CONCEPTS OF MATHEMATICS, SUMMER 1 2014
ASSIGNMENT 9

Due Tuesday, June 24 at the beginning of class. Make sure to include your name, Andrew ID, *and the list of your collaborators* (if any) with your assignment. You may discuss problems with others, but you may *not* keep a written record of your discussions. Please refer to the syllabus for details.

Problem 1 (20 points)

Assume a, b, and n are integers. In this exercise, you will study the integer solutions of the equation $ax \equiv b \bmod n$.

(1) Show that the equation has an integer solution if and only if $\gcd(a, n)$ divides b.

(2) Show further that the integer solution is unique modulo n if and only if a and n are coprime. *Hint: first show that a has an inverse modulo n if and only if a and n are coprime.*

Problem 2 (20 points)

(1) Soldiers in an army are ordered to line up in rows of 5. Once this is done, three soldiers remain. Next, the soldiers are ordered to line up in rows of 7. Three soldiers remain once again. Finally, the soldiers are ordered to line up in rows of 11 and four soldiers remain. Given that the army has less than 500 soldiers, compute its size.

(2) Alice sends Bob the cyphertext $c = 36$. Assume c was encrypted using (the toy version of) the RSA cryptosystem seen in class. Bob's public key is $n = 51$ and $e = 3$.

   (a) Demonstrate that this public key is too small by finding the corresponding private key.

   (b) Find the secret number m that Alice encrypted as c.

Show all your work!

Problem 3 (20 points)

(1) Prove that the number:

1111111111222222222233333333334444444444555555555566666666667777777777
88888888889999999999995071

is divisible by 11 (the number consists of ten consecutive 1s, followed by ten consecutive 2s, ..., followed by ten consecutive 9s, followed by 5071).

(2) Show that in any month (including February, even in leap years), exactly one Tuesday must fall on a day that is a multiple of four (for example, this assignment is due on Tuesday June 24 = $6 \cdot 4$ and the other Tuesdays fall on the 3, 10, or 17 which are not divisible by 4).

Date: June 20, 2014.

Problem 4 (20 points)

Assume p is a prime, and let m be a natural number not divisible by p. For k an integer, write $r(k, p)$ for the remainder of the division of k by p. Using only Euclid's lemma (and without using the result seen in class on existence of inverse modulo p), prove that the function $f : \{0, 1, \ldots, p-1\} \to \{0, 1, \ldots, p-1\}$ given by $f(x) = r(mx, p)$ is a bijection. Use this to give another proof that m has an inverse modulo p. *Hint: First explain why it is enough to show f is an injection.*

Problem 5 (20 points): Wilson's theorem

(1) Assume that p is a prime. Show that if a is its own inverse modulo p, then either $a \equiv 1 \bmod p$, or $a \equiv -1 \bmod p$.

(2) Assume p is a natural number and $p \geq 2$. Show that p is prime if and only if $(p-1)! \equiv -1 \bmod p$. *Hint: To go from left to right, use that each factor in $(p-1)!$ must have an inverse which is also a factor in $(p-1)!$.*

Extra credit (20 points): Euler's totient function

For n a natural number, define:

$$\Phi_n := \{m \in [n] \mid m \text{ and } n \text{ are coprime}\}$$

Euler's totient function $\varphi : \mathbb{N} \to \mathbb{N}$ is defined by $\varphi(n) := |\Phi_n|$. For example, $\varphi(6) = 2$, as $\Phi_6 = \{1, 5\}$: 1 and 5 are the only numbers in $[6]$ coprime to 6. A larger example is $\varphi(28) = 12$: you should convince yourself that 1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, and 27 are all the numbers in $[28]$ that are coprime to 28.

(1) Show that for a prime p, $\varphi(p) = p - 1$.

(2) Show more generally that for a prime p and a natural number $k \geq 1$, $\varphi(p^k) = p^{k-1}(p-1)$.

(3) Show that for coprime natural numbers m and n, $\varphi(mn) = \varphi(m)\varphi(n)$. *Hint: Use the Chinese remainder theorem to see that there is a bijection between Φ_{mn} and $\Phi_m \times \Phi_n$.*

(4) For a natural number $n \geq 2$, give a formula for $\varphi(n)$ in terms of the prime factorization of n.

(5) Assume you have found a very efficient method to compute $\varphi(n)$. Explain how you can break the RSA cryptosystem.