Problem Set 3 Solutions

Due: Monday, September 25 at 8pm

Problem 1. [15 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) $\gcd(\text{rem}(a, b), b) = \gcd(a, b)$ (Hint: Prove the more general fact that $\gcd(a - q \cdot b, b) = \gcd(a, b)$ for all integers $q$.)
   
   Solution. Recall that $\text{rem}(a, b) = a - qb$ 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) \( \text{rem} (nx, dx) = (\text{rem} (n, d)) \cdot x \) when \( x \in \mathbb{N}^+ \).

**Solution.** By the definition of \( \text{rem} \) and the Division Algorithm, \( \text{rem} (n, d) \) 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, \( r' = rx = (\text{rem} (n, d)) \cdot x \) is \( \text{rem} (nx, dx) \).

**Problem 2.** [10 points] Use induction to prove the following statements.

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

You may use the following two facts:

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. \( (\text{rem} (a, n)) \equiv a \pmod{n} \)

**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:

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

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, \( \text{rem} (a_{k+1}, n) \) 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 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

\[
p \mid a_1 \cdot a_2 \cdots a_n \cdot a_{n+1}
\]
By grouping the first \( n \) terms on the right and using the fact cited above, we know that either \( p \mid (a_1 \cdot a_2 \cdots a_n) \) or \( p \mid a_{n+1} \). If the former case, the induction assumption implies that \( p \) divides some some \( a_i \) with \( 1 \leq i \leq n \). Thus, in both cases, \( p \) divides some \( a_i \) as claimed.

By induction, the claim holds for all \( n \geq 1 \).

**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 \( m = \gcd(a, b, c) \) by showing both \( \gcd(a, b, c) \leq m \) and \( m \leq \gcd(a, b, c) \).

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

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

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

Now we show that \( m \leq \gcd(a, b, c) \). 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:

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

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:
\[
1^k + 2^k + \ldots + (p-1)^k \equiv \underbrace{1+1+\ldots+1}_{p-1 \text{ terms}} \pmod{p} \\
\equiv p - 1 \pmod{p} \\
\equiv -1 \pmod{p}
\]

**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:

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

**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 \(a\):

\[
\underbrace{aaaaa \ldots aaaaa}_{3^{n+1} \text{ digits}} = \underbrace{aaa \ldots aag aaaa \ldots aag aaaa \ldots aag}_{3^n \text{ digits} \ 3^n \text{ digits} \ 3^n \text{ digits}} \\
= \underbrace{aaa \ldots aag}_{3^n \text{ digits}} \cdot \underbrace{1000 \ldots 001 000 \ldots 001}_{3^n \text{ digits} \ 3^n \text{ digits}}
\]

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.** \( \text{rem} \ (ka, b) \)

(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 \( \text{rem} \ (k_1a, b) = \text{rem} \ (k_2a, b) \) for some \( k_1 \neq k_2 \) in the range \( 0 \leq k_1, k_2 < b \). This means \( k_1a \equiv k_2a \pmod{b} \), which implies that \( k_1 \equiv k_2 \pmod{b} \) 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:

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

We can rewrite each term as follows:

\[
\text{rem} \ (ka, b) = \text{rem} \ (k[a' \gcd(a, b)], [b' \gcd(a, b)])
\]

\[
= \gcd(a, b) \cdot (\text{rem} \ (ka', b'))
\]

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:

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

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 \( b \).
Problem 7. [20 points] In class and recitation, we will study the RSA cryptosystem. However, we will not be able to give any evidence that it is hard to break the RSA cryptosystem other than proof by reference to eminent authority – i.e., Rivest, Shamir and Adleman as well as a lot of other very smart people over the last few decades were not able to break it. This explains why cryptographers don’t sleep very well.

Here we want to use a cryptosystem, called the Rabin cryptosystem, that has slightly better security justification than RSA. That is, if someone has the ability to break this cryptosystem efficiently, then one also has the ability to factor numbers that are products of two primes. Why should that convince us that it is hard to break the cryptosystem efficiently? Well, mathematicians have been trying to factor efficiently for centuries, and they still haven’t figured out how to do it. So, we are again appealing to a proof by eminent authority, but at least there are more authorities involved here.

What is the cryptosystem? Let $N$ be a product of two very large primes $p, q$ such that $p \equiv q \equiv 3 \pmod{4}$. To send the message $x$, send $\text{rem} \left(x^2, N\right)$.\(^1\)

We need to show that if the person we send the message to knows $p, q$, then they can decode the message. On the other hand, if an eavesdropper who doesn’t know $p, q$ listens in, then we must show that they are very unlikely to figure out this message.

