J/STOW #4: Prime Numbers, Greatest Common Divisor, and Least Common Multiple

Zed Li

November 1, 2019

1 Basic principles

Note: All variables represent integers unless otherwise noted.

Do NOT memorize these properties. Rather, UNDERSTAND them INTUITIVELY. Then you wouldn't have to remember any of the properties to know them and know when to use them. (You do need to remember definitions though.)

1. A *factor* or *divisor* m of n is defined such that there exists k such that $n = km$. We then say that n is *divisible by* m or m *divides* n. We write $m \mid n$ to indicate that m is a divisor of n, while we write $m \nmid n$ to indicate that m is not a divisor of n. For example, $2 \mid 6, -14 \mid 42$ and $67 \mid 0$.

   Properties:

   (a) If $a \mid b$ and $b \mid c$, then $a \mid c$.

   (b) If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$.

   (c) If $a \mid b$, then $b = 0$ or $|b| \geq |a|$.

   (d) If $a \mid b$ and $b \mid a$, then $|a| = |b|$.

   (e) If $b > 0$, then there exist unique q and r such that $a = qb + r$ $(0 \leq r < b)$. Here we call q the quotient of a divided by b, and r the remainder.
   It is easy to see that $q = \left\lfloor \frac{a}{b} \right\rfloor$ where $\lfloor x \rfloor$ is the greatest integer not greater than x. Also, we denote the r value as $(a \bmod b)$.

2. A *multiple* m of n is defined such that there exists k such that $m = kn$, i.e. $n \mid m$.

3. A *prime number* is a positive integer p other than 1 such that 1 and p are its only positive factors. The five smallest primes are 2, 3, 5, 7, 11. A *composite number* is a positive integer other than 1 that is not prime. The five smallest composite numbers are 4, 6, 8, 9, 10.

   Properties:

   (a) Any two prime numbers p, q satisfy $\gcd(p, q) = 1$.

(b) If prime $p \mid ab$, then $p \mid a$ or $p \mid b$.

(c) If prime $p \nmid a$, then $\gcd(p, a) = 1$.

(d) If $a \mid bp$ for prime p and $p \nmid a$, then $a \mid b$ (a direct result of properties 3c and 8a).

4. A *prime factor* of an integer is a factor that is a prime number.

5. A *prime factorization* is the expression of a positive integer greater than 1 as a product of prime numbers. For example, $84 = 2^2 \times 3 \times 7$.

6. $p^\alpha \parallel n$ (read "p^α fully divides n") for prime p means that $p^\alpha \mid n$ but $p^{\alpha+1} \nmid n$. For example, since $360 = 2^3 \times 3^2 \times 5$, we have $2^3 \parallel 360, 3^2 \parallel 360$ and $5^1 \parallel 360$.

7. The *greatest common divisor* of $m_1, m_2, \ldots, m_k$ that are not all zero is the greatest positive integer that divides all of $m_1, m_2, \ldots, m_k$. We denote this as $\gcd(m_1, m_2, \ldots, m_k)$. For example, $\gcd(4, 7) = 1$ and $\gcd(8, -12) = 4$.

   Properties:

   (a) $\gcd(a, ka) = |a|$ for $a \neq 0$.

   (b) $\gcd(a, b) = \gcd(a, b + ka)$.

   (c) Any common factor of a and b divides $\gcd(a, b)$.

   (d) **Bézout's identity:** If $\gcd(a, b) = d$, then there exist x, y (called Bézout's coefficients) such that $ax + by = d$. Specifically, $\gcd(p, q) = 1$ if and only if there exist x, y such that $px + qy = 1$. (See this for an algorithm that computes a possible pair (x, y).)

   (e) $\gcd(ma, mb) = |m| \cdot \gcd(a, b)$.

   (f) If ab is the kth power of some integer ($k \geq 2$), and if $\gcd(a, b) = 1$, then a and b are each the kth power of some integer.

   (g) $\gcd(n^a - 1, n^b - 1) = n^{\gcd(a,b)} - 1$ $(n > 0)$.

   (h) $\gcd(m_1, m_2, \ldots, m_k) = \gcd(\gcd(m_1, m_2), m_3, m_4, \ldots, m_k)$.

8. Calling p and q *coprime* or *relatively prime* means that $\gcd(p, q) = 1$. Similarly, call $p_1, p_2, \ldots, p_k$ coprime if their greatest common divisor is 1. Call $p_1, p_2, \ldots, p_k$ *mutually coprime* if $\gcd(p_i, p_j) = 1$ for any $i \neq j$. For example, 6 and 35 are coprime, 4, 2 and 7 are coprime, and 5, 12 and 7 are mutually coprime.

   Properties:

   (a) If $a \mid bc$ and a, c are coprime, then $a \mid b$.

