Math 301 **Homework 2 – Solutions** **Fall 2014**

Chapter 2: 14, 22, 24, 25, 26, 28.
Due date: Friday, 9/12

14. Show that the Principle of Well-Ordering for the natural numbers implies that 1 is the smallest natural number. Use this result to show that the Principle of Well-Ordering implies the Principle of Mathematical Induction; that is, show that if $S \subset \mathbb{N}$ such that $1 \in S$ and $n+1 \in S$ whenever $n \in S$, then $S = \mathbb{N}$.

Solution: The first part of the problem asks us to apply the Well-Ordering Principle (WOP) to prove something, so immediately we know that the appropriate strategy is to find a nonempty subset F of the natural numbers. Of course, we don't just want to choose subsets of $\mathbb{N}$ at random and hopeful the best (although, that is a good way to get started if you can't think of anything else to do). Rather, we want to construct our subset $F \subseteq \mathbb{N}$ so that *knowing F is well-ordered will help us solve the problem.*

First we define the set of "good" natural numbers to be those that are greater or equal 1. Let $S = \{n \in \mathbb{N} : n \geq 1\}$. Our goal is to prove that all natural numbers are "good," that is, $S = \mathbb{N}$, since this will show that every natural number is greater or equal 1.

Let F be the set of "bad" natural numbers, that is, those numbers that Fail to belong to S. Thus,

$$F = \mathbb{N} - S = \{n \in N : n \ngeq 1\}.$$

Clearly $\mathbb{N}$ is the disjoint union of the sets S and F. We want to show that F is empty, so that $S = \mathbb{N}$. To do so, we will suppose F is not empty and reach a contradiction. If $F \neq \varnothing$, then by the WOP it has a least element. Let d be the least element of F. Then, $d-1$ does not belong to F, so it belongs to S. That is $d-1 \geq 1$. Therefore, $d \geq 1+1 \geq 1$, so $d \in S$, which contradicts $d \in F$. Therefore, $F = \varnothing$, so $S = \mathbb{N}$ which proves that 1 is the smallest natural number. □

The proof that WOP implies the Principle of Mathematical Induction was presented in class. (If you are confused by the proof, please come to office hours and ask about it.)

22. Let $n \in \mathbb{N}$. Use the division algorithm to prove that every integer is congruent mod n to precisely one of the integers $0, 1, \ldots, n-1$. Conclude that if r is an integer, then there is exactly one s in $\mathbb{Z}$ such that $0 \leq s < n$ and $[r] = [s]$. Hence, the integers are indeed partitioned by congruence mod n.

Solution: Fix an arbitrary natural number $r \in \mathbb{N}$. We must show that there exists $s \in \{0, 1, \ldots, n-1\}$ such that r is congruent to s modulo n, that is, $r \equiv s \pmod{n}$. This is equivalent to finding an $s \in \{0, 1, \ldots, n-1\}$ such that $r - s = kn$, for some $k \in \mathbb{Z}$.

By the division algorithm, there exists $k_0 \in \mathbb{Z}$ such that $r = k_0 n + s_0$ where $0 \leq s_0 < n$. Therefore, $r - s_0 = k_0 n$, which proves the first part of the claim. It follows that $r \in [s_0] = \{kn + s_0 : k \in \mathbb{Z}\}$. Since congruence classes are either disjoint or equal, we have $[r] = [s_0]$.

To prove that s_0 is the unique element of $\{0, 1, \ldots, n-1\}$ satisfying $[r] = [s_0]$, suppose s is an element of $\{0, 1, \ldots, n-1\}$ with $k_0 n + s_0 = r = kn + s$ for some $k \in \mathbb{Z}$. By the division algorithm, such a pair (k, s) is unique determined by r and n. Therefore, $k = k_0$ and $s = s_0$. □

N.B. The following exercise (Exercise 23) is not required. It is included here for you reference, since it defines *least common multiple.*

23. Define the *least common multiple* of two nonzero integers a and b, denoted by $\text{lcm}(a, b)$, to be the nonnegative integer m such that both a and b divide m, and if a and b divide any other integer n, then m also divides n. Prove that any two integers a and b have a unique least common multiple.

24. If $d = \gcd(a, b)$ and $m = \text{lcm}(a, b)$, prove that $dm = |ab|$.

Solution: We assume $a, b, d, m \in \mathbb{Z}$ with $d = \gcd(a, b)$ and $m = \text{lcm}(a, b)$. In particular, from the definitions of gcd and lcm, we have $d \geq 1$ and $m \geq 1$. Now, there exist $x, y, u, v \in \mathbb{Z}$ such that the following relations hold:

(i) $a = xd$, and $x < 0$ iff $a < 0$;
(ii) $b = yd$, and $y < 0$ iff $b < 0$;
(iii) $m = ua$, and $u < 0$ iff $a < 0$;
(iv) $m = vb$, and $v < 0$ iff $b < 0$.

