it also divides $r_2 = b_2 - c_2 a_2$; and so on. Tracking divisibility by e in this manner all the way through the process to $a_n = d$ tells us that e divides d.

Thus the integer d given by the process is the greatest common divisor of a and b.

Case 3. If $a > b$, a similar argument to the one in Case 2, with the roles of a and b reversed, shows that a and b have a greatest common divisor.

Since the three cases cover all the possibilities left open by the hypothesis that a and b are positive integers, they have a greatest common divisor. ■

---

* This process is called the Euclidean Algorithm nowadays. It appears in Euclid's *Elements*, which was written about 300 B.C.

3. Suppose that a and b are positive integers and $d = (a, b)$ is their greatest common divisor. Show that there exist integers x and y (which need not be positive) such that $ax + by = d$. *[3]*

Hint: Trace the argument you did for **2** backwards.

SOLUTION. Suppose a and b are positive integers and $d = (a, b)$ is their greatest common divisor. Consider the same three cases considered in the solution to **2** above:

Case 1. In this case $a = b$ and the greatest common divisor is $d = a = b$. Let $x = 1$ and $y = 0$, so $ax + by = a \cdot 1 + b \cdot 0 = a = d$, so there exist integers x and y as required.

Case 2. In this case $a < b$. By the uniqueness of the greatest common divisor of a and b, established in the solution to **2** above, running the process described in that solution for Case 2 will produce d. In fact, $d = a_n$ for some $n \geq 1$ where $b_n = c_n a_n$, but this means that $d = a_n = r_{n-1}$, where $b_{n-1} = c_{n-1}a_{n-1} + r_{n-1} = c_{n-1}a_{n-1} + d$, so $d = b_{n-1} - c_{n-1}a_{n-1}$. If $n - 1 = 0$, this would mean that $d = b_0 - c_0 a_0 = b - c_0 a$, so we could take $x = -c_0$ and $y = 1$ to get $ax + by = d$. On the other hand, if $n - 1 > 0$, we can use the facts that $a_{n-1} = r_{n-2}$, $b_{n-1} = a_{n-2}$, and $b_{n-2} = c_{n-2}a_{n-2} + r_{n-2}$ to write $a_{n-1} = r_{n-2} = b_{n-2} - c_{n-2}a_{n-2}$, and then plug this into $d = b_{n-1} - c_{n-1}a_{n-1}$ to get $d = a_{n-2} - c_{n-1}\left(b_{n-2} - c_{n-2}a_{n-2}\right) = -c_{n-1}b_{n-2} + \left(1 + c_{n-1}c_{n-2}a_{n-2}\right)a_{n-2}$. If $n-2 = 0$, then this boils down to having $x = 1 + c_1 c_0$ and $y = c_1$; if not one can proceed in a similar way, backtracking through the Euclidean algorithm, to eventually obtain the neccessary x and y.

Case 3. If $a > b$, a similar argument to the one in Case 2 above, with the roles of a and b reversed, shows that there exist integers x and y such that $ax + by = d$.

Since the three cases cover all the possibilities left open by the hypothesis that a and b are positive integers, they have a greatest common divisor. ■