COMP 2711H Discrete Mathematical Tools for Computer Science
Tutorial Problems: Number Theory and Cryptography

Problem 1. Determine the digit in the unit's place of the following numbers: (a) 3^{70}, and (b) 9^{1573}.

Problem 2. Use Euclid's extended GCD algorithm to find the multiplicative inverse in Z_{1009} for each of the following: (a) 17, (b)100, and (c) 777.

Problem 3. Show that if m is not prime, then at least $\sqrt{m}$ elements of Z_m do not have multiplicative inverses.

Problem 4. Prove that if $x^{n-1} \equiv 1$ (modulo n) for all integers x that are not multiples of n, then n is prime.

Problem 5. Prove that $n^{13} - n$ is divisible by 2730.

Problem 6. Show that any prime $p > 5$ divides infinitely many integers in the sequence $9, 99, 999, 9999, \ldots$.

Problem 7. Consider the system of congruences $x \equiv 4 \pmod 6$ and $x \equiv 13 \pmod{15}$. Find all solutions to this system of congruences using two different methods: (a) the method of back substitution and (b) the method suggested by the construction used in the proof of the Chinese remainder theorem. (*Hint:* It may be convenient to first transform the congruences to equivalent congruences modulo suitable prime numbers.)

Problem 8. Prove that an integer $n > 1$ is prime if and only if the following holds: $(n-1)! \equiv -1 \pmod n$. (This is known as Wilson's theorem.)

Problem 9. Prove by induction that

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2.$$

In other words, the sum of the cubes of the first n integers is the square of the sum of these n integers.