Math 17500: Midterm Solution

November 3, 2015

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

   As $\gcd(11,13) = 1$, the solution belongs to the congruence class

   $$x \equiv 13 \times a + 9 \times 11 \times b \mod 11 \times 13$$

   with $a, b \in \mathbf{Z}$ satisfying $13a \equiv 1 \mod 11$ and $11b \equiv 1 \mod 13$. 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 $b \equiv -7 \equiv 6 \mod 13$. Thus $x \equiv 13 \times 6 + 9 \times 11 \times 6 \equiv 672 \equiv 100 \mod 143$. In the range $0 < x < 200$, the only solution is $x = 100$.

2. Find all positive integers less than 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 $x^2 - 11 \equiv 0 \mod 49$ must be of the form $x \equiv \pm 2 + 7y$.

   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 $x \equiv -16 \equiv 33 \mod 49$.

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

   By the little Fermat theorem, $2^{12} \equiv 1 \mod 13$. For $1000 \equiv 100 \equiv 4 \mod 12$, we have $2^{1000} \equiv 2^{100} \equiv 2^4 \equiv 3 \mod 13$. Therefore $2^{1000} + 2^{100} \equiv 6 \mod 13$.

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

y	1	2	3	4	5	6	7	8	9	10	11	12
$2^y \mod 13$	2	4	8	3	6	12	11	9	5	10	7	1

   The table shows that $y \mapsto 2^y$ defines a bijection between $\mathbf{Z}/12\mathbf{Z}$ and $(\mathbf{Z}/13\mathbf{Z})^\times$. As it is obvisously a homomorphism of abelian groups, this application defines an isomorphism between $\mathbf{Z}/12\mathbf{Z}$ and $(\mathbf{Z}/13\mathbf{Z})^\times$.

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

   For $y \mapsto 2^y$ defines an isomorphism of abelian groups $\mathbf{Z}/12\mathbf{Z} \to (\mathbf{Z}/13\mathbf{Z})^\times$, it is enough to look for solution of the form $x \equiv 2^y \mod 13$ where y is a congruence class modulo 12. The equation $2^{3y} \equiv 1 \mod 13$ implies that $3y \equiv 0 \mod 12$ and thus $y \equiv 0 \mod 4$. Thus y is congruent to 0, 4 or 8 mod 12. Looking up to above table we infer that x congruent to 1, 3 or 9 modulo 13.

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

   By the previous question, x has to be of the form $1+13t, 3+13t$ or $9+13t$. If $x \equiv 1+13t \mod 169$ then $(1+13t)^3 \equiv 1+3\times 13t \mod 169$ by the binomial formula. The variable t satisfies the equation $3\times 13t \equiv 0 \mod 169$ or equivalently, $t \equiv 0 \mod 13$. Thus $x \equiv 1 \mod 169$.

   If $x = 3+13t \mod 169$ then $(3+13t)^3 \equiv 3^3 + 3\times 3^2 \times 13t \mod 169$ by the binomial formula. The variable t satisfies the equation $27\times 13t \equiv -26 \mod 169$ or equivalently, $t \equiv -2 \mod 13$. Thus $x \equiv -23 \mod 169$.

   If $x = 9+13t \mod 169$ then $(9+13t)^3 \equiv 9^3 + 3\times 9^2 \times 13t \mod 169$ by the binomial formula. The variable t satisfies the equation $3\times 9^2 \times 13t \equiv 117 \mod 169$ or equivalently, $3\times 9^2 t \equiv 9 \mod 13$. Simplifying by 9 that is coprime to 13, we find $27t \equiv 5 \equiv 1 \mod 13$. Thus $x \equiv 22 \mod 169$.

7. Prove that $(\mathbf{Z}/5\mathbf{Z})^\times$ and $(\mathbf{Z}/8\mathbf{Z})^\times$ are not isomorphic as abelian groups.

   For all prime p, $(\mathbf{Z}/p\mathbf{Z})^\times$ is a cyclic group of order $p-1$. In particular $(\mathbf{Z}/5\mathbf{Z})^\times$ is isomorphic to $\mathbf{Z}/4\mathbf{Z}$. On the other hand, direct inspection every element of $(\mathbf{Z}/8\mathbf{Z})^\times$ is its own inverse. In particular the latter can't be isomorphic to $\mathbf{Z}/4\mathbf{Z}$.

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

   For every integer m, $\mathbf{Z}/m\mathbf{Z}$ has no more than $m-1$ elements for the congruence class of 0 isn't invertible. It has exactly $m-1$ elements if and only if every nonzero congruence class module m is invertible and thus m has no strict divisor other than 1. Thus m has to be a prime. In particular $\phi(2^n+1) = 2^n$ if and only if 2^n+1 is a (Fermat) prime.

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

   We have $\phi(2^n+1) \le 2^n$ and $\phi(\mathbf{Z}/2^{2n+1}\mathbf{Z})^\times = 2^{2n}$. Groups of different order can't be isomorphic.

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

    If p is an odd prime $(\mathbf{Z}/p^2\mathbf{Z})^\times$ is a cyclic group of order $p(p-1)$. In other words there is an isomorphism $(\mathbf{Z}/p^2\mathbf{Z})^\times \simeq \mathbf{Z}/p(p-1)\mathbf{Z}$. Via this isomorphism, primitive congruence classes modulo p^2 correspond to invertible class modulo $p(p-1)$. Thus there are exactly $\phi(p(p-1)) = (p-1)\phi(p-1)$ primitive classes modulo p^2.