Problem Set 3 Solutions

Due: Monday, September 27 at 9pm

Problem 1. [25 points] Prove the following assertions:

(a) For all \( c \neq 0, \ a \mid b \) if and only if \( ca \mid cb \).

Solution. The assertion \( a \mid b \) holds if and only if there exists an integer \( k \) such that \( ak = b \). For \( c \neq 0 \), this is true if and only if there exists an integer \( k \) such that \( cak = cb \). And this holds if and only if \( ca \mid cb \).

(b) Every common divisor of \( a \) and \( b \) divides \( \gcd(a, b) \).

Solution. In lecture, we showed that \( \gcd(a, b) = sa + tb \) for some integers \( s \) and \( t \). Let \( m \) be any other common divisor of \( a \) and \( b \). Then \( mx = a \) and \( my = b \) for some integers \( x \) and \( y \). Thus \( \gcd(a, b) = s(mx) + t(my) = m(sx + ty) \), proving that \( m \mid \gcd(a, b) \).

(c) \( \gcd(ka, kb) = k \cdot \gcd(a, b) \) for all integers \( k > 0 \).

Solution. In lecture, we showed that \( \gcd(a, b) \) is the minimum positive value of \( s \cdot a + t \cdot b \) over all \( s, t \in \mathbb{Z} \). Thus, \( k \cdot \gcd(a, b) \) is the minimum positive value of \( k(s \cdot a + t \cdot b) = s \cdot ka + t \cdot kb \), which is equal to \( \gcd(ka, kb) \).

(d) \( \gcd(a \rem b, b) = \gcd(a, b) \) (Hint: Prove the more general fact that \( \gcd(a - q \cdot b, b) = \gcd(a, b) \) for all integers \( q \).)

Solution. Recall that \( a \rem b = a - qb \) for some integer \( q \). We’ll show more generally that \( \gcd(a - qb, b) = \gcd(a, b) \) for all integers \( q \). On one hand, \( \gcd(a, b) \) is the smallest positive value of:

\[ s \cdot a + t \cdot b \]

On the other hand, \( \gcd(a - qb, b) \) is the smallest positive value of:

\[ x \cdot (a - qb) + y \cdot b = x \cdot a + (y - qx) \cdot b \]

These two expressions take on exactly the same set of values, since we can let \( s = x \) and \( t = y - qx \). Thus, in particular, the expressions have the same smallest positive value, and so \( \gcd(a - qb, b) = \gcd(a, b) \) as claimed.
(e) \( nx \ \text{rem} \ dx = (n \ \text{rem} \ d) \cdot x \) when \( x \in \mathbb{N}^+ \).

**Solution.** By the definition of \( \text{rem} \) and the Division Algorithm, \( n \ \text{rem} \ d \) is the unique integer \( r \) satisfying \( n = qd + r \) and \( 0 \leq r < d \). Now if we set \( q' = q \) and \( r' = rx \), then \( nx = q'(dx) + r' \) and \( 0 \leq r' < dx \). Thus, \( r' = rx = (n \ \text{rem} \ d) \cdot x \) is \( nx \ \text{rem} \ dx \).

**Problem 2.** [20 points] Use induction to prove the following statements, which were left unproved in lecture.

(a) \((a_1 \ \text{rem} \ n) \cdot (a_2 \ \text{rem} \ n) \cdots (a_k \ \text{rem} \ n) \equiv a_1 \cdot a_2 \cdots a_k \pmod{n}\)

You may use the following two facts, which were proved in lecture:

1. If \( a_1 \equiv b_1 \pmod{n} \) and \( a_2 \equiv b_2 \pmod{n} \), then \( a_1a_2 \equiv b_1b_2 \pmod{n} \).
2. \((a \ \text{rem} \ n) \equiv a \pmod{n}\)

**Solution.** We proceed by induction on \( k \) with the claim itself as the induction hypothesis.

*Base case:* The claim holds for \( k = 1 \) by the second fact provided above.

*Inductive step:* Now we assume that the claim holds for some \( k \geq 1 \) and prove that the claim holds for \( k + 1 \). Consider the expression:

\[(a_1 \ \text{rem} \ n) \cdot (a_2 \ \text{rem} \ n) \cdots (a_k \ \text{rem} \ n) \cdot (a_{k+1} \ \text{rem} \ n)\]

By the induction assumption, the first \( n \) terms are congruent to \( a_1 \cdot a_2 \cdots a_k \pmod{n} \). By the second fact from above, \((a_{k+1} \ \text{rem} \ n)\) is congruent to \( a_{k+1} \pmod{n} \). Thus, by the first fact above, the whole product is congruent to

\[a_1 \cdot a_2 \cdots a_k \cdot a_{k+1}\]

modulo \( n \). Thus, the claim holds for \( k + 1 \).

