Prime Factorization

Dennis Chen

NQV

These are problems where you want to look at the highest power of a prime that divides a number. This is the v_p function.

🌐 1   Divisiblity

Here is the formal definition of divisibility.

> **Divisibility.** For integers a, b, we say a divides b if and only if there exists some integer c such that $ac = b$. We denote this as $a \mid b$.

This implies the following three facts.

> **Divisibility Results.** Given integers a, b, c,
>
> ■ If $a \mid b$ and $b \mid c$ then $a \mid c$. (This may be referred to as the "chain rule" of divisibility.)
>
> ■ If $a \mid b$ then $a \mid bc$ for all integer c.
>
> ■ If $a \mid b$ and $a \mid c$, then $a \mid b + c$ and $a \mid b - c$.

1.1   P-adic Valuation

P-adic valuation, or the v_p function, asks for the largest power of p that divides an integer.

> **P-adic Valuation.** For a positive integer n, $v_p(n)$ is the largest integer that satisfies $p^{v_p(n)} \mid n$.

Remember that $v_p(n)$ is only defined for prime p.
This implies the following obvious but very useful fact.

> **P-adic Inequality.** If $a \mid b$, then for all primes p, $v_p(a) \leq v_p(b)$.

> **Proof.** We proceed by contradiction. Say $v_p(a) > v_p(b)$. Then $p^{v_p(a)} \mid a \mid b$, implying that $p^{v_p(a)} \mid b$ by the chain rule of divisibility. But $v_p(b)$ is the largest power of p that divides b, contradiction.

1.2   GCD and LCM

> **Greatest Common Divisor.** We define $\gcd(a_1, a_2 \ldots a_n)$ as the largest positive integer such that
>
> $$\gcd(a_1, a_2 \ldots a_n) \mid a_i$$
>
> for all $1 \leq i \leq n$.

> **Least Common Multiple.** We define $\text{lcm}(a_1, a_2 \ldots a_n)$ as the smallest **positive** integer such that
>
> $$a_i \mid \text{lcm}(a_1, a_2 \ldots a_n)$$
>
> for all $1 \leq i \leq n$.

As an exercise, list the divisors of 0, the numbers that 0 divides, and find $\gcd(0, 8)$.

Now we take a look at the prime powers of gcd and lcm .

> **P-adic Maximum and Minimum.** Given integers $a_1, a_2, \ldots, a_n$,
>
> - $v_p(\gcd(a_1, a_2, \ldots, a_n)) = \min(v_p(a_1), v_p(a_2), \ldots, v_p(a_n))$.
> - $v_p(\text{lcm}(a_1, a_2, \ldots, a_n)) = \max(v_p(a_1), v_p(a_2), \ldots, v_p(a_n))$.

The proof is an obvious consequence of the P-adic Inequality.

🌐 2 Well-known Divisor Tricks

You should know everything here.

> **Fundamental Theorem of Arithmetic.** Every number greater than 1 is either a prime or can be uniquely, up to order, expressed as a product of primes.

If you are curious about the proof, you may check out https://gowers.wordpress.com/2011/11/18/proving-the-fundamental-theorem-of-arithmetic/.

> **Number of Divisors.** Say the prime factorization of n is $p_1^{q_1} \cdot p_2^{q_2} \cdots \cdots p_k^{q_k}$. Then n has $(p_1 + 1)(p_2 + 1) \cdots (p_k + 1)$ positive divisors.

> **Proof.** This is a simple combinatorics problem.
> Note that there are $q_i + 1$ numbers between 0 and q_i to pick from, and you choose the exponent of each prime p_i for the divisor. So in total there are $(q_1 + 1)(q_2 + 1) \cdots (q_k + 1)$ choices.

> **Sum of Divisors.** Say the prime factorization of n is $p_1^{q_1} \cdot p_2^{q_2} \cdots \cdots p_k^{q_k}$. Then the sum of the factors of n is
>
> $$\left(\frac{p_1^{q_1+1} - 1}{p_1 - 1} \right) \left(\frac{p_2^{q_1+1} - 1}{p_2 - 1} \right) \cdots \left(\frac{p_k^{q_k+1} - 1}{p_k - 1} \right) =$$
>
> $$\left(1 + p_1 + p_1^2 + \cdots + p_1^{q_1} \right) \left(1 + p_2 + p_2^2 + \cdots + p_2^{q_2} \right) \cdots \left(1 + p_k + p_k^2 + \cdots + p_k^{q_k} \right).$$

The latter part of the proof is going to seem magical. Take some time to digest it.

