HOMEWORK 3

For this week, please answer the following questions from the text. I've copied the problem itself below and the question numbers for your convenience.

(1) (1.19) Suppose that $g^a \equiv 1 \mod m$ and $g^b \equiv 1 \mod m$. Prove that

$$g^{\gcd(a,b)} \equiv 1 \mod m$$

(2) (1.27) Consider the congruence

$$ax \equiv c \mod m$$

(a) Prove that there is a solution if and only if $\gcd(a, m)$ divides c.
(b) If there is a solution, prove that there are exactly $\gcd(a, m)$ distinct solutions.

(Hint: Use the extended Euclidean algorithm.)

(3) (1.28) Let $\{p_1, \dots, p_r\}$ be a set of prime numbers and let

$$N = p_1 \cdots p_r + 1$$

Prove that N is not divisible by any of the p_i. Use this fact to conclude there are infinitely many prime numbers.

(4) (1.32) For each of the following primes p and numbers a, compute $a^{-1} \mod p$ in two ways: (i) Use the extended Euclidean algorithm. (ii) Use the fast power algorithm and Fermat's little theorem.
(a) $p = 47$ and $a = 11$
(b) $p = 587$ and $a = 345$
(c) $p = 104801$ and $a = 78467$

(5) (1.36) This exercise begins the study of squares and square roots modulo p.
(a) Let p be an odd prime number and let b be an integer with $p \not| b$. Prove that either b has two square roots modulo p or else b has no square roots modulo p. In other words, prove that the congruence

$$X^2 \equiv b \mod p$$

has either two solutions or no solutions in $\mathbb{Z}/p\mathbb{Z}$. (What happens for $p = 2$? What happens if $p \mid b$?)
(b) For each the following values of p and b, find all the square roots of b modulo p.
(i) $(p, b) = (7, 2)$
(ii) $(p, b) = (11, 5)$
(iii) $(p, b) = (11, 7)$
(iv) $(p, b) = (37, 3)$
(c) How many square roots does 29 have modulo 39? Why doesn't this contradict ' assertion in (a)?
(d) Let p be an odd prime and let g be a primitive root modulo p. Then any number a is equal to some power g modulo p, say $a \equiv g^k \mod p$. Prove that a has a square root modulo p if and only if k is even.