By the principle of induction, the claim holds for all \( k \geq 1 \).

(b) Let \( p \) be a prime. If \( p \mid a_1 \cdot a_2 \cdots a_n \), then \( p \) divides some \( a_i \).

You may use the fact, proved in lecture, that if \( p \) is a prime and \( p \mid ab \), then \( p \mid a \) or \( p \mid b \).

**Solution.** We proceed by induction on \( n \) with the claim itself as the induction hypothesis.

*Base case:* When \( n = 1 \), the claim asserts that if \( p \mid a_1 \), then \( p \mid a_1 \), which is trivially true.

*Inductive step:* Now we assume that the claim holds for some \( n \geq 1 \) and prove that it holds for \( n + 1 \). Suppose that

\[p \mid a_1 \cdot a_2 \cdots a_n \cdot a_{n+1}\]
Problem 3. [15 points] Prove that the greatest common divisor of three integers \(a, b,\) and \(c\) is equal to their smallest positive linear combination; that is, the smallest positive value of \(sa + tb + uc\), where \(s, t,\) and \(u\) are integers.

Solution. This is nearly a verbatim repetition of the proof for two integers, which appears in the notes.

Let \(m\) be the smallest positive linear combination of \(a, b,\) and \(c\). We’ll prove that \(m = \text{gcd}(a, b, c)\) by showing both \(\text{gcd}(a, b, c) \leq m\) and \(m \leq \text{gcd}(a, b, c)\).

First, we show that \(\text{gcd}(a, b, c) \leq m\). By the definition of common divisor, \(\text{gcd}(a, b, c)\) divides \(a, b,\) and \(c\). Therefore, for every triple of integers \(s, t,\) and \(u\):

\[
\text{gcd}(a, b) \mid sa + tb + uc
\]

Thus, in particular, \(\text{gcd}(a, b, c)\) divides \(m\), and so \(\text{gcd}(a, b, c) \leq m\).

Now we show that \(m \leq \text{gcd}(a, b, c)\). We do this by showing that \(m \mid a\). Symmetric arguments shows that \(m \mid b\) and \(m \mid c\), which means that \(m\) is a common divisor of \(a, b,\) and \(c\). Thus, \(m\) must be less than or equal to the greatest common divisor of \(a, b,\) and \(c\).

All that remains is to show that \(m \mid a\). By the division algorithm, there exists a quotient \(q\) and remainder \(r\) such that:

\[
a = q \cdot m + r \quad \text{(where } 0 \leq r < m)\]

Now \(m = sa + tb + uc\) for some integers \(s\) and \(t\). Substituting in for \(m\) and rearranging terms gives:

\[
a = q \cdot (sa + tb + uc) + r
\]

\[
r = (1 - qs)a + (-qt)b + (-qu)c
\]

We’ve just expressed \(r\) as a linear combination of \(a, b,\) and \(c\). However, \(m\) is the smallest positive linear combination and \(0 \leq r < m\). The only possibility is that the remainder \(r\) is not positive; that is, \(r = 0\). This implies \(m \mid a\).

Problem 4. [10 points] Let \(S_k = 1^k + 2^k + \ldots + (p - 1)^k\), where \(p\) is an odd prime and \(k\) is a positive multiple of \(p - 1\). Use Fermat’s theorem to prove that \(S_k \equiv -1 \pmod{p}\).

Solution. Fermat’s theorem says that \(x^{p-1} \equiv 1 \pmod{p}\) when \(1 \leq x \leq p - 1\). Since \(k\) is a multiple of \(p - 1\), raising each side to a suitable power proves that \(x^k \equiv 1 \pmod{p}\).
Thus:

\[1^k + 2^k + \ldots + (p - 1)^k \equiv 1 + 1 + \ldots + 1 \pmod{p} \]
\[\equiv p - 1 \pmod{p} \]
\[\equiv -1 \pmod{p} \]

**Problem 5.** [10 points] Let \(N\) be a number whose decimal expansion consists of \(3^n\) identical digits. Show by induction that \(3^n \mid N\). For example:

\[3^2 \mid \underbrace{777777777}_{3^2 = 9 \text{ digits}}\]

**Solution.** We proceed by induction on \(n\). Let \(P(n)\) be the proposition that \(3^n \mid N\), where the decimal expansion of \(N\) consists of \(3^n\) identical digits.

