初等数论

吴 伊 涛

2022 年春

Recall:

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

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

Also recall the formula of the order of $n!$ at a prime p:

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

Example: Let k, n be two positive integers and $k < n$, Prove:

$\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is an integer.

Idea of Proof:

In order to prove $\frac{n!}{k!(n-k)!}$ is an integer, by the theorem above, it suffices to prove: for all primes p,

$$ord_p(k!(n-k)!) \leq ord_p(n!)$$

Since "ord_p translate product into addition", the above inequality equivalents to

$$ord_p k! + ord_p (n-k)! \leq ord_p n!$$

where each term is a kind of the order of some factorial at p.

Proof:

It suffices to prove: for all primes p,

$$ord_p(k!(n-k)!) \leq ord_p(n!)$$

We have:

$ord_p(k!(n-k)!)$

$= \sum_{r=1}^{\infty}[\frac{k}{p^r}] + \sum_{r=1}^{\infty}[\frac{n-k}{p^r}]$

$= \sum_{r=1}^{\infty}([\frac{k}{p^r}] + [\frac{n-k}{p^r}])$

$\leq \sum_{r=1}^{\infty}([\frac{k}{p^r} + \frac{n-k}{p^r}])$(Here we use the fact: "If $x, y \in \mathbb{R}$, then $[x] + [y] \leq [x+y]$". We will prove it later)

$= \sum_{r=1}^{\infty}[\frac{n}{p^r}]$

$= ord_p n!$

Now, we show: "If $x, y \in \mathbb{R}$, then $[x] + [y] \leq [x + y]$" .

By definition:

$[x]$ is the largest integer smaller than or equal to x, $[y]$ is the largest integer smaller than or equal to y,

So $[x] + [y]$ is an integer smaller than or equal to $x + y$,

Thus it is smaller than or equal to "the largest integer smaller than or equal to $x + y$", which is $[x + y]$.

Hence $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is an integer. $\square$

$\tau(n)$ and $\sigma(n)$

Def.: Let n be a positive integer, define

$\tau(n) =$ number of positive divisors of n. (Some authors use $\nu(n)$)

$\sigma(n) =$ sum of all positive divisors of n.

Example:

All positive divisors of 6 are: $1, 2, 3, 6$.

$$\tau(6) = 4, \sigma(6) = 1 + 2 + 3 + 6 = 12$$

All positive divisors of 8 are: $1, 2, 4, 8$.

$$\tau(8) = 4, \sigma(8) = 1 + 2 + 4 + 8 = 15$$

Given a specific integer n, we can always(in theory) calculate $\tau(n)$ and $\sigma(n)$ by listing all positive factors of n.

Q: Is there a formula of $\tau(n)$ and $\sigma(n)$?

Some special cases

- Case $n = 1$.

  $\tau(1) = 1, \quad \sigma(1) = 1$

- Case $n = p$ is a prime.

  p has only two positive divisors: $1, p$.

  $\tau(p) = 2, \quad \sigma(p) = p + 1$.

- Case $n = p^m$ is a power of prime.

  p^m has $m+1$ positive divisors: $1, p, p^2, \cdots, p^m$.

  $\tau(p^m) = m + 1, \quad \sigma(p^m) = 1 + p + \cdots p^m = \frac{p^{m+1}-1}{p-1}$.

Theorem: Let $n = p_1^{a_1}p_2^{a_2}\cdots p_l^{a_l}$, where $p_1, p_2, \cdots, p_l$ are pairwise different primes, $a_1, a_2, \cdots, a_l$ are positive integers. Then:

$$\tau(n) = (a_1+1)(a_2+1)\cdots(a_l+1)$$

$$\sigma(n) = (\frac{p_1^{a_1+1}-1}{p_1-1})(\frac{p_2^{a_2+1}-1}{p_2-1})\cdots(\frac{p_l^{a_l+1}-1}{p_l-1})$$

Proof:

A positive integer m divides n(i.e. m is a positive divisor of n), iff for all primes p, $ord_p m \leq ord_p n$.

