

104B Problem Set 4

Rino Sanchez

February 20, 2003

14.4, # 2,4

2. A solution to the congruence $x^2 \equiv -1 \pmod{509}$ is given by $x = 301$. The number 509 is prime. This implies that $509 | (301^3 + 1)$, and $301^2 + 1 = 2 \cdot 89 \cdot 509$. Use this information to work through the method of descent to find a representation of 509 as a sum of two squares.

Here we basically use the method of descent that is explained in the proof of Proposition 14.4.6, by which we start with a number $n = x^2 + y^2$ that is divisible by 509 and step by step dividing a prime q from n , each time obtaining an expression of n/q as a sum of two squares. We start with $q = 2 = 1^2 + 1^2$ and $n = 2 \cdot 89 \cdot 509 = 301^2 + 1$.

$$\frac{n}{q} = \frac{(ax + by)^2 + (ay - bx)^2}{q^2} = \frac{302^2 + 300^2}{2^2} = 151^2 + 150^2$$

Now we proceed with $q = 89 = 8^2 + 5^2$, which is take from Example 14.4.8.

$$509 = \frac{(ax + by)^2 + (ay - bx)^2}{q^2} = \frac{(8 \cdot 151 + 5 \cdot 150)^2 + (8 \cdot 150 - 5 \cdot 151)^2}{89^2} = \frac{1958^2 + 445^2}{89^2} = 22^2 + 5^2$$

We happened to choose the right formula both times, because q divided $ax + by$ and $ay - bx$ each time, but if you check the other possible equations, we don't get integer expressions. To check that you chose the right formula, you only have to check that q divides either $ax + by$ or $ay + bx$ to see which formula to use. If you notice, the second formula simply exchanges x and y .

4. (Fermat, 1630) Show that 21 cannot be expressed as the sum of the squares of two **rational** numbers.

Suppose one can express $21 = (\frac{a}{b})^2 + (\frac{c}{d})^2$, which we can transform to $21b^2d^2 = (ad)^2 + (bc)^2$. Because $21b^2d^2$ is a sum of two squares, we can apply Theorem 14.4.10 to say that every prime divisor of $21b^2d^2$ of the form $4k + 3$ occurs to an even power in its factorization. Now consider the exponent of 3 in the prime factorization of $21b^2d^2$, which must be odd. This contradicts our previous statement, so our assumption that 21 can be expressed as a sum of two squares of rational numbers is not true, finishing the proof. If you think about this proof a little, you can see that any number that is not a sum of two squares of integers cannot be expressed as a sum of two squares of rational numbers either.

17.2, # 2,4,5ac, 7

2. Use Gauss's Lemma to evaluate $(\frac{5}{37})$.

We take the set $\{5, 10, 15, \dots, 900\}$ and reduce modulo 37 to get the smallest absolute value, like $\{5, 10, 15, -17, -12, -7, -2, 3, 8, 13, 18, -14, -9, -4, 1, 6, 11, 16\}$. There are 7 negative numbers there, so $(\frac{5}{37}) = -1$.

4. For the computation of $\left(\frac{3}{p}\right)$, find the number of multiples of 3 in the intervals $(p/2, p)$ and $(3p/2, 2p)$. By considering values of $p \pmod{12}$, determine when this number is even.

Here we follow the equations derived in the notes for Lecture 13. The number of multiples of 3 in the interval $(p/2, p)$ is the same as the number of integers in $(p/6, p/3)$, and the notes say that that number is $\lfloor p/3 \rfloor - \lfloor p/6 \rfloor$. Similarly the number of multiples of 3 in the interval $(3p/2, 2p)$ is $\lfloor 2p/3 \rfloor - \lfloor p/2 \rfloor$. If we replace p by r where $p \equiv r \pmod{12}$, say $p = r + 12k$, then we get

$$\left\lfloor \frac{p}{3} \right\rfloor - \left\lfloor \frac{p}{6} \right\rfloor = \left\lfloor \frac{r}{3} + 4k \right\rfloor - \left\lfloor \frac{r}{6} + 2k \right\rfloor = \left\lfloor \frac{r}{3} \right\rfloor - \left\lfloor \frac{r}{6} \right\rfloor + 2k \equiv \left\lfloor \frac{r}{3} \right\rfloor - \left\lfloor \frac{r}{6} \right\rfloor \pmod{2}$$

and similarly for our second expression. Now we can simply substitute the values of $p = 1, 5, 7, 11$ into the formulas to find all the possible values modulo 12.

$$\left\lfloor \frac{p}{3} \right\rfloor - \left\lfloor \frac{p}{6} \right\rfloor = \begin{cases} \left\lfloor \frac{1}{3} \right\rfloor - \left\lfloor \frac{1}{6} \right\rfloor = 0 - 0 = 0 & p = 1 \\ \left\lfloor \frac{5}{3} \right\rfloor - \left\lfloor \frac{5}{6} \right\rfloor = 1 - 0 = 1 & p = 5 \\ \left\lfloor \frac{7}{3} \right\rfloor - \left\lfloor \frac{7}{6} \right\rfloor = 2 - 1 = 1 & p = 7 \\ \left\lfloor \frac{11}{3} \right\rfloor - \left\lfloor \frac{11}{6} \right\rfloor = 3 - 1 = 2 & p = 11 \end{cases}$$

$$\left\lfloor \frac{2p}{3} \right\rfloor - \left\lfloor \frac{p}{2} \right\rfloor = \begin{cases} \left\lfloor \frac{2}{3} \right\rfloor - \left\lfloor \frac{1}{2} \right\rfloor = 0 - 0 = 0 & p = 1 \\ \left\lfloor \frac{10}{3} \right\rfloor - \left\lfloor \frac{5}{2} \right\rfloor = 3 - 2 = 1 & p = 5 \\ \left\lfloor \frac{14}{3} \right\rfloor - \left\lfloor \frac{7}{2} \right\rfloor = 4 - 3 = 1 & p = 7 \\ \left\lfloor \frac{22}{3} \right\rfloor - \left\lfloor \frac{11}{2} \right\rfloor = 7 - 5 = 2 & p = 11 \end{cases}$$

This means that the totals for each case is even.

