初等数论

吴 伊 涛

2022 年春

Lecture 12. Congruence Equation

Now, we want to consider some congruence equations, e.g. $3x \equiv 5 \pmod{11}$, $x^2 \equiv -1 \pmod{121}$, ... etc.

Recall: when we consider an equation, there are 3 elementary problems:

Q1: Is the equation solvable?

Q2: If it is solvable, how many solutions does it have?

Q3: If it is solvable, find all its solutions.

Also, note that, if $f(x) \in \mathbb{Z}[x]$ is a polynomial with integral coefficients, $a \equiv b \pmod{m}$, then $f(a) \equiv f(b) \pmod{m}$ (p126, Cor).

So, if x_0 is a solution of $f(x) \equiv 0 \pmod{m}$, then all integers congruent to x_0 modulo m are also solutions of $f(x) \equiv 0 \pmod{m}$.

E.g. 9 is a sol. of $3x \equiv 5 \pmod{11}$, then we immediately know that $9+11k$, $k \in \mathbb{Z}$ are also sol. of this equation.

These solutions, actually are same when modulo m, are called <u>equivalent solutions</u>.

The number of solutions of an algebraic congruence equation $f(x) \equiv 0 \pmod{m}$ is defined to be the number of inequivalent solutions.

E.g. $3x \equiv 3 \pmod{15}$.

It is easy to check: from 0 to 14, 1, 6, 11 are solutions of this equation. 16 is also a solution, but $x = 16$ is equivalent to the solution $x = 1$.

Thus, the equation $3x \equiv 3 \pmod{15}$ has 3 solutions in total, and we write them as:

$$x \equiv 1 \pmod{15}, \quad x \equiv 6 \pmod{15}, \quad x \equiv 11 \pmod{15}.$$

It is helpful to see these from another point of view:

The congruence equation $f(x) \equiv 0 \pmod{m}$ actually corresponds to the equation $f(x) = 0$ in $\mathbb{Z}/m\mathbb{Z}$. The number of inequivalent solutions of $f(x) \equiv 0 \pmod{m}$ is actually the number of solutions of $f(x) = 0$ in $\mathbb{Z}/m\mathbb{Z}$.

E.g. $3x \equiv 3 \pmod{15} \longleftrightarrow 3x = \bar{3}$ in $\mathbb{Z}/15\mathbb{Z}$

$x \equiv 1 \pmod{15}$, $x \equiv 6 \pmod{15}$, $x \equiv 11 \pmod{15}$ $\longleftrightarrow x = \bar{1}, \bar{6}, \overline{11}$.

We just consider equations of one varible in this section. But equations with multi-varibles have the same problem: If $x_1 \equiv y_1 \pmod{m}$, $x_2 \equiv y_2 \pmod{m}$, $\cdots$ $x_k \equiv y_k \pmod{m}$, then $f(x_1, x_2, \cdots x_k) \equiv f(y_1, y_2, \cdots y_k) \pmod{m}$. So we also have to consider inequivalent solutions.

$ax \equiv c \pmod{m}$.

The simplest congruence equation is $ax \equiv c \pmod{m}$, where $a, c \in \mathbb{Z}$, $m \in \mathbb{Z}^+$.

We consider Q1 first:

$ax \equiv c \pmod{m}$ has a solution $x \equiv x_0 \pmod{m}$

$\Leftrightarrow$ $a \cdot x_0 \equiv c \pmod{m}$, $\exists\, x_0 \in \mathbb{Z}$.

$\Leftrightarrow$ $\exists\, y_0 \in \mathbb{Z}$, s.t. $ax_0 - c = my_0$

$\Leftrightarrow$ The Diophantine equation $ax + my = c$ has a solution $(x_0, -y_0)$.

$\Leftrightarrow$ $g.c.d.(a, m) \mid c$.

The above discussion actually also tells us how to solve the equation $ax \equiv c \pmod{m}$: If you find all solutions of $ax+my=c$, then you find all solutions of $ax \equiv c \pmod{m}$.

More explicitly, if $(x_0, -y_0)$ is a special solution of $ax+my=c$, then the general solutions of $ax+my=c$ are:

$$\begin{cases} x = x_0 + \dfrac{m}{d} \cdot t \\ y = -y_0 - \dfrac{a}{d} \cdot t \end{cases} \quad t \in \mathbb{Z}, \text{ here } d = g.c.d.(a, m).$$

Thus $x_0 + \frac{m}{d} \cdot t$ $(t \in \mathbb{Z})$ are all integers satisfying the congruence equation. But these solutions may have equivalent ones, for example, x_0 and $x_0 + m$ are equivalent. So, how many inequivalent solutions in $x_0 + \frac{m}{d} t$ $(t \in \mathbb{Z})$?

Claim: There are exactly d inequivalent solutions, and

$$x_0 + \frac{m}{d} \cdot k, \quad k = 0, 1, 2, \cdots, d-1$$

are pairwise inequivalent solutions of $ax \equiv c \pmod m$

Proof:

Clearly, $x_0 + \frac{m}{d} \cdot k$ $(k = 0, 1, 2, \cdots, k-1)$ are pairwise inequivalent solutions of $ax \equiv c \pmod m$. (Since the difference between any two is a positive integer less than m).

