初等数论

吴 伊 涛

2022 年春

Lecture 9. Congruence

We already use the facts " odd + odd = even, odd × odd = odd…" many times. We can summarize these facts as the following:

" + "

	odd	even
odd	even	odd
even	odd	even

" × "

	odd	even
odd	odd	even
even	even	even

These seems really elementary, can we get anything interesting facts from these?

Let's see…

First, let's generalize the above table:

Clearly, $\forall n \in \mathbb{Z}$, the remainder of n divides by 3 should be one of 0, 1, 2. i.e. n is of $3k$, $3k+1$, $3k+2$ type integer.

Thus we have the following table:

" + "

	$3k$	$3k+1$	$3k+2$
$3k$	$6k$	$6k+1$	$6k+2$
$3k+1$	$6k+1$	$6k+2$	$6k+3$
$3k+2$	$6k+2$	$6k+3$	$6k+4$

" × "

	$3k$	$3k+1$	$3k+2$
$3k$	$9k^2$	$9k^2+3k$	$9k^2+6k$
$3k+1$	$9k^2+3k$	$9k^2+6k+1$	$9k^2+9k+2$
$3k+2$	$9k^2+6k$	$9k^2+9k+2$	$9k^2+12k+4$

Now, if we just record the remainder of the number divided by 3, the above two tables turns like:

"+"

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

"×"

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

We can find, from the above multiplication table, that "a $3k+2$ type integer n, if we factorize n as $n = a \cdot b$, then a or b is also a $3k+2$ type integer". Thus we get the following facts:

Prop. A $3k+2$ type positive integer always has a $3k+2$ type prime factor.

Proof:

Clearly, all primes except 3 are of $3k+1$ type or $3k+2$ type.

If n is a $3k+2$ type integer, then $3 \nmid n$.

By Fundamental Theorem of Arithmetic, ~~$n = (-1)$~~ $n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_l^{a_l}$.

If $p_1, p_2, \cdots p_l$ are all of $3k+1$ type integer, then by the multiplication table above, $p_1^{a_1} \cdot p_2^{a_2} \cdots p_l^{a_l}$ is also a $3k+1$ type integer. A contradiction. So, at least one of $p_1, p_2, \cdots p_l$ is a $3k+2$ type integer. $\square$

We can deduce the following consequence:

Theorem: There are infinitely many $3k+2$ type primes.

Proof: Assume not, let $p_1 = 2$, $p_2 = 5$, $\cdots$, p_l are all $3k+2$ type primes.

We construct $N = 3p_2p_3\cdots p_l + 2$.

As N is a $3k+2$ type positive integer, by the above prop, N has a $3k+2$ type prime factor q. So q is one of $p_1, p_2, \cdots p_l$.

If $q = p_1 = 2$, then $q \mid N-2 = 3 \cdot p_2 \cdot p_3 \cdots p_l$, which is an odd number, a contradiction.

If $q = p_i$, $i \in \{2, 3, \cdots, l\}$, then $q \mid 3p_2 \cdots p_l$, thus $q \mid N - 3p_2\cdots p_l = 2$, also a contradiction.

So there are infinitely many $3k+2$ type primes. $\square$

Exercise:

1. Prove that there are infinitely many $4k+3$ type primes.
(Hint: Prove that a $4k+3$ type positive integer always has a $4k+3$ type prime factor).

Example Solve the Diophantine equation

$$x^{2022} + 115x^2 + 2333 = 0$$

Solution:

Assume x_0 is an integral solution of the Diophantine equation $x^{2022} + 115x^2 + 2333 = 0$.

If x_0 is an odd number, then x_0^{2022}, $115x_0^2$ both are odd numbers, thus $x_0^{2022} + 115x_0^2 + 2333$ is a sum of three odd numbers, which is still an odd number, thus unequal to 0. A contradiction.

If x_0 is an even number, then x_0^{2022}, $115x_0^2$ both are even numbers, thus $x_0^{2022} + 115x_0^2 + 2333$ is a sum of an odd number and two even numbers, which is an odd number, thus unequal to 0. A contradiction.

