18.781, Fall 2007 Problem Set 6

Solutions to Selected Problems

Problem 3.2.6 First note that 1009 is a prime number. We need to decide the value of $\left(\frac{150}{1009}\right)$. We can find that

$$\left(\frac{150}{1009}\right) = \left(\frac{2}{1009}\right)\left(\frac{3}{1009}\right)\left(\frac{25}{1009}\right).$$

Because $1009 \equiv 1 \pmod 8$, we have $\left(\frac{2}{1009}\right) = 1$.

By the theorem 3.5, with the fact that $1009 = 3 \cdot 336 + 1$, $\left(\frac{3}{1009}\right) = \left(\frac{1}{3}\right) = 1$.

Since 25 is a square number, $\left(\frac{25}{1009}\right) = 1$.

In conclusion, we have $\left(\frac{150}{1009}\right) = 1$. Therefore, the given equation is solvable. (Actually, $139^2 \equiv 150 \pmod{1009}$.) $\square$

Problem 3.2.7 First, it is easily observed that $x^2 \equiv 13 \pmod p$ has a solution when p is 2 or 13. Now assume that p is neither 2 nor 13. Then p is an odd prime, and we have

$$x^2 \equiv 13 \pmod p \text{ has a solution.} \Leftrightarrow \left(\frac{13}{p}\right) = 1. \Leftrightarrow \left(\frac{p}{13}\right)(-1)^{\frac{13-1}{2}\frac{p-1}{2}} = \left(\frac{p}{13}\right) = 1.$$

By a little computation, we can easily verify that the quadric residues of 13 are $\{1, 3, 4, 9, 10, 12\}$. Therefore, $\left(\frac{p}{13}\right) = 1$ if and only if $p \equiv 1, 3, 4, 9, 10, 12 \pmod{13}$.

Thus we can find that $x^2 \equiv 13 \pmod p$ has a solution when p is 2 or 13 or $p \equiv 1, 3, 4, 9, 10, 12 \pmod{13}$. $\square$

Problem 3.2.11 Suppose that $x^2 \equiv a \pmod{pq}$ is solvable. This implies that there exist a x satisfying $x^2 \equiv a \pmod p$, so it is absurd because a is a quadratic nonresidue of p. Therefore, $x^2 \equiv a \pmod{pq}$ is not solvable.

Problem 3.2.14 Suppose p, q are twin primes satisfying $q = p + 2$. Then clearly they are both odd, and one of the p, q is of the form $4k + 1$. Therefore, $(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1$. Hence we can find that

$$\begin{gathered}\text{There is an integer } a \text{ such that } p \mid (a^2 - q).\\ \Updownarrow \\ \left(\frac{q}{p}\right) = 1. \\ \Updownarrow \\ \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1. \\ \Updownarrow \\ \text{There is an integer } b \text{ such that } q \mid (a^2 - p).\end{gathered}$$

as desired. □

Problem 3.2.19 First suppose that p is a divisor of numbers of both of the forms m^2+1, n^2+2. By the exercise 3.1.20, we have $p \equiv 1 \pmod 4$ and $p \equiv 1$ or $3 \pmod 8$. Therefore, $p \equiv 1 \pmod 8$. By theorem 2.37, with $a = -1, n = 4$, we can conclude that $x^4 \equiv -1 \pmod p$ has a solution. That is equivalent to say that p is a divisor of some number of the form $k^4 + 1$.

Conversely, assume that p is a divisor of some number of the form $k^4 + 1$. Again by the exercise 3.1.20, we have $p \equiv 1 \pmod 8$. This implies that (by again same exercise) p is a divisor of numbers of both of the forms m^2+1, n^2+2, as desired. □

If you have any question, please contact me : Yoonsuk Hyun (yshyun@math.mit.edu)