Number Theory

Homework 8

Kenny Roffo

Due April 4, 2016

1a) Let p be an odd prime. Show that the Diophantine equation

$$x^2 + py + a = 0 \qquad\qquad (a, p) = 1$$

has an integral solution if and only if $(-a/p) = 1$.

According to the quadratic formula, if the above equation has solutions x and y, then the following holds:

$$x = \frac{-0 \pm \sqrt{0^2 - 4(1)(py + a)}}{2(1)} = \pm\sqrt{-py - a}$$

That is, if the above equation has integer solutions x and y, then $x = \pm\sqrt{-py - a}$ (where x and y are integers).

$(\Rightarrow)$: Assume $x^2 + py + a = 0$ has integer solutions. Then $x = \pm\sqrt{-py - a}$. Thus $-py - a$ must be a perfect square, so there exists an integer n such that

$$n^2 = -py - a$$

This implies

$$\begin{aligned}
& p(-y) = n^2 + a \\
\Longrightarrow \quad & p|(n^2 + a) \\
\Longrightarrow \quad & n^2 \equiv -a \pmod{p} \\
\Longrightarrow \quad & (-a/p) = 1
\end{aligned}$$

$(\Leftarrow)$ Now assume $(-a/p) = 1$. Then there exists an integer n such that

$$\begin{aligned}
& (-a/p) = 1 \\
\Longrightarrow \quad & n^2 \equiv -a \pmod{p} \\
\Longrightarrow \quad & p|(n^2 + a) \\
\Longrightarrow \quad & pc = n^2 + a && (c \in \mathbb{Z}) \\
\Longrightarrow \quad & n^2 = -p(-c) - a \\
\Longrightarrow \quad & n^2 = -py - a && (y = -c)
\end{aligned}$$

That is, there exists an integer y such that $-py - a$ is a perfect square. Therefore $x = \sqrt{-py - a}$ is an integer, and so the equation

$$x^2 + py + a = 0$$

has integer solutions.

1b) Determine whether $x^2 + 7y - 2 = 0$ has a solution in the integers.

By 1a, the given equation has integer solutions if and only if $(2/7) = 1$. It was shown in class that $(2/p) = 1$ where p is prime if $p \equiv \pm 1 \pmod 8$. $7 \equiv -1 \pmod 8$, therefore indeed $(2/7) = 1$, so the given equation does have an integer solution.

2a) If p is an odd prime and $(ab, p) = 1$, prove that at least one of a, b or ab is a quadratic residue of p.

It was shown in class that if p is an odd prime, and a, b are integers such that $p \nmid a$ and $p \nmid b$ then $(ab/p) = (a/p)(b/p)$. Since $(ab, p) = 1$, $p \nmid ab$, thus $p \nmid a$ and $p \nmid b$, since p is prime (If p divided either one, then it would have to be the case that p divided their product). Thus the result discussed in class applies. Now, if either (a/p) or (b/p) is 1, then the result follows. If not, then we have

$$(ab/p) = (a/p)(b/p) = (-1)(-1) = 1$$

and the result still follows. Therefore, at least one of $(a/p), (b/p), (ab/p)$ must be 1.

2b) Given a prime p, show that, for some choice of $n > 0$, p divides

$$(n^2 - 2)(n^2 - 3)(n^2 - 6)$$

Consider $n = p + 1$. Then

$$n^2 - 2 = (p + 1)^2 - 2 = p^2 + 2p = p(p + 2)$$

So

$$p|(n^2 - 2)(n^2 - 3)(n^2 - 6)$$

if

$$p|p(p + 1)(n^2 - 3)(n^2 - 6)$$

which is obviously true.

3) Determine whether the following quadratic congruence is solvable:

$$x^2 \equiv 219 \pmod{419}$$

The above congruence is solvable if its corresponding Legendre symbol, $(219/419)$, is 1. We use the corollary to the Law of Quadratic Reciprocity to find this value (note that 419 is prime):

$$\begin{aligned}
(219/419) &= (73/419)(3/419) \\
&= (419/73)(3/419) && \text{By LQR} \\
&= (54/73)(3/419) \\
&= (54/73)(1) && \text{since } 419 \equiv -1 \pmod{12} \text{ by lemma presented in class} \\
&= (3/73)^3(2/73) \\
&= (1)^3(1) && \text{since } 73 \equiv 1 \pmod{12} \text{ and } 73 \equiv 1 \pmod 4 \\
&= 1
\end{aligned}$$

So the given quadratic congruence is solvable.

4) Let p, q be twin primes such that $x^2 \equiv p \pmod{q}$. Prove $x^2 \equiv q \pmod{p}$ is solvable.

Since p and q are twin primes, q is either $p+2$ or $p-2$. Note that all primes are of the form either $4k+1$ or $4k+3$. Whichever form p has, q must be of the other form. By the Law of Quadratic Reciprocity, we know

$$
\begin{aligned}
(p/q)(q/p) &= (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})} \\
&= (-1)^{(\frac{4k+1-1}{2})(\frac{4k+3-1}{2})} && \text{Note the order may have switched here} \\
&= (-1)^{(2k)(2k+1)} \\
&= 1
\end{aligned}
$$

That is, $(p/q)(q/p) = 1$ and since $(p/q) = 1$, this implies $(q/p) = 1$. Therefore, $x^2 \equiv q \pmod{p}$ is solvable.