   (b) If $\gcd(a, b) = d$, then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

   (c) If $\gcd(a, m) = 1$ and $\gcd(b, m) = 1$, then $\gcd(ab, m) = 1$.

   (d) If $m \mid n$, then $\gcd(m, n \pm 1) = 1$ (a direct result of property 7b).

9. The *least common multiple* of nonzero $m_1, m_2, \ldots, m_k$ is the least positive integer that is divisible by all of $m_1, m_2, \ldots, m_k$. We denote this as $\operatorname{lcm}(m_1, m_2, \ldots, m_k)$. For example, $\operatorname{lcm}(4, 7) = 28$ and $\operatorname{lcm}(8, -12) = 24$.

   Properties:

   (a) Any common multiple of a and b is a multiple of $\operatorname{lcm}(a, b)$.
   (b) $\operatorname{lcm}(a, ka) = |ka|$ $(a, k \neq 0)$.
   (c) $\operatorname{lcm}(ma, mb) = |m| \cdot \operatorname{lcm}(a, b)$.
   (d) $\operatorname{lcm}(a, b) \cdot \gcd(a, b) = |ab|$ $(a, b \neq 0)$.
   Warning: $\operatorname{lcm}(m_1, m_2, \ldots, m_k) \cdot \gcd(m_1, m_2, \ldots, m_k) = |m_1 m_2 \cdots m_k|$ is not necessarily true for $k > 2$.
   (e) If $m_1, m_2, \ldots, m_k$ are mutually coprime, then $\operatorname{lcm}(m_1, m_2, \ldots, m_k) = |m_1 m_2 \cdots m_k|$.
   (f) $\operatorname{lcm}(m_1, m_2, \ldots, m_k) = \operatorname{lcm}(\operatorname{lcm}(m_1, m_2), m_3, m_4, \ldots, m_k)$.

2 Practice problems

If you're stuck on a problem, you can scroll to the next page to get some hints.

Note: If not otherwise mentioned, a variable is assumed to be representing an integer.

1. Prove that the fraction $\dfrac{4k+7}{7k+12}$ is reduced to lowest terms.

2. Prove that the number of positive factors of positive integer n is less than $2\sqrt{n}$.

3. Prove Bézout's general identity from the special identity. In other words, prove that there exist integers x, y such that $ax + by = \gcd(a, b)$ assuming we already know that there exist integers x, y such that $a'x + b'y = 1$ if a', b' are coprime.

4. Given that $a \mid bc$ for positive a, b, c, prove that: i) a is composite if $a > b, c$; ii) $\dfrac{bc}{a}$ is composite if $a < b, c$.

5. Given that $a + b \mid a^3 - b^3$ for positive integers a, b satisfying $a \neq b$ and $a + b$ is prime, prove that $a + b \mid ab$. *(SJAMMO 2019 Senior level Q1)*

6. Prove that $2^{2^a} + 1$ and $2^{2^b} + 1$ are coprime for distinct non-negative a, b.

7. Prove that positive integers a, b, c are mutually coprime if and only if

$$\operatorname{lcm}(a, b) \cdot \operatorname{lcm}(b, c) \cdot \operatorname{lcm}(c, a) = [\operatorname{lcm}(a, b, c)]^2.$$

8. The Fibonacci sequence F_n is defined such that $F_0 = 0, F_1 = 1$ and $F_{k+2} = F_{k+1} + F_k$ for $k \geq 0$.

   (a) Prove that F_k and F_{k+1} are coprime for all $k \geq 0$.
   (b) Prove that $F_m \mid F_n$ if and only if $m \mid n$.

Hints...

1. Use Bézout's identity to prove that the numerator and denominator are coprime.

2. The factors are "symmetric" about $\sqrt{n}$.

3. Use property 8b.

4. Proof by contradiction: assuming that the desired conclusion is false, see if you can deduce a contradiction using property 3b.

5. Factor $a^3 - b^3$ and then try to make use of properties 3b and 8a.

6. Assume $a < b$. Then prove that $2^{2^a} + 1 \mid 2^{2^b} - 1$ using property 7g and the difference of squares formula. Using property 7b then completes the proof.

7. Two approaches: 1) Consider the prime factorizations of a, b, c, and express the left and right sides of the equation given as prime factorizations. 2) Make use of properties 9d, 9e, and 9f. You might also have to use inequalities after that: if you prove that $\gcd(a, b) \leq 1$, then it must be true that $\gcd(a, b) = 1$.

8. (a) Make use of property 7b repeatedly on $F_{k+2} = F_{k+1} + F_k$. This technique is called induction. (b) Find a pattern in the remainders of F_{qm-r} ($q \geq 1$, $0 \leq r < m$) when divided by F_m. Prove that the remainder is zero if and only if $r = 0$ by induction. You will eventually have to use the result from part (a).