Since prime divisors of n are $p_1, p_2, \cdots, p_l$, and the order of n at these primes are $a_1, a_2, \cdots, a_l$ respectively, prime factors of m should among $p_1, p_2, \cdots, p_l$, and the order of m at p_i should smaller than or equal to a_i(and greater than or equal to 0 of course).

Hence,

$$m = p_1^{e_1} p_2^{e_2} \cdots p_l^{e_l} \quad (*)$$

Each e_i has $a_i + 1$ choices(from 0 to a_i), and they are independent, thus $(a_1 + 1)(a_2 + 1) \cdots (a_l + 1)$ choices of $(e_1, e_2, \cdots, e_l)$ in total.

By the uniqueness of Fundamental Theorem of Arithmetic, each $(e_1, e_2, \cdots, e_l)$ correspond to pairwise different integers, thus $(a_1+1)(a_2+1) \cdots (a_l+1)$ is just the number of positive divisors of n.

We get the formula of $\tau(n)$.

For the formula of $\sigma(n)$, we just sum (*) for all e_i from 0 to a_i:

$$\sigma(n) = \sum_{e_1, e_2, \cdots, e_l} p_1^{e_1} p_2^{e_2} \cdots p_l^{e_l}$$

which can be split as:

$$\sigma(n) = (\sum_{e_1} p_1^{e_1})(\sum_{e_2} p_2^{e_2}) \cdots (\sum_{e_l} p_l^{e_l})$$

It's straightforward to check this is just the formula in the statement. $\square$

Example:

$10000 = 2^4 \times 5^4$

$\tau(10000) = (4+1) \times (4+1) = 25.$

$\sigma(10000) = \frac{2^5-1}{2-1} \times \frac{5^5-1}{5-1} = 24211.$

Generalization

Note that, we can write $\tau(n)$ and $\sigma(n)$ as:

$$\tau(n) = \sum_{d \in \mathbb{Z}^+, d|n} 1$$

$$\sigma(n) = \sum_{d \in \mathbb{Z}^+, d|n} d$$

In general, we can define a function $\sigma_k(n)$, where k is a nonnegative integer:

$$\sigma_k(n) = \sum_{d \in \mathbb{Z}^+, d|n} d^k$$

Clearly, $\sigma_0(n) = \tau(n), \quad \sigma_1(n) = \sigma(n)$.

Try to find a formula of $\sigma_k(n)$!

Multiplicative Function

Def.: Let $f(x)$ be an arithmetic function, if $\forall a, b$, s.t. $gcd(a, b) = 1$, the equality $f(ab) = f(a)f(b)$ holds, then $f(x)$ is called a multiplicative function.

Example: $f(x) = 1$ is a multiplicative function.

$f(x) = x$ is also a multiplicative function.

It's straightforward to check that $\tau(n)$ and $\sigma(n)$ are multiplicative functions(in fact, $\sigma_k(n)$ are all multiplicative functions).

Remark: Clearly, multiplicative function is determined by its values at the power of primes.

Related Topics 1: Amicable pair

A pair of positive integers (m, n) is called an amicable pair if $\sigma(m) = \sigma(n) = m + n$.

Example: $(220, 284)$, $(17296, 18416)$, $(9363584, 9437056)$, $\cdots$ are all amicable pairs(Check these yourself!).

It is not known whether there exist infinitely many amicable pairs.

Related Topics 2: Sum of squares

Let $S_k(n)$ be the number of representations of n as a sum of k squares of integers. For example,

$1 = (\pm 1)^2 + 0^2 + 0^2 + 0^2 = 0^2 + (\pm 1)^2 + 0^2 + 0^2 = 0^2 + 0^2 + (\pm 1)^2 + 0^2 = 0^2 + 0^2 + 0^2 + (\pm 1)^2$

hence there are $2+2+2+2=8$ possible representations of the number 1 as a sum of 4 squares of integers, so $S_4(1) = 8$.