Next, let's establish a couple of claims that we know (after some experimentation and a few failed proof attempts!) will come in handy later.

Claim 1: $gcd(x, y) = 1$

Proof. Let $gcd(x, y) = k$. Then $x = rk$ and $y = sk$ for some $r, s \in \mathbb{Z}$. Therefore, $a = xd = (rk)d = r(kd)$ and $b = yd = (sk)d = s(kd)$, so kd divides both a and b. Since $d = \gcd(a, b)$, we must have that kd divides d. Thus, $k = 1$. □

Claim 2: $gcd(u, v) = 1$

Proof. Let $gcd(u, v) = k$. Then $u = rk$ and $v = sk$ for some $r, s \in \mathbb{Z}$. Therefore, $m = au = a(rk)$ and $m = bv = b(sk)$, so $m/k = ar$ and $m/k = bs$. That is, m/k is a common multiple of a and b. Since $m = \text{lcm}(a, b)$, we must have that m divides m/k. Therefore, $k = 1$. □

Now, from (i) and (iii) we have $m = ua = uxd$. From (ii) and (iv) we have $m = vb = vyd$. Therefore, $uxd = m = vyd$, so

$$ux = vy \tag{1}$$

From (1), we also have $u = (v/x)y$. Consider the number v/x. From (1), Claim 1, and Exercise 27, it follows that x divides v. From (1), Claim 2, and Exercise 27, it follows that v divides x. Therefore, $v/x = \pm 1$.

Finally, since $u = (v/x)y$, we have

$$dm = dua = adu = ad(v/x)y = (v/x)ady = (v/x)ab.$$

It remains to show that $v/x = \text{sgn}(ab)$, the sign of ab, from which it will follow that $(v/x)ab = |ab|$. Indeed, we have $v/x = \pm 1$ and, from (i) and (iv) above, $x < 0$ iff $a < 0$ and $v < 0$ iff $b < 0$. □

25. Show that $\operatorname{lcm}(a, b) = ab$ if and only if $\gcd(a, b) = 1$.

Solution: This is false! Take, for example, $a = 2$ and $b = -3$. Then $\gcd(2, -3) = 1$ and $\operatorname{lcm}(2, -3) = 6 \neq -6$. (Recall, $\operatorname{lcm}(a, b)$ is defined to be the least *nonnegative* integer m such that both a and b divide m.) Instead, the problem should say, "Show that $\operatorname{lcm}(a, b) = |ab|$ if and only if $\gcd(a, b) = 1$." The proof of this corrected version follows immediately from the statement in Exercise 24, which we just proved above.

26. Prove that $\gcd(a, c) = \gcd(b, c) = 1$ if and only if $\gcd(ab, c) = 1$ for integers a, b, and c.

Solution: We first prove that $\gcd(ab, c) = 1$ implies $\gcd(a, c) = \gcd(b, c) = 1$. Assume $\gcd(ab, c) = 1$, and let $\gcd(a, c) = d$ and $\gcd(b, c) = d'$. Then d divides both a and c, so it divides both ab and c, so it divides $\gcd(ab, c) = 1$. Therefore, $d = 1$. Similarly, d' divides both b and c, so it divides both ab and c, so it divides $\gcd(ab, c) = 1$. Therefore, $d' = 1$. Thus, we have proved $\gcd(ab, c) = 1$ implies $\gcd(a, c) = \gcd(b, c) = 1$.

To complete the proof, we must show $\gcd(a, c) = \gcd(b, c) = 1$ implies $\gcd(ab, c) = 1$. Let $d = \gcd(ab, c)$. Then d divides ab and d divides c. Therefore, $\gcd(a, d)$ divides both a and c, so $\gcd(a, d) = 1$. Finally, we have d divides ab and $\gcd(a, d) = 1$, so Exercise 27 implies that d must divide b. But then d divides both c and b, so divides $\gcd(b, c) = 1$. Therefore, $d = 1$.

N.B. The following exercise (Exercise 27) is not required. It is included here for you reference, since it may be useful when solving 24 or 26 (depending on the proof strategy you use). You may use the result stated in Exercise 27, even if you have not yet proved it.

