Kris Harper
MATH 24200
April 28, 2010

Homework 3

Problem 1. *If $p = 2^n + 1$ is a Fermat prime, show that 3 is a primitive root modulo p.*

Proof. Suppose 3 is not a primitive root modulo p. Then $3^{(p-1)/2}$ is not equivalent to -1 modulo p. But then 3 is a square modulo p. Since $p = 4t+1$ we know there exists an integer a such that $-3 \equiv a^2 \pmod p$. Now consider the equation $2u \equiv -1 + a \pmod p$. We have $4u^2 \equiv a^2 - 2a + 1 \equiv -2a - 2 \pmod p$ and $4u^3 \equiv (-a-1)(a-1) \equiv -a^2 + 1 \equiv 4 \pmod p$ so $u^3 \equiv 1 \pmod p$. But then u has order 3 modulo p which implies $p \equiv 1 \pmod 3$. This is a contradiction and so 3 must be a primitive root modulo p. $\square$

Problem 2. *Use the fact that 2 is a primitive root modulo 29 to find the seven solutions to $x^7 \equiv 1 \pmod{29}$.*

Proof. Note that $a^7 \equiv a^{\phi(29)/4} \equiv 1 \pmod{29}$ if and only if there exists x such that $x^4 \equiv a \pmod{29}$. Since 2 is a primitive root modulo 29, all the solutions of this can be found by raising looking at multiples of 2^4. Note that $2^4 \equiv 16 \pmod{29}$, $(2^2)^4 = 16(2^4) \equiv 24 \pmod{29}$, $(2^3)^4 = 24(2^4) \equiv 7 \pmod{29}$, $(2^4)^4 = 7(2^4) \equiv 25 \pmod{29}$, $(2^5)^4 = 25(2^4) \equiv 23 \pmod{29}$, $(2^6)^4 = 23(2^4) \equiv 20 \pmod{29}$. Thus the seven solutions are 1, 7, 16, 20, 23, 24 and 25. $\square$

Problem 3. *Solve the congruence $1 + x + x^2 + \cdots + x^6 \equiv 0 \pmod{29}$.*

Proof. Thus the the 7th degree cyclotomic polynomial. The solutions to it are the nontrivial solutions to $x^7 \equiv 1 \pmod 7$. By Problem 2 we know the solutions are 7, 16, 20, 23, 24 and 25. $\square$

Problem 4. *Use Gauss' lemma to determine $\left(\frac{5}{7}\right)$, $\left(\frac{3}{11}\right)$, $\left(\frac{6}{13}\right)$, and $\left(\frac{-1}{p}\right)$.*

Proof. We know $(7-1)/2 = 3$ and 5, 10 and 15 reduce to -2, 3 and 1 modulo 7 so $\left(\frac{5}{7}\right) = -1$.

We know $(11-1)/2 = 5$ and 3, 6, 9, 12 and 15 reduce to 3, -5, -2, 1 and 4 modulo 11 so $\left(\frac{3}{11}\right) = (-1)^2 = 1$.

We know $(13-1)/2 = 6$ and 6, 12, 18, 24, 30 and 36 reduce to 6, -1, 5, -2, 6 and -3 modulo 13 so $\left(\frac{6}{13}\right) = (-1)^3 = -1$.

Now we need to consider -1 times the values $\{1, 2, \ldots, (p-1)/2\}$. But clearly all of these are going to be in the set of least residues mod p and they will all be negative. Thus $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. $\square$

Problem 5. *Show that the number of solutions to $x^2 \equiv a \pmod p$ is given by $1 + (a/p)$.*

Proof. If $p \mid a$ then $(a/p) = 0$ and $x = 0$ is the only solution. If a is not a quadratic residue modulo p then there are no solutions and $1 + (a/p) = 0$. If a is a quadratic residue modulo p then there exists x such that $x^2 \equiv a \pmod p$. Note that $-x$ is clearly also a solution. But we know that there are exactly $(2, \phi(2)) = 2$ solutions so there are $2 = 1 + (a/p)$ solutions. $\square$

Problem 6. *Prove that $\sum_{a=1}^{p-1}(a/p) = 0$.*

Proof. We know there are as many residues as nonresidues modulo p. Since these have Legendre symbols 1 and -1 respectively, their sum must be 0. $\square$

Problem 7. *Suppose that $p \equiv 3 \pmod 4$ and that $q = 2p + 1$ is also a prime. Prove that $2^p - 1$ is not prime. One must assume that $p > 3$.*

