

MAT 311: Number Theory

Spring 2008

Solutions to HW5

1. Assume that p is an odd prime. Show that $x^2 \equiv 2 \pmod{p}$ has a solution iff $p \equiv \pm 1 \pmod{8}$.
 The key fact is that $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. The expression in the exponent is clearly independent of the representative of p mod 8, that is, if $p \equiv p' \pmod{8}$, then $(-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{p'^2-1}{8}}$. Now, it is straightforward to check that $(-1)^{\frac{p^2-1}{8}} = 1$ iff p is congruent to 1 or 7 mod 8, as required. □

2. Prove that $x^2 \equiv 16 \pmod{p}$ has a solution for every prime p .
 This is rather a dull question, since $x = 4$ is obviously a solution no matter what p is. □

3. Find the number of solutions of the following congruences: $x^2 \equiv 2 \pmod{59}$, $x^2 \equiv -2 \pmod{59}$.
 The first has no solution by problem 1 since $59 \equiv 3 \not\equiv \pm 1 \pmod{8}$. The second one indeed *has* solutions: Note that the solution exists iff -2 is a QR mod 59, i.e. $\left(\frac{-2}{59}\right) = 1$. But by multiplicativity property of the Legendre symbol we have $\left(\frac{-2}{59}\right) = \left(\frac{-1}{59}\right) \left(\frac{2}{59}\right)$. Now, $\left(\frac{2}{59}\right) = -1$ by problem 1. But recall the fact that $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ for any odd prime p . Hence $\left(\frac{-1}{59}\right) = -1$, and so $\left(\frac{-2}{59}\right) = 1$. Therefore the second congruence has solutions. Now, since $x^2 + 2$ is a second degree polynomial $x^2 \equiv -2 \pmod{59}$ has **at most two** solutions. But note that x is a solution iff $-x$ is a solution; and $x \equiv -x \pmod{59}$ iff $x \equiv 0$, which is obviously not a solution of our congruence at all. Thus, $x^2 \equiv -2 \pmod{59}$ must have **at least two** solutions. Thus it has **precisely two** solutions. □

4. Let g be a primitive root mod p . Show that quadratic residues mod p are g^2, g^4, \dots, g^{p-1} and the quadratic nonresidues mod p are g, g^3, \dots, g^{p-2} . Count the number of QRs and QNs.
 In order the question to make sense we should assume that p is an *odd* prime (of course the case $p = 2$ is trivial to check). Obviously any number in the list g^2, g^4, \dots, g^{p-1} are perfect squares, hence they are automatically QRs. On the other hand, none of the g, g^3, \dots, g^{p-2} are QR mod p , because $\left(\frac{g^{2k+1}}{p}\right) = (g^{2k+1})^{\frac{p-1}{2}} = (g^{p-1})^k \cdot g^{\frac{p-1}{2}} = 1^k \cdot g^{\frac{p-1}{2}} = g^{\frac{p-1}{2}} \neq 1$ since g is a primitive root (i.e. the smallest positive power that makes 1 is $p-1$). It turns out that $g^{\frac{p-1}{2}} = -1$. Thus g^{2k+1} is QN. So there are $\frac{p-1}{2}$ QRs and $\frac{p-1}{2}$ QNs (of course if $p \geq 3$). □

5. Determine how many solutions each of the following congruences has: $x^{12} \equiv 16 \pmod{17}$, $x^{20} \equiv 13 \pmod{17}$, $x^{48} \equiv 9 \pmod{17}$, $x^{11} \equiv 9 \pmod{17}$.
 This is a straightforward application of Theorem 3.27 from NZM. In each case, first find $\gcd(\text{degree of } x, p-1)$, then take the $((p-1)/\gcd)$ th power of the number on the right side of the congruence. If you get $1 \pmod{p}$, then there are \gcd many solutions of the congruence. Otherwise, there are none. As an example, in the first congruence, $\gcd(12, 16) = 4$ and $16^{16/4} \equiv 2^{16} \equiv 1 \pmod{17}$ (last congruence follows from Fermat). Thus there are precisely four solutions. Similarly we have:
 $\gcd(20, 16) = 4$ and $13^{16/4} \equiv 13^4 \equiv 1 \pmod{17}$ (last congruence can be checked easily on a calculator or be done by hand). Thus there are four solutions.
 $\gcd(48, 16) = 16$ and $9^{16/16} \equiv 9 \not\equiv 1 \pmod{17}$. Thus there are no solutions. You could also say that $9^{48} \equiv (9^{16})^3 \equiv 1^3 \equiv 1 \pmod{17}$, thus it cannot be equivalent to $9 \pmod{17}$
 $\gcd(11, 16) = 1$ and $9^{16/1} \equiv 9^{16} \equiv 1 \pmod{17}$ (by Fermat). Thus there is only one solution. □