初等数论

吴 伊 涛

2022 年春

Given an integer n greater than 1, by Fundamental Theorem of Arithmetic, n can be written uniquely as

$$n = p_1^{a_1} p_2^{a_2} \cdots p_l^{a_l}$$

where $p_1, p_2, \cdots, p_l$ are pairwise different primes, $a_1, a_2, \cdots, a_l$ are positive integers. e.g. $10000 = 2^4 \times 5^4$.

Sometimes, the following form is more convenient:

$$n = \prod_p p^{a(p)}$$

where p runs through all primes, $a(p)$ is a nonnegative integer valued function defined on all primes and $a(p) = 0$ for all but finitely many primes.

Examples

- $209 = 11 \times 19$

$$209 = \prod_p p^{a(p)}$$

when $p = 11$, $a(p) = 1$, $p = 19$, $a(p) = 1$, $p =$ other primes such as $2, 3, 5, 7 \cdots$, $a(p) = 0$.

- $180 = 2^2 \times 3^2 \times 5$

$$180 = \prod_p p^{a(p)}$$

When $p = 2$, $a(p) = 2$, $p = 3$, $a(p) = 2$, $p = 5$, $a(p) = 1$, $p =$ other primes such as $7, 11, 13, \cdots$, $a(p) = 0$.

Q: Give a description of $a(p)$ from n (without n's factorization).

Def.: Let p be a prime, n be a nonzero integer, Then there exists a unique nonnegative integer a(Why?), s.t.

$$p^a | n, \quad p^{a+1} \nmid n$$

(and is denoted by $p^a || n$).

The integer a is called **the order of n at (the prime)p**, denoted by $a = ord_p n$.

Examples:

- $11|209$ and $11^2 \nmid 209$(i.e. $11||209$), So $ord_{11}209 = 1$.
- $7 \nmid 209$(i.e. $7^0||209$), So $ord_7 209 = 0$.
- $3^2||180$, So $ord_3 180 = 2$.

Remark:

- $ord_p n$ are always nonnegative integers. And we have $ord_p n = 0$ iff(short for if and only if) $p \nmid n$.
- Obviously, for all nonzero integers n, $ord_p n = ord_p(-n)$.
- If $n = 0$, we set $ord_p 0 = \infty$.
- We'll prove $a(p) = ord_p n$.

Lemma: Let p be a prime, x, y be integers. Then

$$ord_p(xy) = ord_p x + ord_p y$$

Proof:

If $x = 0$ or $y = 0$, then both sides of the equality is ∞, the statement holds。

If $x \neq 0, y \neq 0$, then set $x = p^m a, y = p^n b$, and $p \nmid a$， $p \nmid b$. So

$$ord_p x = m, \quad ord_p y = n$$

We need to prove $ord_p(xy) = m + n$.

Since $xy = p^{m+n}ab$, by "the important corollary" in our proof of the uniqueness of Fundamental Theorem of Arithmetic(Let p be a prime,

a_1, a_2 be two integers, If $p \nmid a_1$,$p \nmid a_2$, then $p \nmid a_1 a_2$), we have $p \nmid ab$.

Hence $ord_p(xy) = m + n$. $\square$

Corollary: Let p be a prime, $x_1, x_2, \cdots, x_n$ be integers. Then

$$ord_p(x_1 x_2 \cdots x_n) = ord_p x_1 + ord_p x_2 + \cdots + ord_p x_n$$

(Hint for Proof: Use induction on n.)

Now, Given an integer n greater than 1,

$$n = \prod_p p^{a(p)}$$

Apply the function ord_q(q is a prime) to both sides of the equation

$$ord_q n = \sum_p a(p) ord_q p \quad (*)$$

Obviously, when $p = q$, $ord_q p = 1$, when $p \neq q$, $ord_q p = 0$.

Apply these to (*):

$$ord_q n = a(q)$$

Which is what we want to prove. $\square$

Application of $ord_p n$

Example: Prove that $\sqrt{2}$ is an irrational number.

Proof:

Assume not, then

$$\sqrt{2} = \frac{p}{q} \qquad (*)$$

where p, q are nonzero integers(Why we assume p, q nonzero?).

