Math 110 Homework 1 Solutions

January 15, 2015

1. (a) Define the phrase m *divides* n.
   (b) Given integers m and n, state the definition of the *greatest common divisor* of m and n.
   (c) Suppose that m and n are two integers such that $m \mid n$. Find $\gcd(m, n)$, and prove your solution.

   Solution: (a) The integer m divides n if there exists an integer r such that $n = mr$.

   (b) The greatest common divisor is the largest positive integer d which divides both m and n. This means that (i) $d \mid m$ and $d \mid n$, and (ii) for any integer c such that $c \mid m$ and $c \mid n$, we have $d \geq c$.

   (c) The greatest common divisor is $|m|$. For suppose a positive integer a divided m. Then by definition there exists an integer r such that $m = ra$. By hypothesis that $m|n$, there also exists an integer s such that $ms = n$. Then

   $$n = ms = (ra)s = (rs)a$$

   which is the definition of $a|n$. Therefore, any divisor of m is automatically a divisor of n. Hence the greatest positive integer which divides both m and n is the largest positive integer which divides m, which is $|m|$.

2. (a) Find the greatest common divisor of 1064 and 856.
   (b) Find integers x and y so that $1064x + 856y = \gcd(1064, 856)$.

   Solution: (a) Use the Euclidean algorithm:

   $$\begin{aligned} 1064 &= 856 \cdot 1 + 208 \\ 856 &= 208 \cdot 4 + 24 \\ 208 &= 24 \cdot 8 + 16 \\ 24 &= 16 \cdot 1 + 8 \\ 16 &= 8 \cdot 2 + 0 \end{aligned}$$

   Therefore the greatest common divisor is 8.

   (b) Now substitute:

   $$\begin{aligned} 8 &= 24 - 16 \\ &= 24 - (208 - 24 \cdot 8) \\ &= -208 + 24 \cdot 9 \\ &= -208 + (856 - 208 \cdot 4) \cdot 9 \\ &= 856 \cdot 9 - 208 \cdot 37 \\ &= 856 \cdot 9 - (1064 - 856) \cdot 37 \\ &= -37 \cdot 1064 + 46 \cdot 856 \end{aligned}$$

   Therefore one solution is to take $x = -37$ and $y = 46$.

3. Complete our proof that the Euclidean algorithm computes the gcd, by showing for $a, b, q, r \in \mathbb{Z}$ with $a = bq + r$ then $\gcd(a, b) = \gcd(b, r)$.
Hint: Show that any common divisor of a and b is also a common divisor of b and r, and vice versa. If the set of common divisors of a and b is the same as the set of common divisors of b and r, then both must have the same greatest common divisor.

Solution: As the hint suggests, we will show that the set of common divisors for a and b is the same as the set of common divisors of b and r.

Suppose that an integer n divides both a and b. The hypothesis n divides a and b implies there are integers s and t such that $a = ns$ and $b = nt$. Then

$$r = a - bq = ns - ntq = n(s - tq).$$

Therefore $n|r$.

Suppose that n divides b and r. Then there are s and t with $b = sn$ and $r = tn$. Substituting

$$a = bq + r = snq + tn = n(sq + t)$$

which means that n divides a.

4. Prove that if $a \in \mathbb{Z}$ such that $a > 1$, then a factors as a product of positive primes, and this factorization is unique up to the order of the factors.
Hint: This result is proven on page 65 of the textbook. You're welcome to read this proof, but be sure to write up your solution in your own words. Remember that we have already proved in class the following result: If p is prime and p divides a product of integers ab, then $p \mid a$ or $p \mid b$.

Solution: See the proof on page 65.

5. In this problem, we will give a classical proof of the infinitude of primes.
   (a) Prove that for any $n \in \mathbb{Z}$, $\gcd(n, n + 1) = 1$. Conclude that if a prime p divides n, then p cannot divide $n + 1$.
   (b) Write a proof that there are infinitely many prime numbers, as follows. Assume that there were only finitely many primes $p_1, p_2, \ldots, p_N$. Consider the number $(p_1 p_2 \cdots p_N + 1)$, and use Part (a) to reach a contradiction.

Solution: (a) Let n be an integer. Suppose $a \mid n$ and $a \mid (n + 1)$. Then $as = n$ and $at = n + 1$ for some $s, t \in \mathbb{Z}$. But $1 = (n + 1) - n = at - as = a(t - s)$ therefore a divides 1. Therefore the only common divisors of n and $n + 1$ are 1 and -1. In particular, a prime cannot divide both n and $n + 1$.

(b) Now suppose there are only finitely many primes $p_1, p_2, \ldots, p_N$. The number $M = (p_1 p_2 \cdots p_N + 1)$ must have a prime factor, which will be one of the primes listed, say p_i. But then we would have $p_i|M$ and $p_i|p_1 p_2 \cdots p_N$, contradicting the first part of this question. Therefore the assumption there are finitely many primes is incorrect.

