Chapter 4.3: The Euclidean Algorithm

Thursday, July 9

Prime Factorizations and gcds

1. Find the prime factorization of 210.
2. Find the prime factorization of 10!
3. Find the prime factorization of 241.
4. How many zeroes does 50! end in?
5. Find the gcd and lcm of each of the following pairs of numbers:

   (a) 13, 39
   (b) 24, 16
   (c) 180, 50
   (d) $2 \cdot 5 \cdot 7 \cdot 11^2, 2^3 \cdot 5^2 \cdot 11$

6. Prove: if $\gcd(a,b) = 1$ and $\gcd(a,c) = 1$ then $\gcd(a,bc) = 1$.
7. Prove: if $p \geq 5$ then $p, p+2$, and $p+4$ cannot all be prime.
8. Prove: For every a, $\gcd(a,0) = |a|$.
9. Prove: For every a, $\gcd(a,a) = |a|$.

Euclidean Algorithm

1. Prove the key lemma in the Euclidean algorithm: $\gcd(qb + r, b) = \gcd(r, b)$. (Hint: Let $d = \gcd(r, b)$ and let $e = \gcd(qb + r, b)$. Show that $d \leq e$ and $e \leq d$ using the definition of gcd.)
2. Use the Euclidean Algorithm to find a solution to $17a + 5b = 1$.
3. Find infinitely many solutions to $17a + 5b = 1$.
4. Use the Euclidean Algorithm to find a solution to $21a + 8b = 1$.
5. Is there a number n such that $7n \equiv 1 \pmod{24}$?
6. Is there a number n such that $15n \equiv 1 \pmod{24}$?

The Prime Property

1. Prove that 0 has the prime property (if $p|ab$ then $p|a$ or $p|b$).
2. Prove that 1 has the prime property.
3. Show that if $5|n$ and $7|n$ then $35|n$.
4. Prove that p is prime if and only if $\mathbb{Z}_p$ has the following property: if $ab = 0$ in $\mathbb{Z}_p$, then $a = 0$ or $b = 0$.
5. Given that 101 is prime, find all solutions to $x^2 \equiv 1 \pmod{101}$.
6. Find all solutions to $x^2 \equiv 1 \pmod{8}$.
7. Find all solutions to $x^2 + 3x \equiv 9 \pmod{11}$.

Miscellany

1. True or False: if $a \equiv b \pmod{24}$ then $a \equiv b \pmod{6}$ and $a \equiv b \pmod{4}$.
2. True or False: If $a \equiv b \pmod{6}$ and $a \equiv b \pmod{4}$ then $a \equiv b \pmod{24}$.
3. Show that if $a|n$ and $b|n$ then $lcm(a, b)|n$.
4. Show that the gap between consecutive prime numbers can be arbitrarily large. (Hint: Consider 10!. What can you say about $10! + 2, 10! + 3, \ldots, 10! + 10$?)
5. Show that if a and b are both positive integers then $(2^a - 1) \pmod{2^b - 1} = 2^{a \bmod b} - 1$.
6. Show that if a and b are positive integers then $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$.