Proof. By geometric series, $\frac{p_i^{q_i+1}-1}{p_i-1} = 1 + p_i + p_i^2 + \cdots + p_i^{q_i}$.

Notice that expanding the product gives you every possible combination of powers of $p_1, p_2, \ldots, p_k$. This means that summing all of these combinations together is equivalent to summing up all of the divisors of n.

For concreteness, we present a few examples.

Example. Find the prime factorization of 216.

Solution. The prime factorization is $2^3 \cdot 3^3$, and this is unique by the Fundamental Theorem of Arithmetic.

Example. Find the number of divisors of 216.

Solution. The prime factorization is $2^3 \cdot 3^3$, as we have established in the previous example. Now note that we can choose the power of 2 of the divisor in 4 ways, and we can choose the power of 3 of the divisor in 4 ways as well. Thus there are $4 \cdot 4 = 16$ total divisors.

Example. Find the sum of the divisors of 216.

Solution. The sum of the divisors is $(2^0 + 2^1 + 2^2 + 2^3)(3^0 + 3^1 + 3^2 + 3^3) = 15 \cdot 40 = 600$.

Expand the sum out to convince yourself that all divisors are characterized exactly once.

Here is a much harder example, motivated by an obvious fact.

Odd Number of Divisors. A number has an odd number of positive divisors if and only if it is a perfect square.

The proof is just looking at the number of divisors formula. Alternatively, each divisor d gets paired off with $\frac{n}{d}$, except for $\sqrt{n}$.

Example (104 NT). Twenty bored students take turns walking down a hall that contains a row of closed lockers, numbered 1 to 20. The first student opens all the lockers; the second student closes all the lockers numbered 2, 4, 6, 8, 10, 12, 14, 16, 18, 20; the third student operates on the lockers numbered 3, 6, 9, 12, 15, 18: if a locker was closed, he opens it, and if a locker was open, he closes it; and so on. For the ith student, he works on the lockers numbered by multiples of i: if a locker was closed, he opens it, and if a locker was open, he closes it. What is the number of the lockers that remain open after all the students finish their walks?

Solution. Note that a locker is only open if it is interacted with an odd number of times, and the number of times a locker is interacted with is the number of divisors it has. Since perfect squares are the only integers with an odd number of divisors, the open lockers are just $1, 4, 9, 16$. Thus 4 lockers are open.

Example (AIME I 2005/12). For positive integers n, let $\tau(n)$ denote the number of positive integer divisors of n, including 1 and n. For example, $\tau(1) = 1$ and $\tau(6) = 4$. Define $S(n)$ by $S(n) = \tau(1) + \tau(2) + \cdots + \tau(n)$. Let a denote the number of positive integers $n \leq 2005$ with $S(n)$ odd, and let b denote the number of positive integers $n \leq 2005$ with $S(n)$ even. Find $|a - b|$.

Solution. Note $\tau(n)$ is odd if and only if n is a perfect square, implying that $S(n)$ is odd if n is greater than an odd number of squares and even if n is greater than an even number of squares.

We can explicitly characterize this as

$$S(n)\begin{cases} \text{is odd if } 1^2 \le n < 2^2 \text{ or } 3^2 \le n < 4^2 \text{ or } 5^2 \le n < 6^2 \text{ or} \dots \\ \text{is even if } 2^2 \le n < 3^2 \text{ or } 4^2 \le n < 5^2 \text{ or } 6^2 \le n < 7^2 \text{ or} \dots \end{cases}.$$

Now we use the difference of squares formula to find a and b. Note that the largest square smaller than 2005 is $44^2 = 1936$, so

$$a - b = (-1^2 + 2^2 - 3^2 + 4^2 - \dots - 43^2 + 44^2) - (-2^2 + 3^2 - 4^2 + 5^2 - \dots + 42^2 - 43^2) - (2005 - 1936 + 1)$$

$$a - b = (1 + 2 + 3 + 4 + \dots + 43 + 44) - (2 + 3 + 4 + \dots + 43) - 70$$

$$a - b = 1 + 44 - 70 = -25.$$

Thus the answer is 25.

🌐 3 Assorted Examples

These are some examples of prime factorization analysis problems. Since this is a technique rather than a theorem, we will show, not tell.