6. Given integers a, b, for what integers d does the equation $ax + by = d$ have integer solutions (x, y)? Justify your answer.

Solution: The equation has a solution if and only d is a multiple of the greatest common divisor of a and b.

Suppose the equation had a solution (x, y). Then if $n|a$ and $n|b$, n divides $ax + by = d$. In particular, taking n to be $\gcd(a, b)$, n must divide d.

Conversly, suppose d is a multiple of $\gcd(a, b)$, say $d = r \gcd(a, b)$ The extended Euclidean algorithm produces x' and y' such that

$$ax' + by' = \gcd(a, b).$$

Multipyling this expression by r, we see

$$a(x'r) + b(y'r) = \gcd(a,b)r = d.$$

7. (a) We saw in class that $\gcd(28, 80) = 4$, and that the equation $80u + 28v = 4$ has solution $u = -1$ and $v = 3$. There are, however, other solutions (u, v). Describe the set of all integer solutions to $80u + 28v = 4$. *Hint:* If we increase or decrease $u = -1$ by adding a multiple of $\frac{28}{4} = 7$, what can we do to $v = 3$ to compensate?

   (b) We proved that if $a, b \in \mathbb{Z}$ and $\gcd(a, b) = d$, then there exists a solution $u, v \in \mathbb{Z}$ to $au + bv = d$. Assuming $u = u_o$ and $v = v_o$ is one solution, describe the set of all integer solutions (u, v).

Solution: (a) Because $80 \cdot 7 - 28 \cdot 20 = 0$, if we add 7 to u we can decrease v by 20 to leave the entire sum unchanged. This suggests the set of all solutions will be $\{(-1 + 7t, 3 - 20t) : t \in \mathbb{Z}\}$. We will prove this in general in the second part.

(b) We show that $\{(u_0 + t\frac{b}{d}, v_0 - t\frac{a}{d}) : t \in \mathbb{Z}\}$ is the set of all solutions to $au + bv = d$.

To prove this, observe that

$$a\left(u_0 + t\frac{b}{d}\right) + b\left(v_0 - t\frac{a}{d}\right) = au_0 + bv_0 + t\frac{ab}{d} - t\frac{ab}{d} = d.$$

So all of these are solutions.

Now let (u, v) be any solution. Then

$$\begin{aligned} 0 &= (au + bv) - (au_0 + bv_0) \\ 0 &= a(u - u_0) + b(v - v_0) \\ a(u - u_0) &= -b(v - v_0) \\ \frac{a}{d}(u - u_0) &= -\frac{b}{d}(v - v_0) \end{aligned}$$

The integer $\frac{a}{d}$ divides the right-hand side of the equation, but it is relatively prime to $\frac{b}{d}$ (this was proven on the quiz). Hence $\frac{a}{d}$ it must divide $(v - v_0)$. There is therefore an integer t such that $(v - v_0) = t\frac{a}{d}$. Substituting shows that $u - u_0 = -t\frac{b}{d}$. Therefore all solutions are of the desired form.

8. (a) Let $a, n \in \mathbb{Z}$, $n > 0$. Define the *congruence class of a modulo n*, and describe the set $\mathbb{Z}/n\mathbb{Z}$.

   (b) Explain in your own words what it means to say that "addition and multiplication of congruence classes modulo n are well-defined".

   (c) If $a \equiv b \pmod{n}$ and $k \mid n$, must $a \equiv b \pmod{k}$? Justify your answer.

Solution: (a) The congruence class is the set of all integers which have the same remainder as a when divided by n. Equivalently, it is

$$\{b \in \mathbb{Z} : n|(a - b)\} = \{a + kn : k \in \mathbb{Z}\}$$

By definition, $\mathbb{Z}/n\mathbb{Z}$ is the set of all such congruence classes. There is an equivalence class for each integer from 0 to $n - 1$.

(b) There is an obvious way to add congruence classes: pick an element from each (called a representative), and add them or multiply them. These operations are well defined if the congruence class of the result does not depend on which element was chosen.

(c) The condition $a \equiv b \pmod{n}$ means that $n|(a - b)$. If $k|n$, then $k|(a - b)$ as well, so $a \equiv b \pmod{k}$.

9. Prove that a has a multiplicative inverse (mod n) if and only if $\gcd(a, n) = 1$.

Solution: Suppose that a has a multiplicative inverse (mod n): there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{n}$. Let $d = \gcd(a, n)$. Then by 8(c) as $d|n$ we have $ab \equiv 1 \pmod{d}$. But this means $d \mid (ab - 1)$, while also $d \mid a \mid ab$. Therefore $d = 1$ by 5(a).