First some definitions. We know what it means for a number to be a square over the integers, that is $s$ is a square if there is another integer $x$ such that $s = x^2$. Over the numbers mod $N$, we say that $s$ is a square modulo $N$ if there is an $x$ such that $s \equiv x^2 \pmod{N}$. If $x$ is such that $0 \leq x < N$ and $s \equiv x^2 \pmod{N}$, then $x$ is the square root of $s$.

(a) What are the squares modulo 5? For each nonzero square in 0, ..., 4, how many square roots does it have?

Solution. 0,1,4 are the squares. 1 and 4 each have 2 square roots (1,4) and (2,3) respectively. 2 and 3 have 0 square roots.

(b) For each integer in 1..14 that is relatively prime to 15, how many square roots (modulo 15) does it have? Note that all the square roots are also relatively prime to 15. We won’t go through why this is so here, but keep in mind that this is a general phenomenon!

Solution. 1,4 each have 4 square roots. 2,7,8,11,13,14 have no square roots.

(c) Suppose that $p$ is a prime such that $p \equiv 3 \pmod{4}$. It turns out that squares modulo $p$ have exactly 2 square roots. First show that $\frac{p+1}{4}$ is an integer. Next figure out the two square roots of 1 modulo $p$. Then show that you can find a “square root mod a prime $p$” of a number by raising the number to the $\frac{p+1}{4}$th power. That is, given $s$,

\(^1\) We will see soon, that there are other numbers that would be encrypted by $\text{rem} \left(x^2, N\right)$, so we’ll have to disallow those other numbers as possible messages in order to make it possible to decode this cryptosystem, but let’s ignore that for now.
to find $x$ such that $s \equiv x^2 \pmod{p}$, you can compute $\text{rem}(s^{p+1}, p)$.

**Solution.** $s \equiv x^2 \pmod{p}$ implies that $s^p \equiv x^{p+1} \equiv x^{\frac{p-1}{2}} \cdot x \pmod{p}$. The square roots of 1 modulo $p$ are just 1 and $-1$. Now by Fermat’s theorem, the latter is equivalent modulo $p$ to both $+x$ and $-x$.

(d) By something called the Chinese Remainder Theorem, one can show that if $p$, $q$ are distinct primes, then $s$ is a square modulo $N = p \cdot q$ if and only if $s$ is a square modulo $p$ and $s$ is a square modulo $q$. In particular, if $s \equiv x^2 \pmod{p} \equiv (x')^2 \pmod{p}$ and $s \equiv y^2 \pmod{p} \equiv (y')^2 \pmod{p}$ then $s$ has exactly four square roots, namely, $s \equiv (xy)^2 \pmod{N} \equiv (x'y)^2 \pmod{N} \equiv (xy)^2 \pmod{N} \equiv (x'y)^2 \pmod{N}$. So, if you know $p$, $q$, using the solution to the previous problem part, you can efficiently find the square roots of $s$! Thus, given the secret key, decoding is easy.

But what if you don’t know $p$, $q$? Suppose as above that $N = p \cdot q$, where $p$, $q$ are two primes equivalent to $3 \pmod{4}$. Let’s assume that the evil message interceptor claims to have a program that can find all four square roots of any number modulo $N$. Show that he can actually use this program to efficiently find the factorization of $N$. Thus, unless this evil message interceptor is extremely smart and has figured out something that the rest of the scientific community has been working on for years, it is very unlikely that this efficient square root program exists!

**Hint:** Pick $r$ arbitrarily from $1, \ldots, N-1$. If $\gcd(N, r) > 1$, then you are done (why?) so you can halt. Otherwise, use the program to find all four square roots of $r$, call them $r, -r, r', -r'$. Note that $r^2 \equiv r'^2 \pmod{N}$. How can you use these roots to factor $N$?

**Solution.** $r^2 - r'^2 \equiv (r + r')(r - r') \pmod{N} \equiv 0 \pmod{N}$. Therefore one of $(r + r')(r - r')$ divides $N = p \cdot q$, and since $p, q$ are primes, it must be the case that one of $(r + r'), (r - r')$ divided $p$, whereas the other divides $q$. So compute $g = \gcd(N, r - r')$. Output $g, N/g$ and halt.

In the actual proof of security of the Rabin cryptosystem, you need to show that if you have a program that can find any square root of a number modulo $N$ then you can factor $N$. But the outline of the proof is essentially the same.

(e) If the evil message interceptor knows that the message is the encoding one of two possible candidate messages (i.e., either “meet at dome at dusk” or “meet at dome at dawn”) and is just trying to figure out which of the two, then can he break this cryptosystem?

**Solution.** Yes, he just needs to square both candidate messages, take the remainder with $N$ (which he knows) and see which one was sent. If it’s so easy, then why is this a secure cryptosystem? Well, it’s still pretty good in the case when there are a lot of possible messages.