**Base case.** \(P(0)\) is true because \(3^0 = 1\) divides every number.

**Inductive step.** Now assume \(P(n)\) for \(n \geq 0\) in order to prove \(P(n + 1)\). Consider a number whose decimal expansion consists of \(3^{n+1}\) copies of the digit \(a\):

\[
\underbrace{aaa\ldots aaa}_{3^{n+1} \text{ digits}} = \underbrace{aaa}_{3^n \text{ digits}} \ldots \underbrace{aaa}_{3^n \text{ digits}} \cdot \underbrace{1000\ldots 001}_{3^n \text{ digits}} \ldots \underbrace{001}_{3^n \text{ digits}}
\]

Now \(3^n\) divides the first term by the assumption \(P(n)\), and 3 divides the second term since the digits sum to 3. Therefore, the whole expression is divisible by \(3^{n+1}\). This proves \(P(n + 1)\).

By the principle of induction \(P(n)\) is true for all \(n \geq 0\).

**Problem 6.** [20 points] Suppose that you have an \(a\)-gallon bucket and a \(b\)-gallon bucket where \(a \leq b\). You also have access to a fountain. In lecture, we proved that you can measure out only multiples of \(\gcd(a, b)\) gallons. The goal of this problem is to prove the converse: you can measure out exactly \(n\) gallons in one bucket provided \(n\) is a multiple of \(\gcd(a, b)\) and \(0 \leq n \leq b\).

Getting exactly \(b\) gallons is easy: fill the \(b\)-gallon bucket. For all other quantities, consider the following procedure:

1. Fill the \(a\)-gallon bucket.

2. Pour the entire contents of the \(a\)-gallon bucket into the \(b\)-gallon bucket, dumping out the \(b\)-gallon bucket whenever it becomes full.
(a) Give a concise expression for the amount of water in the \( b \)-gallon bucket after \( k \) repetitions of this procedure.

Solution. \( ka \ rem \ b \)

(b) Suppose that \( a \) and \( b \) are relatively prime. Show that this expression never takes on the same value twice as \( k \) ranges over the set \( \{0, 1, 2, \ldots, b - 1\} \).

Solution. Assume for the purpose of contradiction that \( k_1 a \ rem \ b = k_2 a \ rem \ b \) for some \( k_1 \neq k_2 \) in the range \( 0 \leq k_1, k_2 < b \). This means \( k_1 a \equiv k_2 a \mod b \), which implies that \( k_1 \equiv k_2 \mod b \) since \( a \) and \( b \) are relatively prime. Since no two values in \( \{0, 1, 2, \ldots, b - 1\} \) are congruent modulo \( b \), we must have \( k_1 = k_2 \), which is a contradiction.

(c) Show that the expression in part (a) takes on all values in \( \{0, 1, 2, \ldots, b - 1\} \) as \( k \) ranges over the set \( \{0, 1, 2, \ldots, b - 1\} \). In other words, every number of gallons between 0 and \( b - 1 \) is obtained within \( b - 1 \) repetitions of the procedure.

Solution. The expression takes on \( b \) values in the range \( \{0, 1, 2, \ldots, b - 1\} \) by the definition of remainder, and these values are all distinct by the preceding problem part. Thus, it must take on every value in the range exactly once.

(d) Now suppose \( a \) and \( b \) are not relatively prime. Prove that the values this expression takes on are exactly the nonnegative multiples of \( \gcd(a, b) \) less than \( b \).

You may find it helpful to isolate the common and relatively prime parts of \( a \) and \( b \). Specifically, define \( a' \) and \( b' \) so that \( a = a' \gcd(a, b) \) and \( b = b' \gcd(a, b) \). Note that \( a' \) and \( b' \) are relatively prime; otherwise, \( a \) and \( b \) would have a greater common divisor.

Solution. Consider the sequence:

\[
0 \ a \rem b, \quad 1 \ a \rem b, \quad 2 \ a \rem b, \quad \ldots, \quad (b' - 1) \ a \rem b
\]

We can rewrite each term as follows:

\[
ka \ rem \ b = k[a' \gcd(a, b)] \ rem [b' \gcd(a, b)] = \gcd(a, b) \cdot (ka' \ rem b')
\]

The first step is substitution and the second uses part (e) of problem 1. Thus, each term in the sequence above is \( \gcd(a, b) \) times the corresponding term in the sequence below:

\[
0 \ a' \rem b', \quad 1 \ a' \rem b', \quad 2 \ a' \rem b', \quad \ldots, \quad (b' - 1) \ a' \rem b'
\]

By the preceding problem part, this is a permutation of \( 0, 1, 2, \ldots, b' - 1 \). Thus, the original sequence is a permutation of:

\[
0 \cdot \gcd(a, b), \quad 1 \cdot \gcd(a, b), \quad 2 \cdot \gcd(a, b), \quad \ldots, \quad (b' - 1) \cdot \gcd(a, b)
\]

And these are the nonnegative multiple of \( \gcd(a, b) \) less than \( b \).