Problem Set 4

Due on Monday, November 4, 2013.

Problem 1: Zero divisors

An element $a \in \mathbf{Z}_n - \{0\}$ is said to be a *zero divisor* modulo n if $ab \equiv 0 \pmod{n}$ for some $b \in \mathbf{Z}_n - \{0\}$.

(a) Explain why there are no zero divisors in $\mathbf{Z}_p$ when p is prime.

(b) Find a zero divisor in $\mathbf{Z}_{33}$.

(c) What is the value of the first element to repeat in the sequence

$$(5^1 \bmod 33), (5^2 \bmod 33), (5^3 \bmod 33), (5^4 \bmod 33), \ldots?$$

(d) Do you think it is possible to find a non-zero number $x \in \mathbf{Z}_{33}$ and a number $k \geq 0$ such that $x^k \equiv 0 \pmod{33}$? Why or why not? Would your answer change for some RSA modulus n other than 33?

(e) Suppose n is not required to be an RSA modulus. Can you find numbers n, x, k such that $x \not\equiv 0$ but $x^k \equiv 0 \pmod{n}$?

In all cases, justify your answers.

Problem 2: Greatest common divisor

The definition of *greatest common divisor* can be extended naturally to a sequence of numbers $(a_1, a_2, \ldots, a_k)$, not all of which are zero; namely, it is the largest integer $d \geq 1$ such that $d \mid a_j$ for all $j = 1, 2, \ldots, k$. Describe an efficient algorithm for computing $\gcd(a_1, \ldots, a_k)$, and explain why it computes the correct answer.

Problem 3: Euler's totient function

Compute $\phi(2600)$. Show your work.

Problem 4: Euler theorem

Compute $3^{699845} \bmod 2600$.

Problem 5: Extended Euclidean algorithm

Use the extended Euclidean algorithm to solve the Diaphantine equation

$$601x - 1251y = 1$$

Show the resulting table of triples as in slide 15 of lecture 12 notes.
[Note: You *may* write a program to produce the table if you wish, but these numbers are small enough to make it quite feasible to carry out the computation by hand or with the aid of a pocket calculator.]

Problem 6: Diffie-Hellman

[Textbook, p.216, problem 7.6.10]

Problem 7: Primitive roots

(a) Find a primitive root g of $p = 761$ and use the Lucas test to prove that you have one.

(b) Find a non-trivial[1] number $g \in \mathbf{Z}_{761}^*$ that fails to be a primitive root of p, and use the Lucas test to prove your answer correct.

[1] Non-trivial means $g \notin \{1, p-1\}$.