PROBLEM SET 13: EXTENDED GCD, FERMAT'S LITTLE THEOREM

1. Let a and b be integers, not both 0. Define gcd(a, b).
2. Find gcd(2584, 1597)
3. Prove that gcd(a, b) = gcd(a – kb, b) for any integer, k.
4. Using the extended Euclidean algorithm, find integers x and y such that ax + by = gcd(a, b) when:

   (A) a = 34, b = 459

   (B) a = 272, b =4356

   (C) a = 156 b = 572
5. Using the extended Euclidean algorithm, find integers x and y such that 3789406027x + 18272779829y = gcd(37894060279, 18272779829). Of course, the calculation below is of great help.

$$\begin{aligned}
37894060279 &= 2 \times 18272779829 + 1348500621 \\
18272779829 &= 13 \times 1348500621 + 742271756 \\
1348500621 &= 1 \times 742271756 + 606228865 \\
742271756 &= 1 \times 606228865 + 136042891 \\
606228865 &= 4 \times 136042891 + 62057301 \\
136042891 &= 2 \times 62057301 + 11928289 \\
62057301 &= 5 \times 11928289 + 2415856 \\
11928289 &= 4 \times 2415856 + 2264865 \\
2415856 &= 1 \times 2264865 + 150991 \\
2264865 &= 15 \times \underline{150991} + 0
\end{aligned}$$

2. State the well-ordering principle.

3. State and prove the division algorithm.

4. Let a and b be integers, not both 0. Prove that there exist integers x and y such that ax + by = gcd(a, b)
.
5. Give Euclid's proof that there exist infinitely many primes.

6. Prove Pythagoras′ theorem that $\sqrt{2}$ is irrational.

7. Prove that a and b are relatively prime if and only if there exist integers x, y for which $ax + by = 1$.

8. Euclid's lemma: Prove that if c divides ab and c is prime then c divides a or c divides b.
Is this statement still true if one removes the hypothesis that c is prime?
What if one assumes that $\gcd(b, c) = 1$?

9. State Fermat's theorem.

10. Using Fermat's theorem show that 17 is a divisor of $11^{104} + 1$.

11. State the Fundamental Theorem of Arithmetic.

12. Given non-zero integer a, prove that $\gcd(a, a+1) = 1$