

104B Problem Set 3

Rino Sanchez

February 13, 2003

9.1, # 1ad, 2bc, 5,6,8

1. Find all quadratic residues and quadratic nonresidues in a complete residue system modulo each of the following integers.

(a) 11: We can simply compute the squares of integers and reduce modulo 11, and this will give us all the quadratic residues.

$$1^2 \equiv 1 \pmod{11}, \quad 2^2 \equiv 4 \pmod{11}, \quad 3^2 \equiv 9 \pmod{11}, \quad 4^2 \equiv 5 \pmod{11}, \quad 5^2 \equiv 3 \pmod{11}$$

We don't have to compute any others because $6 \equiv -5 \pmod{11}$ so we'd get the same squares modulo 11. This means that the quadratic residues modulo 11 are 1, 4, 9, 5, and 3, and the quadratic nonresidues modulo 11 are 2, 6, 7, 8, and 10 (the leftovers).

(d) 33: We can use the same method as in (a), squaring integers relatively prime to 33 and reducing modulo 33.

$$1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 4^2 \equiv 16, \quad 5^2 \equiv 25, \quad 7^2 \equiv 16, \quad 8^2 \equiv 31, \quad 10^2 \equiv 1, \quad 13^2 \equiv 4, \quad 14^2 \equiv 31, \quad 16^2 \equiv 25$$

Therefore, the quadratic residues are 1, 4, 16, 25, and 31, and the quadratic nonresidues are 2, 5, 7, 8, 10, 13, 16, 17, 19, 20, 23, 25, 26, 28, 29, 31, and 32.

2. Evaluate the following Legendre symbols.

(b) $\left(\frac{23}{61}\right)$: So far the only real tool we have (in this section anyway, besides direct computation as in problem 1) is Euler's criterion, which means that we have to compute $23^{30} \pmod{61}$. Mathematica can compute that fairly rapidly, and we find that $23^{30} \equiv -1 \pmod{61}$, so 23 is not a quadratic residue modulo 61. Let us use quadratic reciprocity instead. As $61 \equiv 1 \pmod{4}$, we have

$$\left(\frac{23}{61}\right) = \left(\frac{61}{23}\right) = \left(\frac{-8}{23}\right) = \left(\frac{-1}{23}\right) \cdot \left(\frac{2}{23}\right) = -1 \cdot 1 = -1$$

which confirms our previous calculation.

(c) $\left(\frac{7}{31}\right)$: Once again, we can use Mathematica to deduce that $\left(\frac{7}{31}\right) = 1$ because $7^{15} \equiv 1 \pmod{31}$. Let us corroborate that using quadratic reciprocity. Since both $7 \equiv 31 \equiv 3 \pmod{4}$ we find

$$\left(\frac{7}{31}\right) = -\left(\frac{31}{7}\right) = -\left(\frac{3}{7}\right) = \left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1$$

5. Determine all prime numbers such that $p|n^2 + 1$ for some integer n .

Let's translate to a modular equation: there exist n such that $n^2 \equiv -1 \pmod{p}$, i.e. -1 is a quadratic residue modulo p . By Proposition 9.1.11, for odd primes p , this is true if and only if $p \equiv 1 \pmod{4}$. For $p = 2$, it is clear that $2|1^2 + 1$, so this completes the answer.

6. Determine the number of quadratic residues modulo p^n , where p is an odd prime.

We know that there is a primitive root modulo p^n , say g . Say $a = g^i$ and $x = g^k$. We would like to figure out when $x^2 \equiv a \pmod{p^n}$, so $g^{2k} \equiv g^i \pmod{p^n}$. This last equation holds if and only if $2k \equiv i \pmod{\phi(p^n)}$. Since $\phi(p^n) = p^{n-1}(p-1)$ is even, we can reduce that last equation modulo 2, and we find that i is even. Now we know that the quadratic residues modulo p^n are the even powers of g , so there are exactly $\phi(p^n)/2 = p^{n-1}(p-1)/2$ quadratic residues modulo p^n .

8. Use Euler's Criterion to give another proof of the property

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right).$$

If p divides either a or b , we can easily see that both sides of the equation are 0, so we may assume that p does not divide a or b . It is pretty easy to verify that the equation above is true modulo p using Euler's Criterion.

