Boston University | Number Theory
Summer I 2009 | Kalin Kostadinov

Homework No.8

due 06/15/2009

Problem A: Compute $1234567^{1234} \pmod{15}$ and $123456^{123123} \pmod{77}$.

Problem B: In the lecture we computed that the odd primes for which -1 is a quadratic residue (QR) are the primes $p \equiv 1 \pmod 4$, that -2 is a QR modulo the primes $p \equiv 1 \pmod 8$ and the primes $p \equiv 3 \pmod 8$, and that -5 is a QR modulo the primes $p \equiv 1, 3, 7, 9 \pmod{20}$. Find out for which primes are each of $4, 5, 8$ and -3, respectively, quadratic residues?

Problem C: Euler theorem tells us that if we have two relatively prime natural numbers a and n, and look at the consecutive powers $a^1, a^2, a^3, \cdots$ modulo n, we will eventually get a power of a that is congruent to 1.
Write a program, that takes as an input two positive integers, a and n, checks whether they are relatively prime, and if they are, prints the smallest exponent k, such that $a^k \equiv 1 \pmod{n}$. (2 points)
For example, given $a = 2$ and $n = 7$ your program should print $k = 3$, since $2^1 \equiv 2 \pmod{7}$, $2^2 \equiv 4 \pmod{7}$, $2^3 \equiv 1 \pmod{7}$. Or, given $a = 3$ and $n = 8$ it should print $k = 2$. Or, given $a = 3$ and $n = 7$ it should print $k = 6$.
Modify this program to make a second program which takes as an input a positive integer n and prints all possible exponents k such that $a^k \equiv 1 \pmod{n}$ for some $a \in \mathbb{N}$. (3 points)
For example, for $n = 7$ you should get $k = 1, 2, 3, 6$ (for values of $a = 1, 6, 2, 3$ respectively) and for $n = 8$ you should get only $k = 1, 2$ since $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$.
Use this program and make a table with few columns, say one column for each $n = 5, 7, 6, 8, 9, 10, 11, 12, 14, 18, 21, 25$ and list in each column the values of k you get from the second program.
Use your data to make conjecture about the values could you see in column, i.e. write a statement like this:
Let $n \in \mathbb{N}$. If $k \in \mathbb{N}$ is such that $a^k \equiv 1 \pmod{n}$ for some $a \in \mathbb{N}$, then k has the property that _ _ _ (2 points)
Euler theorem tells us that $a^{\phi(n)} \equiv 1 \pmod{n}$ for $(a, n) = 1$.
The data in the table shows that for a given n there are a lot of values of a such that $a^k \equiv 1 \pmod{n}$ for some $k < \phi(n)$. In fact, there are some numbers n such that for <u>all</u> $a \in \mathbb{N}$, such that $(a, n) = 1$, $a^k \equiv 1 \pmod{n}$ for some k which is less than $\phi(n)$. The first such number is $n = 8$.
Make a conjecture describing which values of n fall in this category. Enlarge the table, if necessary, to test your conjecture. (3 points)

Problem D: Use Fermat's Little theorem to show that the rational fraction $\frac{1}{p}$, when represented as a decimal fraction, repeats its digits with period $p - 1$ (or a divisor of $p - 1$). (10 points)