Thus the Diophantine equation $x^{2022} + 115x^2 + 2333 = 0$ is unsolvable.

· Congruence (in $\mathbb{Z}$).

Def: Let $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$.

We say that a is congruent to b modulo m if $m \mid b-a$.

We denote it by $a \equiv b \pmod{m}$.

E.g. $3 \equiv 18 \pmod{5}$, $19 \equiv 11 \pmod{2}$, $2020 \equiv 4 \pmod{9}$.

Prop. Congruence modulo m is an equivalence relation on the set of integers $\mathbb{Z}$, i.e.

1) $a \equiv a \pmod{m}$, $\forall a \in \mathbb{Z}$,

2) $a \equiv b \pmod{m}$ implies $b \equiv a \pmod{m}$, $\forall a, b \in \mathbb{Z}$,

3) $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ implies $a \equiv c \pmod{m}$ $\forall a, b, c \in \mathbb{Z}$.

Proof:

1) $a - a = 0$ and $m \mid 0$.

2) If $m \mid b-a$, then $m \mid a-b$, i.e. $b \equiv a \pmod{m}$

3) If $m \mid b-a$, $m \mid c-b$.

then $m \mid c-a = (c-b)+(b-a)$, i.e. $a \equiv c \pmod{m}$.

$\square$

Prop. 1) If $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$,

then $a + c \equiv b + d \pmod{m}$

2) If $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$

then $a - c \equiv b - d \pmod{m}$.

3) If $a \equiv b \pmod{m}$, $t \in \mathbb{Z}$,

then $ta \equiv tb \pmod{m}$.

4) If $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$

Then $a \cdot c \equiv b \cdot d \pmod{m}$.

Proof:

1) 2) 3) leave to the reader.

4). If $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$.

Then $m \mid b-a$, $m \mid d-c$.

Thus $bd - ac = (b-a) \cdot d + a \cdot (d-c)$ is a multiple of m,

$\therefore$ $ac \equiv bd \pmod{m}$. $\square$

Cor. Let $f(x) \in \mathbb{Z}[x]$ be a polynomial with integral coefficients.

If $a \equiv b \pmod{m}$, then $f(a) \equiv f(b) \pmod{m}$.

Cor. Given $f(x) \in \mathbb{Z}[x]$, then $\forall k \in \mathbb{Z}$,

$f(k) \equiv f(0) \pmod{2}$ or $f(k) \equiv f(1) \pmod{2}$.

Example Solve the Diophantine equation

$$x^{2022} + 115x^2 + 2333 = 0$$

Solution:

Denote the Diophantine equation $x^{2022} + 115x^2 + 2333 = 0$ by $f(x) = 0$.

Assume x_0 is an integral solution of the Diophantine equation $f(x) = 0$.

Clearly, $x_0 \equiv 0$ or $1(mod\ \ 2)$.

If $x_0 \equiv 0(mod\ \ 2)$, then $f(x_0) \equiv f(0)(mod\ \ 2)$, so $f(x_0) \equiv 2333 \equiv 1(mod 2)$, a contradiction to $f(x_0) \equiv 0(mod\ \ 2)$.

If $x_0 \equiv 1(mod\ \ 2)$, then $f(x_0) \equiv f(1)(mod\ \ 2)$, so $f(x_0) \equiv 1+115+2333 \equiv 1(mod 2)$, a contradiction to $f(x_0) \equiv 0(mod\ \ 2)$.

Thus the Diophantine equation $x^{2022} + 115x^2 + 2333 = 0$ is unsolvable.

Remark

- In general, we can prove:

  Given an integral coefficients polynomial $f(x)$, if the constant term of $f(x)$(i.e. $f(0)$) and the sum of all coefficients of $f(x)$(i.e. $f(1)$) both are odd numbers, then $f(x) = 0$ is unsolvable.