Proof. Since $p \equiv 3 \pmod 4$ and $q = 2p+1$ we see that $q \equiv 7 \pmod 8$ so $(2/q) = 1$. Thus there exists m such that $m^2 \equiv 2 \pmod q$. Then $2^p \equiv 2^{(q-1)/2} \equiv m^{q-1} \equiv 1 \pmod q$. Thus $q \mid 2^p - 1$. If $p > 3$ then $2^p - 1 > 2p + 1$ so q is not the only factor and $2^p - 1$ is not prime. $\square$

Problem 8. *Let $f(x) \in \mathbb{Z}[x]$. We say that a prime p divides $f(x)$ if there is an integer n such that $p \mid f(n)$. Describe the prime divisors of x^2+1 and x^2-2.*

Proof. A prime p is a prime divisor of x^2+1 if there exists n such that $p \mid (n^2+1)$. But this simply means $n^2 \equiv -1 \pmod p$ so $(-1/p) = 1$. Thus p divides x^2+1 if and only if $(-1)^{(p-1)/2} = 1$ or $p \equiv 1 \pmod 4$. Likewise, $p \mid x^2 - 2$ if and only if $(2/p) = 1$, or p is congruent to 1 or -1 modulo 8. $\square$

Problem 9. *Show that any prime divisor of $x^4 - x^2 + 1$ is congruent to 1 modulo 12.*

Proof. Suppose that p is a prime divisor of x^4-x^2+1. Then $x^4-x^2+1 \equiv 0 \pmod p$ so $4x^4+4x^2+4 \equiv= (2x^2-1)^2+3 \equiv 0 \pmod p$ and $(2x^2-1)^2 \equiv -3 \pmod p$. Likewise $x^4-2x^2+1 \equiv (x^2-1)^2 \equiv -x^2 \pmod p$. From this we know $1 = (-3/p) = (-1/p)(3/p) = (-1)^{(p-1)/2}(3/p)$. So either $(-1)^{(p-1)/2} = -1$ and $(3/p) = -1$ or $(-1)^{(p-1)/2} = 1$ and $(3/p) = 1$. But note that $1 = (-x^2/p) = (-1/p)(x/p)(x/p) = (-1/p)(x/p)^2 = (-1/p)$. Thus $(-1/p) = 1$ and therefore $(3/p) = 1$ as well. From quadratic reciprocity and the fact that $(p-1)/2 \equiv 0 \pmod 2$, we know $(3/p) = (p/3) = 1$. But 1 is the only nontrivial quadratic residue modulo 3 so it follows that $p \equiv 1 \pmod 3$ and $p \equiv 1 \pmod 4$ so $p \equiv 1 \pmod{12}$. $\square$

Problem 10. *Use the fact that $U(\mathbb{Z}/p\mathbb{Z})$ is cyclic to give a direct proof that $(-3/p) = 1$ when $p \equiv 1 \pmod 3$.*

Proof. Since $p \equiv 1 \pmod 3$ we know $p = 3t+1$ and $\phi(p) = 3t$. Since $U(\mathbb{Z}/p\mathbb{Z})$ is cyclic there exists some element ρ which generates a subgroup of order 3, i.e., that has order 3. We also have $\rho^2+\rho+1 = \rho^3+\rho^2+\rho = \rho(\rho^2+\rho+1)$. Since $\rho \neq 1$ it must be the case that $\rho^2+\rho+1 = 0$. Thus $4\rho^2+4\rho+4 = 0$ and $-3 = 4\rho^2+4\rho+1 = (2\rho+1)^2$. Thus $(-3/p) = 1$. $\square$

Problem 11. *Using quadratic reciprocity find the primes for which 7 is a quadratic residue. Do the same for 15.*

Proof. We wish to solve $(7/p) = 1$ for p. By quadratic reciprocity and the fact that $7 \equiv 3 \pmod 4$ we know $(7/p) = -(p/7)$. By a simple calculation, we see the quadratic residues modulo 7 are 1, 2 and 4. Thus we need $p \equiv 3 \pmod 7$, $p \equiv 5 \pmod 7$ or $p \equiv 6 \pmod 7$. These are the primes for which 7 is a quadratic residue.

We have precisely the same setup as before since $15 \equiv 3 \pmod 4$. Thus $(15/p) = -(p/15)$. Another quick check shows that 1, 4, 6, 9, and 10 are quadratic residues modulo 15. Thus $p \equiv 2$, $p \equiv 7$, $p \equiv 8$, $p \equiv 11$, $p \equiv 12$, $p \equiv 13$ and $p \equiv 14$ are values of p such that 15 is a quadratic residue modulo p. $\square$