HOMEWORK 6

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) (2.18) Solve each of the following simultaneous systems of congruences (or explain why no solution exists).
   (a) $x = 3 \mod 7$ and $x = 4 \mod 9$
   (b) $x = 137 \mod 423$ and $x = 87 \mod 191$
   (c) $x = 133 \mod 451$ and $x = 237 \mod 697$
   (d) $x = 5 \mod 9$, $x = 6 \mod 10$, and $x = 7 \mod 11$
   (e) $x = 37 \mod 43$, and $x = 22 \mod 49$, and $x = 18 \mod 71$.

(2) (2.21)
   (a) Let a, b, c be positive integers and suppose that
   $$a \mid c, b \mid c, \text{and } \gcd(a, b) = 1$$
   Prove that $ab \mid c$.
   (b) Let c and c' be two solutions to the system of simultaneous congruences (2.7) in the Chinese remainder theorem (Theorem 2.24). Prove that
   $$c = c' \mod m_1 m_2 \cdots m_k$$

(3) (2.23) Use the method described in Sect. 2.8.1 to find square roots modulo the following composite moduli.
   (a) Find a square root of 340 modulo 437. (Note that $437 = 19 \cdot 23$.)
   (b) Find a square root of 253 modulo 3143.
   (c) Find four square roots of 2833 modulo 4189. (The modulus factors as $4189 = 59 \cdot 71$. Note that your four square roots should be distinct modulo 4189.)
   (d) Find eight square roots of 813 modulo 868.

(4) (2.25) Suppose $n = pq$ with p and q distinct odd primes.
   (a) Suppose that $\gcd(a, pq) = 1$. Prove that if the equation $x^2 = a \mod n$ has any solution then it has four solutions.
   (b) Suppose that you have a machine that could find all four solutions for some a. How could you use this machine to factor n?

(5) (2.28) Use the Polig-Hellman algorithm (Theorem 2.31) to solve the discrete logarithm problem
   $$g^x = a \mod p$$
   in each of the following cases.
   (a) $p = 433$, $g = 7$, $a = 166$
   (b) $p = 746497$, $g = 10$, $a = 243278$
   (c) $p = 41022299$, $g = 2$, $a = 39183497$ (Hint: $p = 2 \cdot 29^5 + 1$.)
   (d) $p = 1291799$, $g = 17$, $a = 192988$ (Hint: $p - 1$ has a factor of 709).