- Try to solve the Diophantine equation

$$x^{2022} - 2022x^{2020} + 1234 = 0$$

Example Solve the Diophantine equation

$$x^2 + y^2 = 3z^2$$

Solution:

Assume (a, b, c) is a primitive integer solution of the Diophantine equation $x^2 + y^2 = 3z^2$, i.e. $gcd(a, b, c) = 1$.

Since $a^2 + b^2 \equiv 3c^2 \equiv 0(mod3)$, it then follows that $a^2 \equiv 0(mod3)$ and $b^2 \equiv 0(mod3)$, which leads to $3|a$ and $3|b$.

Apply $a = 3u, b = 3v$ to the equation $a^2 + b^2 = 3c^2$, it then follows that $3|c$.

So $3|gcd(a, b, c) = 1$, a contradiction.

So the Diophantine equation $x^2 + y^2 = 3z^2$ has no primitive integer solutions. The only possible solution is $(0, 0, 0)$.

By checking, we find $(0, 0, 0)$ is indeed a solution. Thus the Diophantine equation $x^2 + y^2 = 3z^2$ has a unique solution $(0, 0, 0)$.

- Repeated squaring method.

Given $a, b, m \in \mathbb{Z}^+$, we want to calculate the remainder of a^b divided by m.

We introduce a notation first:

Def: $a \pmod m$:= the remainder of a divided by m.

E.g. $11 \pmod 8 = 3$, $30 \pmod{11} = 8$, $2020 \pmod 9 = 4$

$8^2 \pmod 5 = 4$.

E.g. Calculate $11^{48} \pmod{2020}$.

Clearly, it is cumbersome to calculate 11^{48} out and then divide it by 2020. We introduce the following "Repeated squaring method"

Sol:

$11 \pmod{2020} = 11$, $11^2 \pmod{2020} = 11^2 = 121$

$11^4 \pmod{2020} = 121^2 \pmod{2020} = 501$

$11^8 \pmod{2020} = 501^2 \pmod{2020} = 521$

$11^{16} \pmod{2020} = 521^2 \pmod{2020} = 761$

$11^{32} \pmod{2020} = 761^2 \pmod{2020} = 1401$.

Now, $48 = 32 + 16$.

$\therefore 11^{48} \pmod{2020} = 11^{32} \cdot 11^{16} \pmod{2020} = \left(11^{32} \pmod{2020} \cdot 11^{16} \pmod{2020}\right) \pmod{2020}$

$= 1401 \times 761 \pmod{2020}$

$= 1621$.

The above method is called "repeated squaring method". The principle is:

$$ab \pmod m = \big(a \pmod m \cdot b \pmod m\big) \pmod m$$

which clearly from $a \equiv x \pmod m,\ b \equiv y \pmod m \Longrightarrow ab \equiv xy \pmod m$ (page 126, 4)).

E.g. $119 \times 748 \pmod{10} = \big(119 \pmod{10} \times 748 \pmod{10}\big) \pmod{10}$

$= 9 \times 8 \pmod{10} = 2.$

Now, let's state the "repeated squaring method"

Aim: Calculate $a^b \pmod m$

Step 1: Convert b to binary representation:

$$b = (C_k C_{k-1} \cdots C_1 C_0)_2$$

Step 2: Calculate $a^{2^i} \pmod m$, $i = 0, 1, 2, \cdots k$

Note that $a^{2^{j+1}} \pmod m = \left(a^{2^j} \pmod m\right)^2 \pmod m$

So, just "repeated square".

Step 3: Multiply those $a^{2^i} \pmod m$ where $C_i = 1$. (Actually more delicate if $m \gg 1$).

In fact, $b = C_k \cdot 2^k + C_{k-1} \cdot 2^{k-1} + \cdots + C_1 \cdot 2 + C_0$.

$$\therefore\ a^b \pmod m = \Big(\big(a^{2^k}\big)^{C_k} \pmod m \cdot \big(a^{2^{k-1}}\big)^{C_{k-1}} \pmod m \cdots a^{C_0} \pmod m\Big) \pmod m$$

(Note that if $C_i = 0$, $(a^{2^i})^{C_i} \pmod m = 1$.

if $C_i = 1$, $(a^{2^i})^{C_i} \pmod m = a^{2^i} \pmod m$.

