Math 435 Number Theory I
Midterm 2
November 11, 2005

1) Calculate $\phi(4500)$.

$$\phi(4500) = \phi(125 * 9 * 4) = \phi(125)\phi(9)\phi(4) = (125 - 25)(9 - 3)(4 - 2) = 1200$$

2) Calculate $5^{423}(\text{mod } 33)$

$\phi(33) = \phi(3)\phi(11) = 20$. Thus

$$5^{423} \equiv (5^{20})^{21}5^3 \equiv 125 \equiv 26(\text{mod } 33).$$

3) a) How many primitive roots are there in U_{23}?

$\phi(22) = \phi(2)\phi(11) = 10$.

b) 5 is a primitive root in U_{23}. Below is a table of powers of 5 mod 23.

n	1	2	3	4	5	6	7	8	9	10	11
5^n	5	2	10	4	20	8	17	16	11	9	22

n	12	13	14	15	16	17	18	19	20	21	22
5^n	18	21	13	19	3	15	6	7	12	14	1

Find all solutions to $X^6 \equiv 6 \pmod{23}$

$6 \equiv 5^{18}$. Thus we want to find k such that $5^{6i} \equiv 5^{18} \pmod{23}$. We need to have $6i \equiv 18 \pmod{22}$. There will be two solutions. Both are solutions to $3i \equiv 9 \pmod{11}$. The solutions are $i = 3, 14$ and $x = 10, 13$.

4) Let $f(X) = X^3 - 2X + 9$. Note that $3, 4$ are the solutions to $f(X) \equiv 0 \pmod{5}$. Use Hensel's Lemma to find all solutions to $f(X) \equiv 0 \pmod{25}$.

First look for solutions $x = 3 + 5k$.

$$\begin{aligned} f(x) &\equiv f(3) + f'(3)(5k) \pmod{25} \\ &\equiv 30 + 25(5k) \pmod{25} \end{aligned}$$

Since $25 \not| 30$ there are no solutions mod 25 congruent to 3.

Next look for solutions $x = 4 + 5k$.

$$\begin{aligned} f(x) &\equiv f(4) + f'(4)(5k) \pmod{25} \\ &\equiv 65 + 46(5k) \pmod{25} \end{aligned}$$

Dividing by 5, we see that we have to solve

$$13 + 46k \equiv 0 \pmod 5$$

or $3 + k \equiv 0 \pmod 5$. Thus $k \equiv 2 \pmod 5$. Thus the unique solution to $f(X) \equiv 0 \in \mathbb{Z}_{25}$ is $4 + 5(2) = 14$.

5) Calculate $\left(\dfrac{139}{211}\right)$.

$$\begin{aligned} \left(\frac{139}{211}\right) &= -\left(\frac{211}{139}\right) \\ &= -\left(\frac{72}{139}\right) \\ &= -\left(\frac{2}{139}\right)^3 \left(\frac{3}{139}\right)^3 \\ &= (-1)^4(\pm 1)^2 \\ &= 1 \end{aligned}$$

6) Let p be an odd prime. Sketch a proof that $X^2 \equiv -1 \pmod p$ has a solution if and only if $p \equiv 1 \pmod 4$.

By Euler's criterion

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Thus $\left(\dfrac{-1}{p}\right) = 1$ if and only if $\frac{p-1}{2}$ is even, if and only if $p \equiv 1 \text{mod } 4$.

7) Let $n > 2$. Suppose g is a primitive root mod n.

a) Suppose i is even. Prove that g^i is not a primitive root. [Hint: You may use the fact that $\phi(n)$ is even.]

$$(g^i)^{\frac{\phi(n)}{2}} = (g^{\frac{\phi(n)}{2}})^i \equiv 1 \pmod{n}$$

Thus g^i is not a primitive root.

b) Prove that g and h are primitive roots mod n, then gh is not a primitive root mod n.

$h = g^i$ for some i. By a) i is odd. But $gh = g^{i+1}$ and $i + 1$ is even, thus gh is not a primitive root.