Elementary Number Theory

Midterm Review

Number Theory Midterm and Solutions

Andrew Dong

Professor Ngo Bau Chau
Minh-Tam Trinh

November 12, 2015

Math 17500: Midterm

1. Find all positive integers x less than 200 such that $x \equiv 1$ mod 11 and $x \equiv 9$ mod 13

Notice that gcd(11,13) = 1 which implies that the solution belongs to the congruence class

$$x \equiv 1 * 13 * a + 9 * 11 * b \text{ mod } 11 * 13$$

where a,b ∈ Z satisfying 13a ≡ 1 mod 11 and
11b ≡ 1 mod 13.
The equation $13a \equiv 2a \equiv 1$ mod 11 has solution $a \equiv 6$ mod 11.
The equation $11b \equiv -2b \equiv 1$ mod 13 has solution b $\equiv -7 \equiv 6$ mod 13.
Therefore, $x \equiv 13 * 6 + 9 * 11 * 6 \equiv 100$ mod 143.
In the range $0 < x < 200$, the only solution is x = 100.

2. Find all positive Integers less than 100 such that $x^2 \equiv 11$ mod 49

We first find the solution of the equation $x^2 - 11 \equiv x^2 - 40$ mod 7. This equation has two solutions: $x \equiv \pm 2$ mod 7.
The solution of the equation $x^2 - 11 \equiv 0$ mod 49 then must have the form $x \equiv 2$ + 7y.
If x = 2 + 7y, we have $(2 + 7y)^2 - 11 \equiv 28y - 7$ mod 49. This is equivalent to
$4y \equiv 1$ mod 7 and
$y \equiv 2$ mod 7.
In this case $x \equiv 16$ mod 49.
If x = -2 + 7y, a similar calculation implies

3. Find the residue of $2^{1000} + 2^{100}$ modulo 13

4. Check that 2 is a primitive root modulo 13 by calculating the residue modulo 13 of all powers of 2

5. Find all residue classes x modulo 13 such that $x^3 \equiv 1$ mod 13

6. Find all residue classes x modulo 169 such that $x^3 \equiv 1$ mod 169

7. Prove that $(Z/5Z)^x and (Z/8z)^x$ are not isomorphic as abelian groups

8. Prove that $2^n + 1$ is a prime if and only if $\phi(2^n + 1) = 2^n$

9. Prove that $(Z/(2^{n+1})Z)^x$ and $(Z/2^{2^n+1}Z)^x$ are not isomorphic as abelian groups

10. Let p be an odd prime. How many primitive roots modulo p^2 are there? Justify your answer