CS-210 Discrete Mathematics

Problem Set 10

1. Prove that two integers a and b have the same remainders modulo m if and only if m divides $a-b$. This is actually the definition of residue classes modulo m, just work out the arithmetic, using the division algorithm to verify $a-b$ is an integer iff a and b belong to the same residual class $\mod m$

2. In each case either prove the statement or find a counterexample.

   (a) The sum of any three consecutive integers (positive or negative) is divisible by 3.

   (b) The product any two even integers is divisible by 4.

   (c) The product of any four consecutive integers (positive or negative) is divisible by 8.

   (d) If $a-b$ has remainder 0 when divided by m, then a and b have remainders 0 when divided by m.

   (e) If n is an odd integer, then $3n+3$ is divisible by 6.

3. For any integer i and $m > 0$, define $A_{i,m} =: \{x \mid \exists\, y \in \mathbb{Z} : x = i + ym\}$.

   (a) Prove that if $a \equiv b \pmod{m}$, then $A_{a,m} = A_{b,m}$.

   (b) Prove that if $a \not\equiv b \pmod{m}$, then $A_{a,m} \cap A_{b,m} = \emptyset$.

4. Let p and q be two primes (with $p \neq q$). Prove that $\log_p(q)$ is irrational.
   Hint: Assume that it is rational and draw a contradiction to the uniqueness in the Fundamental Theorem of Arithmetic.

5. Prove that for any integers a and b, $gcd(a, b)$ can be written as a linear combination of a and b. i.e. $\exists\, s, t \mid gcd(a, b) = sa + tb$. In the class we actually gave a constructive proof, i.e. we found s and t through the extended Euclidean algorithm. Now you have to prove it with the following steps.

   - Make a set of all positive linear combinations of a and b.
   - Apply principle of well-ordering on the above set to select an element g of it.
   - Show that g divides both a and b
   - Using the fact that g belongs to the above set, show that any common divisor of a and b must divide g also. This proves that all other common divisors are less than g.

6. As a corollary to the above question, prove that *Any integer d divides a and b if and only if d divides $gcd(a, b)$.*

7. Give at least two examples to show that the assertion of the Fermat's little theorem is not valid if we do not require the modulus to be a prime.

8. Find the values of $3^{302} \mod 5, 3^{302} \mod 7, 3^{302} \mod 11, 3^{302} \mod 385$
   Hint: Use FLT for the first three and CRT for the last one

9. (a) Prove that $a \mid b$ if and only if $gcd(a, b) = a$.

(b) Let $b > 9a$, Show that $gcd(a, b) = gcd(a, b - 2a)$

(c) Show that If a is even and b is odd, then $gcd(a, b) = gcd(\frac{a}{2}, b)$

(d) Show that if a is even and b is even, then $gcd(a, b) = 2gcd(\frac{a}{2}, \frac{b}{2})$

10. Show that whenever a and b are both positive integers, then $(2^a - 1) \mod (2^b - 1) = 2^{a \mod b} - 1$.

11. (a) Show that the system of congruences $x \equiv a_1(\mod m_1)$ and $x \equiv a_2(\mod m_2)$ has a solution if and only if $gcd(m_1, m_2) \mid a_1 - a_2$.

    (b) Show that the solution in part (a) is unique modulo $lcm(m_1, m_2)$.

12. Suppose that p is a prime and $0 < k < p$

    (a) k is self-inverse if $k^2 \equiv 1(\mod p)$. Prove that k is self-inverse if and only if either $k = 1$ or $k = p - 1$.

    (b) Prove $(p - 1)! \equiv -1(\mod p)$

13. Prove that for $n > 2$ there exist a prime number between n and $n!$.

14. Suppose the RSA modulus $n = pq$ is the product of distinct 200 digit primes p and q. A message $m \in [0 \ldots n)$ is called dangerous if $gcd(m, n) = p$ or $gcd(m, n) = q$, because such an m can be used to factor n and so crack RSA.

    Estimate the fraction of messages in $[0 \ldots n)$ that are dangerous to the nearest order of magnitude.

15. Let p, q be relatively prime (i.e. $gcd(p, q) = 1$). Prove that the system of equations

$$x = a(\mod p)$$

$$x = b(\mod q)$$

has a unique solution for x modulo pq.