Chapter 4.3: The Euclidean Algorithm

Thursday, July 9

Prime Factorizations and gcds

1. Find the prime factorization of 210.
$$210 = 2 \cdot 3 \cdot 5 \cdot 7$$

2. Find the prime factorization of 10!
$$10! = 2^8 \cdot 3^3 \cdot 5^2 \cdot 7$$

3. Find the prime factorization of 241.
$$241 = 241$$

4. How many zeroes does 50! end in?

   The prime factorization of 50! includes the terms 2^47 and 5^12. Since an ending zero is a sign that the number is divisible by $10 = 2 \cdot 5$, 50! ends in 12 zeroes.

5. Find the gcd and lcm of each of the following pairs of numbers:

   (a) 13, 39
   gcd(13,39) = 13, lcm(13,39) = 39

   (b) 24, 16
   gcd(24,16) = 8, lcm(24,16) = 48

   (c) 180, 50
   gcd(180,50) = 30, lcm(180,50) = 900

   (d) $2 \cdot 5 \cdot 7 \cdot 11^2, 2^3 \cdot 5^2 \cdot 11$
   gcd $= 2 \cdot 5 \cdot 11$, lcm $= 2^3 \cdot 5^2 \cdot 7 \cdot 11^2$

6. Prove: if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$ then $\gcd(a, bc) = 1$.

   If $\gcd(a, b) = \gcd(a, c) = 1$ then there exist m, n such that $am + bn = 1$ and s, t such that $as + ct = 1$. Multiplying the first equality by ct gives $amct + bnct = ct$, so $as + amct + bnct = as + ct$ and so $a(s + mct) + bc(nt) = 1$, which implies that $1 = \gcd(a, bc)$.

   Alternately: There are x and y such that $bx \equiv cy \equiv 1 \pmod a$, so $(yx)bc \equiv y(xb)c \equiv yc \equiv 1 \pmod a$. Since bc has a multiplicative inverse mod a, $\gcd(a, bc) = 1$.

7. Prove: if $p \geq 5$ then $p, p + 2$, and $p + 4$ cannot all be prime.

   At least one of the three terms must be divisible by 3: if $p = 3n$ then p is divisible by 3, if $p = 3n + 1$ then $3|p + 2$, and if $p = 3n + 2$ then $3|p + 4$. Since $p \geq 5$ the term divisible by 3 must be composite.

8. Prove: For every a, $\gcd(a, 0) = |a|$.

   $a|a$ and $-a|a$ for any a, and $a|0$ for any a, so $|a|$ is a common divisor of a and 0. It must be the largest since if $d|a$ then $|d| \leq |a|$.

9. Prove: For every a, $\gcd(a, a) = |a|$.

   $|a|$ is a commond divisor. It must be the largest since if $d|a$ then $|d| \leq |a|$.

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 $d \le e$ and $e \le d$ using the definition of gcd.)

   Let $d = \gcd(qb+r,b)$ and let $e = \gcd(r,b)$. Since $d|(qb+r)$ and $d|b$ it follows that $d|r$. This means that d is a common divisor of r and b, so $d \le e$ since e is by definition the greatest common divisor of r and b.

   Similarly, $e|r$ and $e|b$, so $e|(qb+r)$. e is therefore a common divisor of $qb+r$ and b, meaning that $e \le d$ (since d is the greatest common divisor of $qb+r$ and b).

2. Use the Euclidean Algorithm to find a solution to $17a + 5b = 1$.

$$
\begin{aligned}
17 &= 3 \cdot 5 + 2 \\
5 &= 2 \cdot 2 + 1 \\
5 - 2 \cdot 2 &= 1 \\
17 - 3 \cdot 5 &= 2 \\
5 - 2 \cdot (17 - 3 \cdot 5) &= 1 \\
7 \cdot 5 - 2 \cdot 17 &= 1
\end{aligned}
$$

3. Find infinitely many solutions to $17a + 5b = 1$.

   Use the fact that $17 \cdot (-5k) + 5 \cdot (-17k) = 0$ for any k.

4. Use the Euclidean Algorithm to find a solution to $21a + 8b = 1$.

$$
\begin{aligned}
21 - 2 \cdot 8 &= 5 \\
8 - 5 &= 3 \\
5 - 3 &= 2 \\
3 - 2 &= 1 \\
3 - (5 - 3) &= 1 \\
2 \cdot 3 - 5 &= 1 \\
2 \cdot (8 - 5) - 5 &= 1 \\
2 \cdot 8 - 3 \cdot 5 &= 1 \\
2 \cdot 8 - 3 \cdot (21 - 2 \cdot 8) &= 1 \\
8 \cdot 8 - 3 \cdot 21 &= 1
\end{aligned}
$$

5. Is there a number n such that $7n \equiv 1 \pmod{24}$?

   Yup... $7 \cdot 7 = 49 \equiv 1 \pmod{24}$.