> **Example (Dennis' Mock AIME 2020/4).** Find the number of ordered pairs of positive integers (a, b) such that $\gcd(a, b) = 20$ and $\operatorname{lcm}(a, b) = 19!$

Solution.

1. Note $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$, so $ab = 20!$

2. Let $\frac{a}{20} = x$ and $\frac{b}{20} = y$. Then note $\gcd(x, y) = 1$ and $\operatorname{lcm}(a, b) = \operatorname{lcm}(20x, 20y) = 20\operatorname{lcm}(x, y) = 20xy$. Thus $xy = \frac{19!}{20}$.

3. Note picking (x, y) uniquely determines (a, b).

4. Now note we have to either assign *all* of the powers of a prime to x or to y.

5. Check how many primes divide $\frac{19!}{20}$.

> **Example (AIME 1987/7).** Let $[r, s]$ denote the least common multiple of positive integers r and s. Find the number of ordered triples (a, b, c) of positive integers for which $[a, b] = 1000$, $[b, c] = 2000$, and $[c, a] = 2000$.

Solution.

1. Let $a = 2^a \cdot 5^x$, $b = 2^b \cdot 5^y$, $c = 2^c \cdot 5^z$.

2. Note that $\max(a, b) = 3$, $\max(b, c) = 4$, $\max(c, a) = 4$. This notably implies $c = 4$. (Why can't we have $a = 4$ or $b = 4$?)

3. Note that $\max(x, y) = \max(y, z) = \max(z, x) = 3$. How many of x, y, z can be less than 3 at a time? How many ways can we do this?

4. Multiply the number of ways to distribute the powers of 2 by the number of ways to distribute the powers of 5.

Here is a prime factorization analysis problem that doesn't have GCD or LCM in the problem statement.

Example (ARML 2008). If n has 60 positive factors, compute the largest number of positive factors that n^2 could have.

Solution. Let the prime factorization of n be $p_1^{q_1} \cdot p_2^{q_2} \cdot \cdots \cdot p_k^{q_k}$. Then note

$$(p_1 + 1)(p_2 + 1) \cdots (p_k + 1) = 60.$$

We want to maximize

$$(2p_1 + 1)(2p_2 + 1) \cdots (2p_k + 1).$$

This occurs when $p_1 = p_2 = 1, p_3 = 2, p_4 = 4$. Thus our answer is $3 \cdot 3 \cdot 5 \cdot 9 = 405$.

❂ 4 Problems

Minimum is [45 ♟]. Problems denoted with ♞ are required. (They still count towards the point total.)

> "I won't ask you to buy me curry bread anymore. Goodbye."
>
> Yugami-kun Has No Friends

[1 ♟] Problem 1 Answer the following:

- What are the divisors of 0?

- What integers does 0 divide?

- Find $\gcd(0, 8)$.

- Why isn't something like $\text{lcm}(0, 8)$ defined?

[1 ♟] Problem 2 (AMC 10A 2005/15) Find the number of positive cubes that divide $3! \cdot 5! \cdot 7!$

[1 ♟] Problem 3 (AMC 8 2013/10) What is the ratio of the least common multiple of 180 and 594 to the greatest common factor of 180 and 594?

[2 ♞] Problem 4 (PUMaC 2016) What is the smallest positive integer n such that $2016n$ is a perfect cube?

[2 ♟] Problem 5 (SMT 2018) One of the six digits in the expression $435 \cdot 605$ can be changed so that the product is a perfect square N^2. Compute N.

[2 ♟] Problem 6 (AIME I 2010/1) Maya lists all the positive divisors of 2010^2. She then randomly selects two distinct divisors from this list. Let p be the probability that exactly one of the selected divisors is a perfect square. The probability p can be expressed in the form $\frac{m}{n}$, where m and n are relatively prime positive integers. Find $m + n$.

[2 ♟] Problem 7 (AMC 12B 2002/12) For which integers n is $\dfrac{n}{20 - n}$ the square of an integer?

[3 ♞] Problem 8 (Scrabbler AMC 10) Let n be the smallest positive integer with the property that $\text{lcm}(n, 2020!) = 2021!$, where $\text{lcm}(a, b)$ denotes the least common multiple of a and b. How many positive factors does n have?