5. Find congruences characterizing prime numbers p for which the following integers are quadratic residues.

(a) 15: First we use the fact that $\lfloor 15/p \rfloor = \lfloor 3/p \rfloor \cdot \lfloor 5/p \rfloor$. We know that $\lfloor 3/p \rfloor = 1$ if and only if $p \equiv \pm 1 \pmod{12}$, and $\lfloor 5/p \rfloor = 1$ if and only if $p \equiv 1, 9, 11, 19 \pmod{20}$. Solving for all the possibilities using the Chinese Remainder Theorem, we got solutions $p \equiv 1, 49, 11, 59 \pmod{60}$ (the 60 is from the g.c.d. of 12 and 20), so these are cases where $\lfloor 15/p \rfloor = 1$. The rest of the cases are where $\lfloor 3/p \rfloor = -1$ and $\lfloor 5/p \rfloor = -1$, which is when $p \equiv 5, 7 \pmod{12}$ and when $p \equiv 3, 7, 13, 17 \pmod{20}$ respectively. Again, we solve using the Chinese Remainder Theorem to arrive at the solutions $p \equiv 53, 17, 43, 7 \pmod{60}$.

(b) 7: Since $7 \equiv 3 \pmod{4}$, we have $\lfloor 7/p \rfloor = \lfloor p/7 \rfloor$ when $p \equiv 1 \pmod{4}$ and $\lfloor 7/p \rfloor = -\lfloor p/7 \rfloor$ when $p \equiv 3 \pmod{4}$. Then $\lfloor p/7 \rfloor = 1$ if and only if $p \equiv 1, 2, 4 \pmod{7}$. Thus for $p \equiv 1 \pmod{4}$, the solutions also satisfy $p \equiv 1, 2, 4 \pmod{7}$, and for $p \equiv 3 \pmod{4}$, the solutions also satisfy $p \equiv 3, 5, 6 \pmod{7}$ (the quadratic nonresidues modulo 7). This gives solutions $p \equiv 1, 9, 25, 3, 19, 27 \pmod{38}$.

7. Characterize all primes such that every quadratic nonresidue is also a primitive root.

The answer is those primes that are of the form $2^k + 1$. Euler's Criterion tells us that a is a quadratic nonresidue if and only if $a^{(p-1)/2} \equiv -1 \pmod{p}$, but since there are only two square roots of 1 modulo p (and also because $(a^{(p-1)/2})^2 = a^{p-1} \equiv 1 \pmod{p}$ by Fermat's Little Theorem), the equation $a^{(p-1)/2} \equiv -1 \pmod{p}$ is equivalent to $a^{(p-1)/2} \not\equiv 1 \pmod{p}$. The condition that a is a primitive root modulo p is that $a^{(p-1)/q} \not\equiv 1 \pmod{p}$ for every prime q that divides $p-1$. The difference between Euler's Criterion and this condition is that for Euler's Criterion you only need $a^{(p-1)/q} \not\equiv 1 \pmod{p}$ to hold for $q = 2$ (one reason that primitive roots are all quadratic nonresidues). Now if the only prime dividing $p-1$ is 2, then we have

$p = 2^k + 1$ for some $k \geq 0$. For these primes, any a satisfying $a^{(p-1)/2} \not\equiv 1 \pmod{p}$ also satisfies $a^{(p-1)/q} \not\equiv 1 \pmod{p}$ for primes q dividing $p-1$ (of which there is only $q = 2$).

Now p is not of the form $2^k + 1$, or equivalently, that some odd prime q divides $p-1$. Let g be a primitive root modulo p . Then consider g^q . We can easily see that g^q is not a primitive root because $(g^q)^{(p-1)/q} = g^{p-1} \equiv 1 \pmod{p}$, but g^q is a quadratic nonresidue because $(g^q/p) = (g/p)^q = (-1)^q = -1$. This finishes the proof that it is only modulo primes of the form $2^k + 1$ where we have every quadratic nonresidue also a primitive root.

17.3, # 1ac, 4

1. Evaluate the following Jacobi symbols

(a) $\left(\frac{45}{93}\right)$: We can just work this out by hand using the definition of the Jacobi Symbol:

$$\left(\frac{45}{93}\right) = \left(\frac{45}{3}\right) \cdot \left(\frac{45}{31}\right) = 0$$

(c) $\left(\frac{1054}{1069}\right)$: We can compute using quadratic reciprocity for Jacobi symbols (Theorem 17.3.5):

$$\left(\frac{1054}{1069}\right) = \left(\frac{2}{1069}\right) \cdot \left(\frac{17}{1069}\right) \cdot \left(\frac{31}{1069}\right) = -\left(\frac{1069}{17}\right) \cdot \left(\frac{1069}{31}\right) = -\left(\frac{-2}{17}\right) \cdot \left(\frac{-2}{31}\right) = -1 \cdot 1 \cdot -1 = 1$$