Math 173A - Homework 3

1. Do the following exercises from the textbook. 2.17, 2.18a and d, 2.21, 2.25, 2.27.

2. Let $p = 601$, which is prime.

   (a) Show that if an integer $r < 600$ divides 600, then it divides at least oone of 300, 200, 120 (these numbers are 600/2, 600/3, and 600/5).

   (b) Show that if the order of 7 in $\mathbb{F}_{601}$ is less than 600, then it divides one of the numbers 300, 200, 120.

   (c) A calculation shows that

   $$7^{300} \equiv 600, \quad 7^{200} \equiv 576 \quad 7^{120} \equiv 423 \pmod{601}.$$

   Why can we conclude that the order of 7 does not divide 300, 200, or 120?

   (d) Show that 7 is a primitive root in $\mathbb{F}_{601}$.

   (e) In general, suppose p is a prime and $p - 1 = q_1^{e_1} q_2^{e_2} \cdots q_s^{e_s}$ is the factorization of $p - 1$ into primes. Describe a procedure to check whether a number g is a primitive root mod p.

3. Let $p \equiv 3 \pmod 4$ be a prime. Show that $x^2 \equiv -1 \pmod p$ has no solutions. *Hint: Suppose a solution x exists. Raise both sides to the power $(p-1)/2$.*