Worksheet 4.3 & 4.4 - Primes and Greatest Common Divisors and Solving Congruences

1. Determine whether the integers in each of these sets is pairwise relatively prime.
   (a) 11, 15, 19
   (b) 14, 15, 21
   (c) 12, 17, 31, 37
   (d) 7, 8, 9, 11

2. What are the greatest common divisors and least common multiple of these pairs of integers?
   (a) $3^7 \cdot 5^3 \cdot 7^3$, $2^{11} \cdot 3^5 \cdot 5^9$
   (b) $11 \cdot 13 \cdot 17$, $2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$
   (c) 23^{31}, 23^{17}
   (d) $41 \cdot 43 \cdot 53$, $41 \cdot 43 \cdot 53$
   (e) $3^{13} \cdot 5^{17}$, $2^{12} \cdot 7^{21}$
   (f) 1111, 0

3. Use the Euclidean algorithm to find
   (a) $\gcd(1, 5)$.
   (b) $\gcd(123, 277)$.
   (c) $\gcd(1529, 14038)$.
   (d) $\gcd(100, 101)$.
   (e) $\gcd(1529, 14039)$.
   (f) $\gcd(11111, 111111)$.

4. Show that 15 is an inverse of 7 modulo 26.

5. Find an inverse of a modulo m for each of these pairs of relatively prime integers.
   (a) $a = 2$, $m = 17$
   (b) $a = 34$, $m = 89$

6. Solve each of these congruences using the modular inverses found in parts (b), of Exercise 5.

$$34x \equiv 77 \mod 89$$

7. Use the construction in the proof of the Chinese remainder theorem to find all solutions to the system of congruences

$$x \equiv 1 \mod 2,$$

$$x \equiv 2 \mod 3,$$

$$x \equiv 3 \mod 5,$$

and

$$x \equiv 4 \mod 11.$$

8. Use Fermats little theorem to find $712 \mod 13$.

9. Find the discrete logarithms of 5 and 6 modulo 19 to the base 2.