6. Is there a number n such that $15n \equiv 1 \pmod{24}$?

   No, since $3 = \gcd(15, 24)$ but 1 is not divisible by 3.

The Prime Property

1. Prove that 0 has the prime property (if $p|ab$ then $p|a$ or $p|b$).

   If $0|ab$ then $ab = 0$, so $a = 0$ or $b = 0$, so $0|a$ or $0|b$.

2. Prove that 1 has the prime property.

   Trivially, since $1|a$ for any a.

3. Show that if $5|n$ and $7|n$ then $35|n$.

   Let $n = 5k$ and $n = 7j$. Then $5k = 7j$, so (since 5 has the prime property) $5|j$. We can then write $j = 5m$, so $n = 7j = 7 \cdot 5m = 35m$ for some m, meaning $35|n$.

4. Prove that $p \geq 2$ is prime if and only if $\mathbb{Z}_p$ has the following property: if $ab = 0$ in $\mathbb{Z}_p$, then $a = 0$ or $b = 0$.

   Written in terms of modular arithmetic, this is the same as the prime property: if $p|ab$ then $p|a$ or $p|b$.

   Proof that all primes have the prime property: Say that $p|ab$. If $p|a$ then we are done. If $p \nmid a$ then $\gcd(a, p) = 1$, so $p|b$.

   Proof that composite numbers do not have the prime property: If m is composite then $m = nc$ for some $n, c \geq 2$. Then $m|nc$ but $m \nmid n$ and $m \nmid c$.

5. Given that 101 is prime, find all solutions to $x^2 \equiv 1 \pmod{101}$.

   If $x^2 \equiv 1 \pmod{101}$ then $(x+1)(x-1) = x^2 - 1 \equiv 0 \pmod{101}$, so by the above result $(x+1) \equiv 0 \pmod{101}$ or $x - 1 \equiv 0 \pmod{101}$. Therefore, $x \equiv \pm 1 \pmod{101}$.

   We can then check that both of these solutions work.

6. Find all solutions to $x^2 \equiv 1 \pmod 8$.

   1,3,5,7 are all solutions.

7. Find all solutions to $x^2 + 3x \equiv 9 \pmod{11}$.

   If $x^2 + 3x \equiv 9 \pmod{11}$ then adding 2 to both sides gives $(x+1)(x+2) = x^2 + 3x + 2 \equiv 0 \pmod{11}$. Since 11 is prime, this means that $x \equiv -1 \pmod{11}$ or $x \equiv -2 \pmod{11}$.

   So the only two solutions with $0 \leq x < 11$ are $x = 9$ and $x = 10$.

Miscellany

1. True or False: if $a \equiv b \pmod{24}$ then $a \equiv b \pmod 6$ and $a \equiv b \pmod 4$.

   True. If $a = b + 24k$ then $a = b + 4 \cdot (6k) = b + 6 \cdot (4k)$.

2. True or False: If $a \equiv b \pmod 6$ and $a \equiv b \pmod 4$ then $a \equiv b \pmod{24}$.

   False: $a = 0, b = 12$ is a counterexample.

3. Show that if $a|n$ and $b|n$ then $lcm(a, b)|n$.

   Let $l = lcm(a, b)$. Proof by contradiction: Suppose $l \nmid n$. Then we can use the Division Algorithm to write $n = ql + r$ with $0 \leq r < l$. But since $a|n$ and $a|l$, it follows that $a|r$, and similarly $b|r$. This would mean that r is a common multiple of a and b that is smaller than l... a contratiction.

   Therefore our assumption that $l \nmid n$ was incorrect.

4. Show that the gap between consecutive prime numbers can be arbitrarily large. (Hint: Consider 10!. What can you say about $10! + 2, 10! + 3, \ldots, 10! + 10$?)

   Since $n! = 1 \cdot 2 \cdot \ldots \cdot n$, for any $2 \leq k \leq n$, $k|(n! + k)$, so there are $(n-1)$ composite numbers in a row after $n!$.

5. Show that if a and b are both positive integers then $(2^a - 1) \pmod{2^b - 1} = 2^{a \bmod b} - 1$.

   Use the fact that by the factorization of $x^n - 1$ in general, $2^{nk} - 1$ is divisible by $2^k - 1$ for any n.

   Let $a = qb + r$, so that $r = a$ mod b. Then

$$\begin{aligned} 2^a - 1 &= 2^{qb+r} - 1 \\ &= 2^{qb} \cdot 2^r - 2^r + 2^r - 1 \\ &= 2^r(2^{qb} - 1) + 2^r - 1 \\ &\equiv 2^r - 1 \pmod{b} \end{aligned}$$

6. Show that if a and b are positive integers then $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$.

   Comes from using the Euclidean algorithm on $2^a - 1$ and $2^b - 1$ and combining with the previous result.