Squaring (*), we get:

$$2q^2 = p^2 \qquad (**)$$

Apply ord_2 to (**), we get:

$$ord_2(2q^2) = ord_2(p^2) \qquad (***)$$

LHS of $(***) = ord_2 2 + 2ord_2 q = 1 + 2ord_2 q$ is odd.

RHS of $(***) = 2ord_2p$ is even.

A contradiction. Thus $\sqrt{2}$ is an irrational number. $\square$

Remarks

- Similarly, we can prove:

  Let m be a positive integer, if there exists a prime number p, s.t. $ord_p m$ is odd, then $\sqrt{m}$ is an irrational number.

- We can also prove:

  Let m be a positive integer, m is a square if and only if for any prime p, $ord_p m$ is even. (Hint: Use Fundamental Theorem of Arithmetic.)

- Combining above, we get:

  $\sqrt{m}$ is irrational if and only if m is not a square.

- Prove $\sqrt{1000009}$ is irrational.

Least Common Multiple

Def.: Let a, b be two integers, then an integer m satisfying the following conditions:

1. $a|m$, $b|m$.
2. If $a|n$,$b|n$, then $m|n$.
3. $m \geq 0$

is called a**least common multiple of** a, b, and is denoted by $m = lcm(a, b)$.

Remarks:

- We can prove that $lcm(a, b)$ is unique via the definition of the least common multiple of a, b.

- If $a \neq 0,\ b \neq 0$, then $lcm(a,b) =$ the least positive integer in the common multiples of a, b(Why we assume $a \neq 0,\ b \neq 0$?).
- Similarly, we can define the least common multiple of $a_1, a_2, \cdots, a_k$, we leave it to you.

Relation between gcd and lcm

Theorem: Let a, b be two positive integers, with factorizations(as before):

$$a = \prod_p p^{a(p)}, \quad b = \prod_p p^{b(p)}$$

Then

$$gcd(a, b) = \prod_p p^{min\{a(p),b(p)\}}$$

$$lcm(a, b) = \prod_p p^{max\{a(p),b(p)\}}$$

In particular,

$$gcd(a, b) \cdot lcm(a, b) = a \cdot b$$

Example:

$180 = 2^2 \times 3^2 \times 5$

$84 = 2^2 \times 3 \times 7$

By the theorem above:

$gcd(180, 84) = 2^2 \times 3 \times 1 \times 1 = 12$

$lcm(180, 84) = 2^2 \times 3^2 \times 5 \times 7 = 1260$

Remark: In order to use the above theorem to find $gcd(a, b)$, we need to know the factorization of a, b first. When $a, b \gg 1$, it is extremely hard to get the factorization of a, b. We will introduce a method far more efficient later.

A useful method

Theorem: Let a, b be two nonzero integers, Then:

$\frac{a}{b}$ is an integer iff for all primes p, $ord_p b \leq ord_p a$.

Proof:

If $\frac{a}{b} = c \in \mathbb{Z}$, then $a = bc$, So $ord_p a = ord_p b + ord_p c \geq ord_p b$.

Conversely, If $ord_p b \leq ord_p a$ for all primes p, we then set

$$c = \pm \prod_p p^{ord_p a - ord_p b}$$

(If $sgn(a) = sgn(b)$, then set "+" in the above equality, otherwise, set "-")

It's easy to check $bc = a$(Check it yourself!), so $\frac{a}{b} = c$ is an integer. $\square$

Example:

$a = 88, b = 48$.

Since there is a prime $p = 3$, s.t. $ord_3 48 = 1 \nleq ord_3 88 = 0$, So $\frac{88}{48}$ is not an integer.

Remark: The above example seems stupid, we will see some examples make sense later.

Arithmetic functions

- $[x]$

Def.: Let x be a real number, then

$[x]$ is defined to be the largest integer smaller than or equal to x(integral part of x),

$\{x\} := \quad x - [x]$(fraction part of x).

Examples:

$[4.8] = 4, \quad \{4.8\} = 0.8$

$[\pi] = 3, \quad \{\pi\} = \pi - 3$

$[-2.5] = -3, \quad \{-2.6\} = 0.4$

$[-\pi] = -4, \quad \{-\pi\} = 4 - \pi$

Note that $0 \leq \{x\} < 1$!

