Homework 4

Theory of Numbers (Fall 2014)
Rutgers University
Swastik Kopparty

Due Date: Monday, November 17, 2014

Questions

1. Suppose p is a prime and $p \equiv 4k+3$. Let $a \in \mathbb{Z}_p$. We will see a simple way to compute the square root of a in $\mathbb{Z}_p$.

   Observe that $(p+1)/4$ is an integer. Let $b = a^{(p+1)/4} \mod p$.

   Prove that $b^2 \equiv a \mod p$.

   Thus compute the square root of 8 mod 23.

2. Let p and q be distinct odd primes. Let $n = p \cdot q$.

   Let $a \in \mathbb{Z}_n$. Show that a is a perfect square mod n if and only if $a \mod p$ is a perfect square mod p, and $a \mod q$ is a perfect square mod q.

   Thus compute the number of perfect squares in $\mathbb{Z}_n$.

3. Prove that $10^n \equiv 1 \mod 3$ for each $n \geq 0$.

   Use this to prove the correctness of the divisibility-by-3 test: a number m is divisible by 3 if and only if the sum of its digits (in the standard base-10 representation) is divisible by 3.

   Hint: Suppose the digits of m are $m_k m_{k-1} \cdots m_1 m_0$.

4. Compute the set of perfect cubes in each of: $\mathbb{Z}_5, \mathbb{Z}_7, \mathbb{Z}_{11}, \mathbb{Z}_{13}, \mathbb{Z}_{17}, \mathbb{Z}_{19}, \mathbb{Z}_{23}$. (Don't show your work, just list the cubes).

   Observe something about these sets, and make a conjecture.

5. **BONUS:** Show that the product of any 4 consecutive integers is divisible by 24.