Find exact formulas for $S_k(n)$ is a classical problem in number theory. There are exact formulas known in a number of cases, for example, Jacobi proved the following formula

$$S_4(n) = 8 \sum_{d \in \mathbb{Z}^+, d|n, 4 \nmid d} d$$

where d runs through all positive divisors of n but $4 \nmid d$.

For example, all positive divisors of 666 are not multiples of 4, so

$$S_4(666) = 8 \sum_{d \in \mathbb{Z}^+, d|666, 4\nmid d} d = 8 \sum_{d \in \mathbb{Z}^+, d|666} d = 8\sigma(666)$$

Since $666 = 2 \times 3^2 \times 37$, thus

$$S_4(666) = 8\sigma(666) = 8 \cdot 3 \cdot \frac{3^3 - 1}{3 - 1} \cdot 38 = 11856$$

Thus there are 11856 possible representations of the number 666 as a sum of 4 squares of integers.

Related Topics 3: Perfect Number

Def.: A positive integer n is called a Perfect Number, if $\sigma(n) = 2n$.

Example:

$\sigma(6) = 12 = 2 \times 6$, so 6 is a perfect number.

$\sigma(28) = \sigma(4)\sigma(7) = 7 \times 8 = 56 = 2 \times 28$, so 28 is a perfect number.

Q: Find all perfect numbers?

Theorem（Euclid）： If $2^p - 1$ is a prime, Then $2^{p-1}(2^p - 1)$ is a perfect number.

Proof:

Since $\sigma(n)$ is a multiplicative function, and $gcd(2^{p-1}, 2^p - 1) = 1$, So

$$\sigma(2^{p-1}(2^p - 1)) = \sigma(2^{p-1})\sigma(2^p - 1) = \frac{2^p - 1}{2 - 1}(2^p - 1 + 1) = (2^p - 1)2^p$$

i.e. $2^{p-1}(2^p - 1)$ is a perfect number. $\square$

Theorem（Euler）： If n is an even perfect number, then

$$n = 2^{p-1}(2^p - 1)$$

where $2^p - 1$ is a prime.

Proof:

First, n is even, so $n = t2^s$, where t is odd, and $s = ord_2 n$ is a positive integer.

Since $\sigma(n)$ is a multiplicative function, and $gcd(t, 2^s) = 1$(since t is odd), so

$$\sigma(n) = \sigma(t)\sigma(2^s) = \sigma(t)(2^{s+1} - 1)$$

On the other hand, n is a perfect number, so

$$\sigma(n) = 2n = 2^{s+1}t$$

Combining these, we get

$$\sigma(t)(2^{s+1} - 1) = 2^{s+1}t \qquad (*)$$

Since $2^{s+1} - 1$ and 2^{s+1} are adjacent integers, thus they are coprime integers(We'll prove it later). So 2^{s+1} is a divisor of $\sigma(t)$.

Let $\sigma(t) = q2^{s+1}$, Apply this to (*), we get $t = q(2^{s+1} - 1)$. Note that $2^{s+1} - 1 \neq 1$(since $s = ord_2 n$ is a positive integer), so $t \neq q$.

Now, we have $\sigma(t) = q2^{s+1} = t + q$,

If $q \neq 1$, then q is a positive divisor of t, and is different from 1 or t.

By definition of $\sigma(t)$, $\sigma(t) \geq 1 + t + q$, a contradiction to $\sigma(t) = t + q$.

So $q = 1$, $t = 2^{s+1} - 1$.

Hence $\sigma(t) = t + 1$, which means that t has only two positive divisors: 1 and t itself, so t is a prime.