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \pmod{p}$$

But equivalence modulo p is not necessarily equality in the integers, so what do we do? Well, both sides of our desired equation must equal ± 1 , and since p is odd, we have $1 \not\equiv -1 \pmod{p}$ (or otherwise $2 \equiv 0 \pmod{p}$). This means if the two sides are equivalent modulo p , we must either have both sides equal to 1 or both sides equal to -1. This finishes the proof.

17.1, # 1

1. Evaluate the following Legendre symbols.

$$(a) \quad \left(\frac{3}{43}\right) = -\left(\frac{43}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

$$(b) \quad \left(\frac{2}{43}\right) = (-1)^{42 \cdot 44/8} = (-1)^{231} = -1$$

$$(c) \quad \left(\frac{3}{67}\right) = -\left(\frac{67}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

$$(d) \quad \left(\frac{2}{47}\right) = (-1)^{46 \cdot 48/8} = (-1)^{46 \cdot 6} = 1$$

$$(e) \quad \left(\frac{2}{41}\right) = (-1)^{40 \cdot 42/8} = (-1)^{5 \cdot 42} = 1$$

$$(f) \quad \left(\frac{6}{53}\right) = \left(\frac{2}{53}\right) \cdot \left(\frac{3}{53}\right) = (-1)^{52 \cdot 54/8} \cdot -\left(\frac{53}{3}\right) = -1 \cdot -\left(\frac{1}{3}\right) = 1$$

9.2, # 1, 6ac

1. Determine the set S_{2^r} with $p - 1 = 2^r s$, s odd, for the following primes.

(a) 17: First we notice that $17 - 1 = 16 = 2^4 \cdot 1$. Now S_{2^4} is a set with 2^4 integers relatively prime to p that are also distinct modulo 17. The only way that could be is if $S_{2^4} = \{1, 2, 3, \dots, p - 1\}$ modulo 17. Another way to see this is we usually choose a quadratic nonresidue, like 3 which is a primitive root. Then our set is $3^1, 3^2, \dots, 3^{p-1}$, which modulo 17 is the set of all integers relatively prime to 17.

(b) 57: 57 is not a prime number, so the methods here don't apply.

9.3, # 1ab

1. Determine if each of the following congruences has a solution. If the congruence has solutions, then find all the roots.

(a) $x^2 \equiv 61 \pmod{169}$: First we reduce this equation modulo 13 (as $169 = 13^2$), getting $x^2 \equiv -4 \equiv 9 \pmod{13}$, and we have $x \equiv \pm 3 \pmod{13}$ as solutions. To find the other solutions, we set $x_0 = \pm 3 + 13k$ and try to solve for k .

$$x_0^2 = 9 \pm 78k + 169k^2 \equiv 9 \pm 78k \equiv 61 \pmod{169}$$

Then we can simplify to get $\pm 78k \equiv 52 \pmod{169}$, and we can divide the whole equation by 13 and get an equation modulo 13. This is because the equation above means that there is some integer r such that $\pm 78k = 52 + 169r$, and dividing by 13 we get $\pm 6k = 4 + 13r$, so this means that $\pm 6k \equiv 4 \pmod{13}$. We multiply by ∓ 2 (the inverse of ± 6 modulo 13), and we get $k \equiv \pm 8 \pmod{13}$. We get possible solutions to the equation above are $\pm 3 \pm 13 \cdot 8 = \{\pm 101, \pm 107\}$, but only ± 101 are actually solutions.

(b) $x^2 \equiv 869 \pmod{961}$: We first reduce modulo 31 (as $961 = 31^2$), and we get $x^2 \equiv 1 \pmod{31}$, which only has solutions $x \equiv \pm 1 \pmod{31}$. We then let $x_0 = \pm 1 + 31k$ and solve for k .

$$x_0^2 = 1 \pm 62k + 961k^2 \equiv 1 \pm 62k \equiv 869 \pmod{961}$$

This simplifies to $\pm 62k \equiv 868 \pmod{961}$, which we can divide by 31 to get an equation modulo 13 as we did before, giving us $\pm 2k \equiv 28 \pmod{31}$, and we find that $k \equiv \pm 14 \pmod{31}$. Now we check the possibilities and find that $x_0 \equiv \pm 435 \pmod{961}$ are solutions.