Problem Set 3

Due: Monday, September 27 at 9pm

revised September 26, 2004, 1258 minutes

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

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

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

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

(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 \( q \).)

(e) \( nx \ rem \ dx = (n \ rem \ d) \cdot x \) when \( x \in \mathbb{N}^+ \).

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

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

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

(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 \( p \mid b \).

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.
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 \( S_k \equiv -1 \pmod{p} \).

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:

\[
3^2 \mid 777777777
\]

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

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.

(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 \( \{0, 1, 2, \ldots, b-1\} \).

(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.

(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.