So $n = t2^s = (2^{s+1} - 1)2^s$, where $2^{s+1} - 1$ is a prime. $\square$

Mersenne Prime

Def.: A prime of the form $2^p - 1$ is called a <u>Mersenne Prime</u>.

Remark:

- It's easy to see that only if p is a prime, $2^p - 1$ "may be" a prime.
- Conjecture: There are infinitely many Mersenne primes.

  See textbook(Section 7.3) for more details.

Odd Perfect Number

Euler gave a perfect answer to even perfect number.

Conj： Are there odd perfect numbers?

Primality Test and Factorization

By Fundamental Theorem of Arithmetic, every integer greater than 1 can be written uniquely as the product of primes.

Now, given an integer $n \gg 1$, how to get n's factorization? In particular, how to determine(efficiently) if n is prime?

• Primality Test and Factorization

Lemma: If n is a composite number, then n has a prime factor smaller than or equal to $[\sqrt{n}]$, and vice versa.

Proof:

If n is a composite number, then $n = ab$, where $a, b > 1$.

WLOG(short for without loss of generality), assume $a \le b$, so $a^2 \le ab = n$, $a \le [\sqrt{n}]$。

Since $a > 1$, so a has prime factors.

Clearly, prime factors of a are also prime factors of b. We get the first part of the statement.

The second part of the statement is trivial. $\square$

By the above lemma , we have the following(Primality Test and Factorization) "Trial division" :

Example: Is 139 a prime or not?

Solution:

$\sqrt{139} \approx 11.79$, $[\sqrt{139}] = 11$. Primes smaller than or equal to 11 are: 2、3、5、7、11. We need to check if they are prime factors of 139(If one of them is a prime factor of 139, then 139 is a composite, otherwise, 139 is a prime).

$$139 = 2 \times 69 + 1 \qquad 2 \nmid 139$$

$$139 = 3 \times 46 + 1 \qquad 3 \nmid 139$$

$$139 = 5 \times 27 + 4 \qquad 5 \nmid 139$$

$$139 = 7 \times 19 + 6 \qquad 7 \nmid 139$$

$$139 = 11 \times 12 + 7 \qquad 11 \nmid 139$$

So 139 is a prime.

Remarks

- For a given integer n(in decimal representation), we have some quick methods to check if n has prime factors $2, 3, 5, 11$:

  Let n be an integer, $(a_k a_{k-1} \cdots a_0)_{10}$ be the decimal representation of n. Prove the following:

  a) n can be divided by 2 iff(short for if and only if) the last digit of n can be divided by 2(i.e. a_0 can be divided by 2).

  b) n can be divided by 5 iff the last digit of n can be divided by 5(i.e. a_0 can be divided by 5).

  c) n can be divided by 3 iff the sum of digits of n can be divided by 3(i.e. $a_0 + a_1 + \cdots + a_k$ can be divided by 3).

  d) n can be divided by 11 iff the sum of digits in the odd positions of

n minus the sum of digits in the even positions of n can be divided by 11(i.e. $(a_0 + a_2 + a_4 + \cdots) - (a_1 + a_3 + a_5 + \cdots)$ can be divided by 11).

- Based on "Trial division", there is a method called "Eratosthenes Sieve" to find all primes from 1 to n.(See Textbook Section 3.1)

- When $n \gg 1$, "Trial division" is inefficient: it takes $\Omega(\sqrt{n})$ steps to determine if n is prime.

Fermat's factorization method

When an odd integer n can be factorize as $n = ab$ where $|a - b|$ not too large, Fermat's factorization method is an efficient method.

Lemma: If n is an odd positive integer, then there is a one-to-one correspondence between factorizations of n into two positive integers and differences of two squares that equal n.

Idea of Proof:

If $n = ab$, then

$$n = ab = (\frac{a+b}{2})^2 - (\frac{a-b}{2})^2$$

Conversely $n = s^2 - t^2$, then

$$n = (s+t)(s-t)$$

Fermat's factorization method

- Input: An odd integer n greater than 1.
- Step1: Take $t = \lceil \sqrt{n} \rceil$
- Step2: Check if $t^2 - n$ is a square.

