MATH 350 ASSIGNMENT 10, SPRING 2017

Due in class on Monday, April 3

> Un phénomène dont la probabilité est 10^{-50} ne se produira donc jamais, ou du moins ne sera jamais observé. — Émile Borel, *Les probabilités et a vie*

Part 1.

1. For the cases $n = 77$ and $n = 385$, determine the number of elements $b \in \mathbb{Z}/n\mathbb{Z}$ such that $b^{n-1} \neq 1 \bmod n$. (It is the number of witnesses in $\mathbb{Z}/n\mathbb{Z}$ that n is not a prime number according to Fermat's little theorem.)

2. Let p be an odd prime number. Recall that we have shown in class that there exists an element $\xi \in (\mathbb{Z}/p^2\mathbb{Z})^\times$ such that every element of $(\mathbb{Z}/p^2\mathbb{Z})^\times$ can be written as ξ^a for a uniquely determined element $a \in \mathbb{Z}/p(p-1)\mathbb{Z}$. Use this fact to show that for every positive integer the equation
$$x^k = 1 \bmod p^2$$
has exactly $\gcd(k, p(p-1))$ solutions in $\mathbb{Z}/p^2\mathbb{Z}$.

   (Note: This question is closely related to the next one.)

3. Let n be an odd positive integer and let p be a prime number such that $n \equiv 0 \pmod{p^2}$.

   (a) Use problem 2 above to show that the number of elements of the set
$$\{x \in (\mathbb{Z}/p^2\mathbb{Z})^\times : x^{n-1} = 1 \bmod p^2\}$$
   is equal to $\gcd(p-1, n-1)$.

   (b) Show that the number of solutions of $x \in \mathbb{Z}/n\mathbb{Z}$ of the equation
$$x^{n-1} = 1 \mod n$$
   is at most $\frac{(p-1)n}{p^2} \leq \frac{n}{4}$.

Part 2. Extra credit problems

A. Suppose that p, q are two odd prime numbers, $p \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$. Let $n = p \cdot q$. Determine the number of Miller-Rabin witnesses mod n for n to be a composite number.

B. Let n be an odd positive composite integer. Show that at least $3/4$ of the elements of the set $\mathbb{Z}/n\mathbb{Z} \smallsetminus \{0 \bmod n\}$ are Miller-Rabin witnesses.

C. Estimate the *average* number of steps needed to compute the Legendre symbol $\left(\frac{a}{p}\right)$ for a given prime number p and a number $a < p$. both $\leq 2^n - 1$. The estimate should be expressed in n.

   [Note: In the course of answering this question you need to specify the precise meaning of "average".]