Conversely, if $\gcd(a, n) = 1$ there is an integer solution (x, y) such that

$$ax + ny = 1.$$

Reducing this equation modulo n, we see

$$ax \equiv 1 \pmod{n}.$$

10. Find a multiplicative inverse for 27 (mod 80).

Solution: Use the extended Euclidean algorithm to solve $27x + 80y = 1$ as in problem 2. It gives $x = 3, y = -1$ as a solution. Therefore 3 (mod 80) is a multiplicative inverse.

11. **(Optional – Challenge Question)** Prove that if p is prime, then for any $a, b, n \in \mathbb{Z}$ with $n > 0$,

$$(a + b)^{p^n} \equiv a^{p^n} + b^{p^n} \pmod{p}.$$

This result is affectionately known as "The Freshman's Dream".

Solution: We first prove this for $n = 1$ using the binomial theorem. Write

$$(a + b)^p = a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \ldots + b^p$$

However, for $1 \leq m \leq p - 1$, $\binom{p}{m}$ is a multiple of p. To see this, use the definition $\binom{p}{m} = \frac{(p)!}{m!(p-m)!}$ and note p cannot divide $m!$ or $(p - m)!$ as all terms in these products are less than p. Therefore all of the terms except the first and last are zero modulo p, so

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

For general n, use induction (ie $(a + b)^{p^2} \equiv (a^p + b^p)^p \equiv a^{p^2} + b^{p^2} \pmod{p}$).

12. **(Optional – Challenge Question)** Let $p(x)$ be a polynomial with integer coefficients. A real number z is a *root* of p if $p(z) = 0$. A congruence class $[a]$ modulo n is a *root* of p if $p(a) \equiv 0 \pmod{n}$. A polynomial $p(x)$ of degree d has at most d distinct real roots.
    (a) Find a composite number n and a degree d polynomial $p(x)$ with integer coefficients such that more than d distinct congruence classes modulo n are roots of $p(x)$.
    (b) Prove that if $q \in \mathbb{Z}$ is prime, and $p(x)$ is a degree d polynomial with integer coefficients, then at most d congruence classes modulo q are roots of $p(x)$. (This question is tricky!)

Solution: Take $n = 6$ and $p(x) = (x - 2)(x - 3)$. Then $x = 2, 3$ are obvious solutions, but $x = 0, 5$ are also solutions. This has do with the fact that 2 is a zero divisor: $2 \cdot 3 \equiv 0 \pmod{6}$.

The second part is an important fact written up in many books on abstract algebra. See for example Proposition 17 of Chapter 9 of Dummit and Foote.

13. **(Optional – Challenge Question)** Let $\mathbb{Q}[x]$ denote the set of polynomials $f(x)$ with rational coefficients. The goal of this question is to adapt our theory of divisibility to polynomials. Note that a polynomial is called *monic* if its leading coefficient is 1.

(a) What should it mean for a polynomial $f(x)$ to *divide* a polynomial $g(x)$? Define the greatest common denominator of $f(x)$ and $g(x)$. (This should be a monic polynomial that is "greatest" in the sense of having highest degree). What is the analogue of a prime number?

(b) Prove that if $f(x)$, $g(x)$ are nonzero polynomials in $\mathbb{Q}[x]$, then there are polynomials $u(x)$ and $v(x)$ such that $f(x)u(x) + g(x)v(x) = \gcd(f(x), g(x))$. You can adapt our proof from class of the analogous statement for integers, replacing integer inequalities with inequalities involving the polynomials' degrees.

Solution: This is a standard fact written up in many books on abstract algebra. See for example Theorem 3 of Chapter 9 of Dummit and Foote (which uses 8.1 extensively).

14. **(Optional – Challenge Question)** The Euclidean algorithm also adapts to computing the gcd of polynomials in $\mathbb{Q}[x]$.

(a) Use the Euclidean algorithm and polynomial division to find the gcd $d(x)$ of $(x^5 - x^3 - x^2 + 1)$ and $(x^3 - 2x^2 - x + 2)$.

(b) Find polynomials $u(x)$ and $v(x)$ so that

$$(x^5 - x^3 - x^2 + 1)u(x) + (x^3 - 2x^2 - x + 2)v(x) = d(x).$$

Solution: (a) We divide:

$$x^5 - x^3 - x^2 + 1 = (x^2 + 2x + 4) \cdot (x^3 - 2x^2 - x + 2) + 7x^2 - 7$$
$$x^3 - 2x^2 - x + 2 = (7x^2 - 7)\frac{1}{7}(x - 2).$$

Therefore $x^2 - 1$ is the greatest common divisor.

(b) Rearranging the first equation gives

$$x^2 - 1 = \frac{1}{7} \cdot (x^5 - x^3 - x^2 + 1) - \frac{1}{7}(x^2 + 2x + 4) \cdot (x^3 - 2x^2 - x + 2)$$