Remark:

- Some times we use $\lfloor x \rfloor$(floor function) instead of $[x]$, with a related function $\lceil x \rceil$(ceiling function), which is defined to be the smallest integer larger than or equal to x. We will see the applications of them later.

- Obviously, $\lfloor x \rfloor \leq x \leq \lceil x \rceil$, with equality holds(simultaneously) if and only if x is an integer.

Applications of $[x]$

- Factorization of $n!$.

Recall: $n! = 1 \times 2 \times \cdots \times n$, e.g.

$3! = 1 \times 2 \times 3 = 6, 4! = 1 \times 2 \times 3 \times 4 = 24$。

Q: How to get the factorization of $n!$?

When n is small, we can factorize all integers from 1 to n, and then make a product, e.g.

$8! = 1\times2\times3\times4\times5\times6\times7\times8 = 1\times2\times3\times(2\times2)\times5\times(2\times3)\times7\times2^3 = 2^7 \times 3^2 \times 5 \times 7$

Q: When n is large, how to get the factorization of $n!$?

Recall: Given an integer m greater than 1, by Fundamental Theorem of Arithmetic, m can be written uniquely as

$$m = \prod_p p^{a(p)}$$

where $a(p) = ord_p(m)$.

Thus, to get the factorization of $n!$, it suffices to calculate $ord_p(n!)$.

Lemma: Let a, b be two positive integers, then the number of multiples of b from 1 to a is just $[\frac{a}{b}]$, i.e.

$$|\{x : 1 \leq x \leq a, b|x\}| = [\frac{a}{b}]$$

Idea of proof:

In $1, 2, \cdots, b$, b is the only multiple of b.

Similarly:

In $kb+1, kb+2, \cdots, kb+b$, $kb+b$ is the only multiple of b.

So the number of multiples of b from 1 to a is just those consecutive disjoint chains from 1 to a, which is just $[\frac{a}{b}]$.

Factorization of $n!$

The following theorem tells us how to calculate $ord_p(n!)$ via the function $[x]$.

Theorem: Let p be a prime, n be a positive integer. Then:

$$ord_p(n!) = [\frac{n}{p}] + [\frac{n}{p^2}] + [\frac{n}{p^3}] + \cdots = \sum_{r=1}^{\infty} [\frac{n}{p^r}]$$

(Note that when $r \gg 1$, $0 < \frac{n}{p^r} < 1$, so $[\frac{n}{p^r}] = 0$, which means the above infinite series is a sum of finite nonzero integers.)

Corollary: Let p be a prime, n be a positive integer. Then:

$$n! = \prod_{p} p^{ord_p(n!)}$$

where

$$ord_p(n!) = [\frac{n}{p}] + [\frac{n}{p^2}] + [\frac{n}{p^3}] + \cdots = \sum_{r=1}^{\infty} [\frac{n}{p^r}]$$

Example: Factorize 30! into the product of prime powers.

Solution:

Primes smaller than or equal to 30 are $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$. It suffices to calculate the order of 30! at these primes.

$ord_2 30! = [\frac{30}{2}] + [\frac{30}{2^2}] + [\frac{30}{2^3}] + [\frac{30}{2^4}] = 15 + 7 + 3 + 1 = 26$

$ord_3 30! = [\frac{30}{3}] + [\frac{30}{3^2}] + [\frac{30}{3^3}] = 10 + 3 + 1 = 14$

$ord_5 30! = [\frac{30}{5}] + [\frac{30}{5^2}] = 6 + 1 = 7$

$ord_7 30! = [\frac{30}{7}] = 4$

$ord_{11} 30! = [\frac{30}{11}] = 2$

$ord_{13} 30! = [\frac{30}{13}] = 2$

$ord_{17} 30! = [\frac{30}{17}] = 1$

$ord_{19}30! = [\frac{30}{19}] = 1$

$ord_{23}30! = [\frac{30}{23}] = 1$

$ord_{29}30! = [\frac{30}{29}] = 1$

So $30! = 2^{26} \times 3^{14} \times 5^7 \times 7^4 \times 11^2 \times 13^2 \times 17 \times 19 \times 23 \times 29$.