27. Let $a, b, c \in \mathbb{Z}$. Prove that if $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

28. Let $p \geq 2$. Prove that if $2^p - 1$ is prime, then p must also be prime.

Solution: We will prove the (equivalent) contrapositive statement: if p is not prime, then $2^p - 1$ is not prime. Indeed, let $p = uv$ for some integers $u \geq 2$ and $v \geq 2$. Recall the following easily verified fact: for any real numbers a, b, and any integer $n > 0$,

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + ab^{n-2} + b^{n-1}).$$

(You can easily check this identity by multiplying out the right-hand side and noting that all terms are canceled in the resulting "telescoping sum" except for a^n and $-b^n$.)

Now, let us apply this identity with $a = 2^u$, $b = 1$, and $n = v$, as follows:

$$\begin{aligned} 2^p - 1 &= 2^{uv} - 1 \\ &= (2^u)^v - 1 \\ &= (2^u)^v - 1^v \\ &= (2^u - 1)(2^{v-1} + 2^{v-2} + 2^{v-3} + \cdots + 2 + 1). \end{aligned} \tag{2}$$

Since $u \geq 2$, we have $2^u - 1 > 1$, so Equation (2) presents $2^p - 1$ as a composite number. Thus, $2^p - 1$ is not prime. □

Optional Programming Exercise. If you wish to earn a bit of extra credit, you are encouraged to try the following:

(1) (1/4) Sign up for a Sage account at [sagemath.org](http://www.sagemath.org).
(2) (1/4) Create a new project named ”Math 301” and then create a Sage Worksheet within that project. Name your worksheet ”Eratosthenes” or ”Ackermann” or ”DivisionAlgorithm” (depending on which problem you plan to solve in the next part).
(3) (1/2) In the worksheet you created above, solve one of the three programming exercises described on page 31 of our textbook. These are also included below for your reference.

To get credit for this assignment, when you have finished, you must either send me your .sagews file by email, or invite me to be a collaborator on your Math 301 project. You must also email me a few sentences describing your experience and your first impressions of Sage.

More notes on Sage Assignment 1

The number in parentheses indicates the fraction of the percentage point that each part is worth.

The following are some notes about each part of the assignment:

(1) Go to cloud.sagemath.org.
(2) First create a new project by clicking the link that says ”New Project.” Name the project ”Math 301,” then click the Math 301 link that appears. Wait for your new project to load, then either click ”New” or ”Create or Import a File, Worksheet...” In the box where it says, ”Name your file,” enter the name ”Eratosthenes” or ”Ackermann” or ”DivisionAlgorithm” (depending on which problem you plan to solve in the next part). Then, where it says ”Select the type,” choose ”Sage Worksheet.”
(3) You are to solve one of the three problems described on [page 35 of our textbook](https://github.com/willia
Fall2014/blob/master/homework/pdf/SageAssignment1.pdf).

There is plenty of online documentation for Sage. If you need help, please ask! Also, you can find some nice examples of Sage programs that are specifically related to our course at http://abstract.ups.edu/sage-aata.html.

Programming Exercises.

(1) **The Sieve of Eratosthenes.** One method of computing all of the prime numbers less than a certain fixed positive integer N is to list all of the numbers n such that $1 < n < N$. Begin by eliminating all of the multiples of 2. Next eliminate all of the multiples of 3. Now eliminate all of the multiples of 5. Notice that 4 has already been crossed out. Continue in this manner, noticing that we do not have to go all the way to N; it suffices to stop at $\sqrt{N}$. Using this method, compute all of the prime numbers less than $N = 250$. We can also use this method to find all of the integers that are relatively prime to an integer N. Simply eliminate the prime factors of N and all of their multiples. Using this method, find all of the numbers that are relatively prime to $N = 120$. Using the Sieve of Eratosthenes, write a program that will compute all of the primes less than an integer N.

(2) Let $\mathbb{N}^0 = \mathbb{N} \cup \{0\}$. Ackermann's function is the function $A : \mathbb{N}^0 \times \mathbb{N}^0 \to \mathbb{N}^0$ defined by the equations

$$\begin{aligned} A(0, y) &= y + 1, \\ A(x + 1, 0) &= A(x, 1), \\ A(x + 1, y + 1) &= A(x, A(x + 1, y)). \end{aligned}$$

Use this definition to compute $A(3, 1)$. Write a program to evaluate Ackermann's function. Modify the program to count the number of statements executed in the program when Ackermann's function is evaluated. How many statements are executed in the evaluation of $A(4, 1)$? What about $A(5, 1)$?

(3) Write a computer program that will implement the Euclidean algorithm. The program should accept two positive integers a and b as input and should output $\gcd(a, b)$ as well as integers r and s such that

$$\gcd(a, b) = ra + sb.$$