SPCS CRYPTOGRAPHY
HOMEWORK 7

Please try all the unmarked problems. #, $\star$ problems are both optional, with $\star$ 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 10.5 - 10.6; For primality testing, see http://www.akalin.cx/intro-primality-testing

1. Using a calculator/Sage/otherwise, check by Fermat's test for $x = 2$ and 3 whether the following are primes.
   (a) 601
   (b) 2047
   (c) 294409

2. Repeat the last exercise, with Miller-Rabin test instead.

3. It is known that 503 is a prime with 5 being a primitive root modulo 503. Using Shank's baby-step-giant-step algorithm, find an x such that
$$5^x \equiv 193 \bmod 503$$

4. It is known that 8641 is a prime with 17 being a primitive root modulo 8641. Using Pohlig-Hellman algorithm, find an x such that
$$17^x \equiv 2108 \bmod 8641$$

5. Recall that *Carmichael numbers* n are integers that are not prime, but for any $(a, n) = 1$, $a^{n-1} \equiv 1 \bmod n$. They are those that would likely fool the Fermat test.
   (a) We said that 561 is a Carmichael number but we never actually checked it. Using Chinese remainder theorem, check that 561 is a Carmichael number, i.e. for all $(a, 561) = 1$,
$$a^{560} \equiv 1 \bmod 561.$$
   (Hint: $561 = 3 \cdot 11 \cdot 17$.)
   (b) Korselt's criterion says that a composite integer n is a Carmichael number if and only if n is odd, square-free and $p - 1 | n - 1$ for all $p | n$. Use it to check that 561 is a Carmichael number.
   $\star$ (c) Prove Korselt's criterion.

$\star$ 6. In Pohlig-Hellman, we showed two ways of calculating $k \bmod q^m$ for a prime q and integer m such that $q^m | p - 1$:
   - Directly consider q^m-th power test.
   - First calculate $k \bmod q$, then $k \bmod q^2$, ..., all the way to $k \bmod q^m$.

   Compare the time complexity of these two methods for fixed q and changing m.

$\star$ 7. If n is a positive integer, The *n-th factorial* $n!$ means $n \times (n-1) \times \cdots \times 1$.
   (a) If n is a composite number, show that $(n-1)! \equiv 0 \bmod n$.
   (b) If $n = p$ is a prime number, show that $(p-1)! \equiv -1 \bmod p$. This is *Wilson's theorem.*
   (c) Design a primality test using Wilson's theorem. What is the running time?