Example: Calculate $gcd(666!, 999^{88})$。

Solution:

$999 = 3^3 \times 37$, So $999^{88} = 3^{264} \times 37^{88}$(This is the factorization of 999^{88}).

Now we calculate the order of 666! at 3 and 37:

$ord_3 666! = [\frac{666}{3}] + [\frac{666}{3^2}] + [\frac{666}{3^3}] + [\frac{666}{3^4}] + [\frac{666}{3^5}] = 222 + 74 + 24 + 8 + 2 = 330.$

$ord_{37} 666! = [\frac{666}{37}] = 18.$

So the factorization of 666! is $3^{330} \times 37^{18} \times \cdots$(we omit the other prime powers).

So $gcd(666!, 999^{88}) = 3^{264} \times 37^{18}$.

Example: The binary representation of 100! ends in exactly x consecutive zeros, find the value of x.

Solution:

Note that the integer x satisfy the following relations:

$$2^x | 100!, \quad 2^{x+1} \nmid 100!$$

So $x = ord_2 100!$.

Hence $x = ord_2 100! = [\frac{100}{2}] + [\frac{100}{2^2}] + [\frac{100}{2^3}] + [\frac{100}{2^4}] + [\frac{100}{2^5}] + [\frac{100}{2^6}] = 50 + 25 + 12 + 6 + 3 + 1 = 97$.

So there are 97 consecutive zeros at the tail of the binary representation of 100!.

Example: The hexadecimal representation of 100! ends in exactly x consecutive zeros, find the value of x.

Solution:

Note that the integer x satisfy the following relations:

$$16^x | 100!, \quad 16^{x+1} \nmid 100!$$

which equivalent to

$$2^{4x} | 100!, \quad 2^{4x+4} \nmid 100!$$

Hence $x = [\frac{ord_2 100!}{4}]$(Why? Check it yourself!)

So $x = [\frac{ord_2 100!}{4}] = [\frac{97}{4}] = 24$.

So there are 24 consecutive zeros at the tail of the hexadecimal representation of 100!.

Example: The decimal representation of 100! ends in exactly x consecutive zeros, find the value of x.

Solution:

Note that the integer x satisfy the following relations:

$$10^x | 100!, \quad 10^{x+1} \nmid 100!$$

which equivalent to

$2^x | 100!, 5^x | 100!, \ 2^{x+1} \nmid 100!$ 或 $5^{x+1} \nmid 100!$

Hence $x = min\{ord_2 100!, ord_5 100!\}$(Why? Check it yourself!)

We already get $ord_2 100! = 97$, and $ord_5 100! = [\frac{100}{5}] + [\frac{100}{5^2}] = 20 + 4 = 24$.

So $x = min\{ord_2 100!, ord_5 100!\} = min\{97, 24\} = 24$. So there are 24 consecutive zeros at the tail of the decimal representation of 100!.

Example: The duodecimal representation of 100! ends in exactly x consecutive zeros, find the value of x.

Solution:

Note that the integer x satisfy the following relations:

$$12^x | 100!, \quad 12^{x+1} \nmid 100!$$

which equivalent to

$2^{2x} | 100!, 3^x | 100!$， $2^{2x+2} \nmid 100!$ 或 $3^{x+1} \nmid 100!$

Hence $x = min\{[\frac{ord_2 100!}{2}], ord_3 100!\}$(Why? Check it yourself!)

We already get $ord_2 100! = 97$, and $ord_3 100! = [\frac{100}{3}] + [\frac{100}{3^2}] + [\frac{100}{3^3}] + [\frac{100}{3^4}] = 33 + 11 + 3 + 1 = 48$.

So $x = min\{[\frac{ord_2 100!}{2}], ord_3 100!\} = min\{[\frac{97}{2}], 48\} = 48$

So there are 48 consecutive zeros at the tail of the duodecimal representation of 100!.

Use a similar method to solve the following problem(s):

The binary(resp. hexadecimal, decimal, duodecimal, $base - b$) representation of $\binom{100}{50} = \frac{100!}{50!50!}$ ends in exactly y consecutive zeros, find the value of y.

谢谢！