  Yes, then we get a factorization of n.

  No, let $t = t + 1$.
- Step3: Check if $t = \frac{n+1}{2}$.

  Yes, Output: "n is a prime number".

  No, goto step 2.

Example: Is 6077 a prime or a composite? Give your reason. If 6077 is a composite, factorize it into prime powers.

Solution:

$$t = \lceil \sqrt{6077} \rceil = 78$$

$78^2 - 6077 = 7$ is not a square.

$79^2 - 6077 = 164$ is not a square.

$80^2 - 6077 = 323$ is not a square.

$81^2 - 6077 = 484 = 22^2$ is a square!

So

$$6077 = 81^2 - 22^2 = (81 - 22)(81 + 22) = 59 \times 103$$

So 6077 is a composite and $6077 = 59 \times 103$.

Remark

Only if n can be factorize as $n = ab$ where $|a - b|$ not too large, Fermat's factorization method is an efficient method, otherwise, it's inefficient.

Example: Use Fermat's factorization to check if 3287 is a prime and factorize it when it is a composite.

Solution:

$$t = \lceil \sqrt{3287} \rceil = 58$$

$58^2 - 3287 = 77,$ is not a square.

$59^2 - 3287 = 194,$ is not a square.

$60^2 - 3287 = 313,$ is not a square.

$61^2 - 3287 = 434,$ is not a square.

$62^2 - 3287 = 557,$ is not a square.

$63^2 - 3287 = 682,$ is not a square.

$64^2 - 3287 = 809,$ is not a square.

$65^2 - 3287 = 938,$ is not a square.

$66^2 - 3287 = 1069,$ is not a square.

$67^2 - 3287 = 1202,$ is not a square.

$68^2 - 3287 = 1337,$ is not a square.

$69^2 - 3287 = 1474,$ is not a square.

$70^2 - 3287 = 1613,$ is not a square.

$71^2 - 3287 = 1754,$ is not a square.

$72^2 - 3287 = 1897,$ is not a square.

$73^2 - 3287 = 2042,$ is not a square.

$$74^2 - 3287 = 2189, \text{ is not a square.}$$

$$75^2 - 3287 = 2328, \text{ is not a square.}$$

$$76^2 - 3287 = 2489, \text{ is not a square.}$$

$$77^2 - 3287 = 2642, \text{ is not a square.}$$

$$78^2 - 3287 = 2797, \text{ is not a square.}$$

$$79^2 - 3287 = 2954, \text{ is not a square.}$$

$$80^2 - 3287 = 3113, \text{ is not a square.}$$

$$81^2 - 3287 = 3274, \text{ is not a square.}$$

$$82^2 - 3287 = 3437, \text{ is not a square.}$$

$$83^2 - 3287 = 3602, \text{ is not a square.}$$

$$84^2 - 3287 = 3769, \text{ is not a square.}$$

$$85^2 - 3287 = 3938, \text{ is not a square.}$$

$$86^2 - 3287 = 4109, \text{ is not a square.}$$

$87^2 - 3287 = 4282$, is not a square.

$88^2 - 3287 = 4457$, is not a square.

$89^2 - 3287 = 4634$, is not a square.

$90^2 - 3287 = 4813$, is not a square.

$91^2 - 3287 = 4994$, is not a square.

$92^2 - 3287 = 5177$, is not a square.

$93^2 - 3287 = 5362$, is not a square.

$94^2 - 3287 = 5549$, is not a square.

$95^2 - 3287 = 5738$, is not a square.

$96^2 - 3287 = 5929 = 77^2$, is a square!

So $3287 = 96^2 - 77^2 = (96 - 77) \times (96 + 77) = 19 \times 173$, thus 3287 is a composite and $3287 = 19 \times 173$.

谢谢！