18.781 Problem Set 9

Due Monday, November 21 in class. There will be no problem set due on November 28; the next set will be due on Monday, December 5.

1. Suppose that $p$ and $q$ are prime numbers, and $m$ is an integer.

   (a). If $p$ does not divide $q - 1$, prove that every element of $\mathbb{Z}/q\mathbb{Z}$ is a $p$th power. In particular, the equation
   \[ m \equiv x^p \pmod{q} \]
   always has a solution.

   (b). Suppose that $p$ divides $q - 1$, and that $m \not\equiv 0 \pmod{q}$. Prove that
   \[ m \equiv x^p \pmod{q} \]
   has a solution if and only if $m^{(q-1)/p} \equiv 1 \pmod{q}$.

2. Suppose that $p$ and $q$ are distinct odd primes. Prove that there is never a “primitive root modulo $pq$”; that is, there is no element of $(\mathbb{Z}/pq\mathbb{Z})^\times$ having order equal to $(p - 1)(q - 1)$.

3. Suppose that $p_1, \ldots, p_r$ are distinct prime numbers. Find the smallest positive integer $m$ leaving remainder $p_1 - 1$ on division by $p_1$, $p_2 - 1$ on division by $p_2$, \ldots, and $p_r - 1$ on division by $p_r$. Prove that your answer is correct.

4. Here is another way to state quadratic reciprocity. You can use quadratic reciprocity as stated in the text to do this problem.

   Suppose $p$ and $q$ are odd primes. Define $\epsilon_p = (-1)^{(p-1)/2}$. Prove that $\epsilon_p p$ is a square modulo $q$ if and only if $q$ is a square modulo $p$.

5. Problem 4 says that (for fixed $p$) the question of whether $\epsilon_p p$ is a square modulo $q$ depends only on the class of $q$ modulo $p$. How can this be consistent with the results of problems 9.8.3 and 9.8.4 in the text, where the answers depend on the class of $q$ modulo $4p$?