Elementary Number Theory

Problem Set: Week 6

A selection of exercises on Simultaneous Linear Congruences and supplementary exercises on Quadratic Residues

Andrew Dong

Professor Ngo Bao Chau
Minh-Tam Trinh

November 19, 2015

Math 17500: Problem Set Week 6

1. Find all integers satisfying both congruences $x \equiv 10$ mod 24 and $x \equiv 16$ mod 18

Solution:

$x \equiv 10$ mod 24 $\Rightarrow x = 10$ + 24t.
Putting this value of x into our second congruence $x \equiv 16$ mod 18 we get
$10 + 24t \equiv 16$ mod 18 which becomes $24t \equiv 6$ mod 18 which becomes $4t \equiv 1$ mod 3 which can be rewritten $t \equiv 1$ mod 3. Thus t = 1 + 3s where $s \in Z$.

Plugging in this value for t into our original congruence, we get $x = 10 + 24(1 + 3s) = 34 + 72s$. Thus $x \equiv 34$ mod 72. Notice that 72 is the lcm(24,28).

2. Find all integers satisfying both congruences $x \equiv 8$ mod 9 and $x \equiv 31$ mod 33

Solution:

$x \equiv 8$ mod 9 implies that x = 8 + 9t for integer valued t. Plugging this value of x into our second congruence yields the congruence $8 + 9t \equiv 31$ mod 33 or $9t \equiv 23$ mod 33. Since gcd(9,33) = 3 and 3 does not divide 23, t has no solutions, thus there are no integers satisfying both congruences.

3. Prove that there exists integer $x \in Z$ satisfying $x \equiv m$ mod a and $x \equiv n$ mod b if and only if $m \equiv n$ mod gcd(a,b). In that case, find the general form of the solution

Solution:

If an integer solution x exists then $x \equiv m$ mod a and $x \equiv n$ mod b and thus $a|(x - m)$ and $b|(x - n)$. Let c = gcd(a,b) so c divides both a and b and therefore also divides x-m and x-n. Notice that c must divide (x-n) - (x-m) = m - n, which is equivalent to saying that $m = n$ mod c $\sim m \equiv n$ mod gcd(a,b).

The general solution forms a single congruence class mod(y) where y = lcm(a,b). Suppose x_0 is any solution of the congruences. Then an integer x is a solution to the congruences if and only if $x \equiv x_0$ mod (a) and $x \equiv x_0$ mod (b). This implies that $x - x_0$ is divisible by a and b, or equivalently $x - x_0$ is divisible by their least common multiple lcm(a,b). Thus, the general solution consists of a single congruence clas x_0 mod lcm(a,b).

4. Solve the system of congruences:
$2x + 36 \equiv 1$ mod 17
$5x + 10y \equiv 2$ mod 17

Solution:

$2x \equiv 16$ mod 17 $\implies$ $x \equiv 8$ mod 16.

We then have $40 + 10y \equiv 2$ mod 17 $\implies$ $10y \equiv 13$ mod 17 $\implies$ [y] = [3] since $3 * 10 = 30 = 13$ mod 17.

5. Solve the system of congruences:
$2x + 3y \equiv 1$ mod 24
$6x + 10y \equiv 2$ mod 24

Solution:

we write our first congruence
$6x + 9y \equiv 3$ mod 24. Subtracting our second congruence from this transformation of our first congruence we get $y \equiv 23$ mod 24.
Putting this value back into our first congruence we get $2x - 3 \equiv 1$ mod 24. Thus $2x \equiv 4$ mod 24 and $x \equiv 2$ mod 12.

6. Solve the congruence equation $x^2 \equiv 61$ mod 100

Solution:

The congruence equation has solutions for $x \equiv 19$ mod 50 and $\equiv 31$ mod 50.

7. Solve the congruence equation $x^2 \equiv 61$ mod 1000

Solution:

Actually, this congruence equation doesn't have any solutions because $x \equiv 19$ mod 50 and $\equiv 31$ mod 50 both fail mod for $x^2 \equiv 61$ mod 1000.

8. Exercise 7.20

Question: Show that, for each $r \geq 1$, there are infinitely many primes $p \equiv 1$ mod (2^r).

Solution:

Suppose there are instead finitely many primes $p \equiv 1$ mod (2^r). Name them $p_1, ..., p_k$ and define a = $2p_1 * ... * p_k$ and $m = a^{2^{2-1}} + 1$ which is divisible by an odd prime p. Since a has order 2^r in U_p, by Lagrange's theorem we have that $2^r | p - 1$. This implies the congruence $p \equiv 1 mod (2^r)$ which means that p = p_i for some i and p divides a. But since p divies m, we have that $p | m - a^{2r-1} = 1$, which is a contradiction. Thus, there must be infinitely many primes $p \equiv 1$ mod (2^r). $\square$

9. Exercise 7.21

Question: For which values of n is -1 a quadratic residue mod (n)?

Solution:

We determine the values for which -1 is a quadratic residue mod n by our corollary that $-1 \in Q_p \iff p \equiv 1$ mod 4. However, we know that a value n is in the set of quadratic residues over n if and only if a $\in$ the set of quadratic residues over n_i for where $n = n_1 * n_2 * ... * n_i$ where n_i are mutually coprime.

To determine values n can take, we must check the cases for two quadratic residue sets, Q_{2^e} and Q_{n_i} where $n_i > 2$. For the case of Q_{2^e} we know that e must equal 0 or 1 for $-1 \in Q_{2^e}$. For the case of Q_{n_i} where $n_i > 2$ we apply our corollary and claim that $-1 \in Q_{n_i}$ where $n_i > 2 \iff n_1 \equiv 1 mod 4$.

Taking the results from these two cases we conclude that -1 is a quadratic residue mod(n) for values n not divisible by 4 or any prime of the form $p \equiv 3$ mod 4.

10. Exercise 7.23

Question: Show that if $n > 2$ then a quadratic residue mod (n) cannot also be a primitive root mod (n).

Solution:

By definition, for $n > 2$ the set of quadratic residues Q_n in Z_n is a proper subgroup of the set of units in Z_n, U_n. We also know that if a is in the set of quadratic residues then so are all powers of a. Recall that an element a is a primitive root if every number coprime to it is congruent to a power of g modulo a. Using the fact that the set of quadratic residues is strictly smaller than the set of units and the fact that all powers of a are in the set of quadratic residues for a quadratic residue, we know that there exists some elements of U_n that are not a power of a and thus a cannot be a primitive root mod (n).