E.g. Calculate $999^{1000} \pmod{1001}$.

Sol: Since $999 \equiv -2 \pmod{1001}$, $999^{1000} \equiv (-2)^{1000} \equiv 2^{1000} \pmod{1001}$

$\therefore 999^{1000} \pmod{1001} = 2^{1000} \pmod{1001}$.

Now, convert 1000 to binary representation, we get:

$$1000 = (1111101000)_2 = 2^3 + 2^5 + 2^6 + 2^7 + 2^8 + 2^9$$

Then, let's calculate $2^{2^i} \pmod{1001}$, $i = 0, 1, 2, \cdots, 9$.

$2^{2^0} \pmod{1001} = 2$. $\qquad 2^{2^1} \pmod{1001} = 2^2 \pmod{1001} = 4$

$2^{2^2} \pmod{1001} = 4^2 \pmod{1001} = 16$, $\quad 2^{2^3} \pmod{1001} = 16^2 \pmod{1001} = 256$

$2^{2^4} \pmod{1001} = 256^2 \pmod{1001} = 65536 \pmod{1001} = 471$.

$2^{2^5} \pmod{1001} = 471^2 \pmod{1001} = 221841 \pmod{1001} = 620$.

$2^{2^6} \pmod{1001} = 620^2 \pmod{1001} = 384400 \pmod{1001} = 16$

$2^{2^7} \pmod{1001} = 16^2 \pmod{1001} = 256$

$2^{2^8} \pmod{1001} = 256^2 \pmod{1001} = 471$

$2^{2^9} \pmod{1001} = 471^2 \pmod{1001} = 620$.

Thus

$$\begin{aligned} 2^{1000} \pmod{1001} &= 2^{2^3} \cdot 2^{2^5} \cdot 2^{2^6} \cdot 2^{2^7} \cdot 2^{2^8} \cdot 2^{2^9} \pmod{1001} \\ &= 256 \times 620 \times 16 \times 256 \times 471 \times 620 \pmod{1001} \\ &= 562. \end{aligned}$$

So $999^{1000} \pmod{1001} = 562$.

Rmk 1: We will introduce some simplifications of the above method. Anyway, the "repeated squaring method" shows that $a^b \pmod m$ is easy to get: roughly $O(\log_2 b)$ times of two integers' (smaller than m) multiplications.

Rmk 2: Note that $2^{2^i} \pmod{1001}$ is a cyclic sequence:

$$2, 4, 16, 256, 471, 620, 16, 256, 471, 620, \cdots$$

We will explain these later.

Remark

- The Repeated Squaring Method is efficient.

Example

Alice is using her computer to calculate

$$1234567890987654321^{2021202220232024}(mod 31415926535897932626)$$

If the computer use 1 second to calculate the product of two 20-digits number, and 1 second to calculate the remainder of a 40-digits number divided by a 20-digits number, then is it possible to get the result in 5 minutes? Give your reason and estimate a bound of time.

Solution

Let's use "repeated squaring method".

First, write out the binary presentation of $b = 2021202220232024$, it's just divide b by 2 repeatedly, thus takes almost no time.

Now, suppose we already know $x^{2^i}(modm)$(where $x = 12345678900987654321$, $m = 31415926535897932626$), which should be a 20-digit(or less) number, then we square it to get a 40-digit(or less) number and then divide the result by m, all these cost at most 2 seconds, we then get $x^{2^{i+1}}(modm)$, thus by induction, we could get $x^{2^i}(modm)$ for all $i \leq k$ in $2k$ seconds.

Now multiply all $x^{2^i}(mod m)$ if the i-th digit in the binary presentation is 1 in the same way as above: multiply the first 2 numbers and then divide it by m, and then multiply the result with the 3rd number and then divide it by m......

Thus the total time is at most $4k$ where $k = [log_2 b] = 50$, so we can finish the computation in 5 minutes. In fact, an upper bound of the time is 200 seconds.

谢谢！