SPCS CRYPTOGRAPHY
HOMEWORK 4

Please try all the unmarked problems. #, ⋆ problems are both optional, with ⋆ problems being harder. You are strongly encouraged to work in groups, but you have to write up the solution on your own.

Reference for today's lecture: Chapter 6.3, 9.3 of textbook. For the graph cryptosystem, see http://csunplugged.org/wp-content/uploads/2014/12/unplugged-18-public_key_encryption_0.pdf

1. For $p > 2$ prime, we always have $gcd(2, p) = 1$, so Fermat's little theorem says that
$$2^{p-1} \equiv 1 \bmod p$$
Try to compute $2^{560} \bmod 561$. Is 561 a prime?

2. Let p be a prime, and a be an integer. Define the Legendre symbol
$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \text{ divides } a \\ 1 & \text{if } a \text{ is a square/quadratic residue modulo } p \\ -1 & \text{if } a \text{ is not a square/quadratic residue modulo } p \end{cases}$$
Compute
   (a) Compute $\left(\frac{3}{5}\right)$, $\left(\frac{7}{5}\right)$, $\left(\frac{11}{5}\right)$ and $\left(\frac{13}{5}\right)$.
   (b) Compute $\left(\frac{5}{3}\right)$, $\left(\frac{5}{7}\right)$, $\left(\frac{5}{11}\right)$ and $\left(\frac{5}{13}\right)$.
   (c) Can you guess a relationship between $\left(\frac{p}{5}\right)$ and $\left(\frac{5}{p}\right)$ for a prime $p \neq 5$?

3. Let $p > 2$ be a prime. Show that -1 is a square modulo p if and only if $p \equiv 1 \bmod 4$.

\# 4. Fill in the details of the following proof that there are infinitely many primes $\equiv 1 \bmod 4$.
Suppose not. Assume that $p_1, \cdots, p_k$ are all the possible primes $p \equiv 1 \bmod 4$. Consider
$$N = 4(p_1 \cdots p_k)^2 + 1$$
and let $p|N$ be a prime factor.
   (a) Show that p cannot be one of $p_1, \cdots, p_k$.
   (b) Show that -1 is a square modulo p.
   (c) Hence show that $p \equiv 1 \bmod 4$. You just found a prime which is $\equiv 1 \bmod 4$, yet is not among the primes $p_1, \cdots, p_k$ we listed. Contradiction.

5. (a) Find a primitive root g for 7. For your choice of primitive root, what powers of g would give you another primitive root?
   (b) Do the same exercise with 7 replaced by 11.
⋆ (c) Let p be a prime, and g be a primitive root. Based on the last two parts, make a guess about what k would g^k be another primitive root. Can you prove your guess? Thus try to find the number of primitive roots mod p.

6. Let $p > 2$ be a prime.
   (a) Find the number of elements of $(\mathbb{Z}/p^2\mathbb{Z})^*$.

(b) Given that $(\mathbb{Z}/p^2\mathbb{Z})^*$ (under multiplication) has a generator, devise a test to check whether $a \bmod p^2$ is a square modulo p^2.

7. Find a primitive root modulo 31.

   You may use a computer - Sage is free, open source mathematical software that is particularly useful in number theory. You can use it online at http://cloud.sagemath.com. See http://www.math.ucla.edu/~gschaeff/crypto/SageWorksheet.pdf for a quick introduction.

   (For those who know Python, syntax of Sage is very similar to Python.)

8. (a) Design your own "good graph". Put your name on the graph and put it on the board.
   (b) Find a friend and send him/her a message, using his/her public key (the good graph). You may encode A by 11, B by 12 and so on. For example, HI is encoded as 1819. Send them in groups of 2. For example, $HIJOHN$ would be sent by three messages 1819, 2025, 1824.
   (c) Challenge another friend to decipher your message. Hopefully that friend would be in despair trying to do so.