[3 ♟] Problem 9 (Switzerland Prelimiary Round 2018/N1) Let $n \geq 2$ be a positive integer, and let $d_1, \cdots, d_r$ be all the positive divisors of n that are smaller that n. Determine all n for which

$$\text{lcm}(d_1, \cdots, d_r) \neq n.$$

[3 ♞] Problem 10 (AMC 12A 2016/22) How many ordered triples (x, y, z) of positive integers satisfy $\text{lcm}(x, y) = 72$, $\text{lcm}(x, z) = 600$, and $\text{lcm}(y, z) = 900$?

[4 ♟] Problem 11 (CMC 10A 2021/22) For a certain positive integer n, there are exactly 2021 ordered pairs of positive divisors (d_1, d_2) of n for which d_1 and d_2 are relatively prime. What is the sum of all possible values of the number of divisors of n?

[4 ♟] Problem 12 (AHSME 1987/23) If p is a prime and both roots of $x^2 + px - 444p = 0$ are integers, then what is p?

[4 ♟] **Problem 13 (HMMT 2018)** Distinct prime numbers p, q, r satisfy the equation

$$2pqr + 50pq = 7pqr + 55pr = 8pqr + 12qr = A$$

for some positive integer A. What is A?

[6 ♟] **Problem 14 (DMC 10C 2021/21)** Richard thinks of a positive integer n and writes the base ten representations of $n!$ and $(n + 1)!$ on a board. He then erases the zeroes to the right of the last nonzero digit of each number (if any exist), resulting in two numbers a and b. If one of a and b is 4 times the other, what is the sum of all possible values of n less than 1000?

[6 ♟] **Problem 15 (AMC 12B 2007/24)** Find all pairs of positive integers (a, b) such that $\gcd(a, b) = 1$ and $\frac{a}{b} + \frac{14b}{9a}$ is an integer.

[6 ♟] **Problem 16 (AIME I 2020/10)** Let m and n be positive integers satisfying the conditions

- $\gcd(m + n, 210) = 1$,

- m^m is a multiple of n^n, and

- m is not a multiple of n.

Find the least possible value of $m + n$.

[6 ♟] **Problem 17 (ARML 2010)** Compute the smallest positive integer n such that n^n has at least $1,000,000$ positive divisors.

[6 ♟] **Problem 18 (AMC 10B 2018/23)** How many ordered pairs (a, b) of positive integers satisfy the equation

$$a \cdot b + 63 = 20 \cdot \mathrm{lcm}(a, b) + 12 \cdot \gcd(a, b),$$

where $\gcd(a, b)$ denotes the greatest common divisor of a and b, and $\mathrm{lcm}(a, b)$ denotes their least common multiple?

[9 ♞] **Problem 19 (AMC 12A 2021/25)** Let $d(n)$ denote the number of positive integers that divide n, including 1 and n. For example, $d(1) = 1, d(2) = 2$, and $d(12) = 6$. (This function is known as the divisor function.) Let

$$f(n) = \frac{d(n)}{\sqrt[3]{n}}.$$

There is a unique positive integer N such that $f(N) > f(n)$ for all positive integers $n \neq N$. What is the sum of the digits of N?

[9 ♟] **Problem 20 (AMC 10A 2018/22)** Let a, b, c, and d be positive integers such that $\gcd(a, b) = 24$, $\gcd(b, c) = 36$, $\gcd(c, d) = 54$, and $70 < \gcd(d, a) < 100$. Which of the following must be a divisor of a?

(A) 5   **(B)** 7   **(C)** 11   **(D)** 13   **(E)** 17

[9 ♟] **Problem 21 (AMC 12B 2010/25)** For every integer $n \geq 2$, let $\mathrm{pow}(n)$ be the largest power of the largest prime that divides n. For example $\mathrm{pow}(144) = \mathrm{pow}(2^4 \cdot 3^2) = 3^2$. What is the largest integer m such that 2010^m divides $\prod_{n=2}^{5300} \mathrm{pow}(n)$?

[13 ♟] **Problem 22 (ISL 2007/N2)** Let $b, n > 1$ be integers. Suppose that for each $k > 1$ there exists an integer a_k such that $b - a_k^n$ is divisible by k. Prove that $b = A^n$ for some integer A.

[13 ♟] **Problem 23 (PUMaC 2016)** Let $k = 2^6 \cdot 3^5 \cdot 5^2 \cdot 7^3 \cdot 53$. let S be the sum of $\frac{\gcd(m,n)}{\text{lcm}(m,n)}$ over all ordered pairs of positive integers (m, n) where $mn = k$. If S can be written in simplest form as $\frac{r}{s}$, compute $r + s$.