Now, we have to show: $\forall t \in \mathbb{Z}$, $x_0 + \frac{m}{d} \cdot t$ is equivalent to one of $x_0 + \frac{m}{d} \cdot k$ $(k = 0, 1, 2, \cdots k-1)$.

Use Division Algorithm, $t = q \cdot d + r$, $0 \leq r \leq d-1$.

Then $x_0 + \frac{m}{d} \cdot t \equiv x_0 + \frac{m}{d} \cdot r \pmod m$. Thus the solution $x = x_0 + \frac{m}{d} \cdot t$ is equivalent to $x = x_0 + \frac{m}{d} \cdot r$. $\square$

Summarizing above, we have the following proposition:

Prop. Let $m \in \mathbb{Z}^+$, $a, c \in \mathbb{Z}$, $a \neq 0$, $d = g.c.d.(a, m)$.

The congruence equation $ax \equiv c \pmod m$ has solutions if and only if $d | b$.

If $d | b$, then there are exactly d solutions.

If x_0 is a solution (which can be find via applying Extended Euclidean Algorithm on the Diophantine equation $ax + my = c$), then all solutions of $ax \equiv c \pmod m$ are:

$$x \equiv x_0 \pmod m, \quad x \equiv x_0 + \frac{m}{d} \pmod m, \quad \cdots, \quad x \equiv x_0 + \frac{m}{d} \cdot (d-1) \pmod m.$$

Cor. Let $m \in \mathbb{Z}^+$, $a \in \mathbb{Z}$ and g.c.d. $(a, m) = 1$. $c \in \mathbb{Z}$.

Then $ax \equiv c \pmod{m}$ has one and only one solution.

In particular, $ax \equiv 1 \pmod{m}$ has a unique solution,

and we call this solution as a^{-1} (modulo m).

The above corollary shows that why we always consider the residue class coprime to m: If a is coprime to m, then we can multiply the equation $a \cdot b \equiv ac \pmod{m}$ by a^{-1}, we then get $b \equiv c \pmod{m}$. We have "division" in case g.c.d. $(a, m) = 1$!

E.g. Solve the congruence equation

$$6x \equiv 3 \pmod{15}.$$

Sol:

1st, solve the equation $6x + 15y = 3$.

We find a special solution $x = 3$, $y = -1$.

2nd. Use the above prop.

So, all sol. of the congruence equation $6x \equiv 3 \pmod{15}$ are: (Don't forget to check your answer!)

$$x \equiv 3 \pmod{15}, \quad x \equiv 8 \pmod{15}, \quad x \equiv 13 \pmod{15}.$$

Note: We always simplify our final solutions to the integers between 0 and $m-1$.

Example: Solve $123x \equiv 456 \pmod{2022}$.

Solution:

Step 1: Calculate $\gcd(123, 2022)$.

$a = 2022$	
$b = 123$	$q_1 = 16$
$r_1 = 54$	$q_2 = 2$
$r_2 = 15$	$q_3 = 3$
$r_3 = 9$	$q_4 = 1$
$r_4 = 6$	$q_5 = 1$
$r_5 = 3$	$q_6 = 2$
$r_6 = 0$	

$\therefore \gcd(123, 2022) = r_5 = 3 \mid 456$

So $123x \equiv 456 \pmod{2022}$ is soluable, It has 3 solutions.

Step 2: Use Extended Euclidean Algorithm to find a special solution of $123x + 2022y = 456$.

k	0	1	2	3	4	5
q_k		16	2	3	1	1
P_k	1	16	33	115	148	263
Q_k	0	1	2	7	9	16

$$Q_k \cdot a - P_k \cdot b = (-1)^{k+1} \cdot r_k$$

$$\therefore \quad 2022 \times 16 - 123 \times 263 = 3$$

So $123x + 2022y = 3$ has a special solution $(-263, 16)$.

So $123x + 2022y = 456$ has a special solution:

$$x = -263 \times \frac{456}{3} = -39976$$

$$y = 16 \times \frac{456}{3} = 2432$$

Thus $123x \equiv 456 \pmod{2022}$ has a special solution:

$$x \equiv -39976 \equiv 464 \pmod{2022}.$$

Step 3: Write out all solutions of $123x \equiv 456 \pmod{2022}$:

$123x \equiv 456 \pmod{2022}$ has 3 solutions:

$$x \equiv 464 \pmod{2022}$$

$$x \equiv 464 + \frac{2022}{3} \equiv 1138 \pmod{2022}$$

$$x \equiv 464 + 2 \times \frac{2022}{3} \equiv 1812 \pmod{2022}.$$

Step 4: Check your solutions!

Leave to you.

Remark

Sometimes, we can simplify the repeated squaring method via ”finding the inverse”.

Example Calculate Calculate $2023^{1000}(mod 2048)$.

Solution:

$2048 = 2^{11}$, $\phi(2048) = 2^{11} - 2^{10} = 1024$. Since 2023 is coprime to 2048, by Euler’s theorem,

$$2023^{1024} \equiv 1(mod \;\; 2048)$$

So

$$2023^{1000} \equiv 2023^{-24}(mod \;\; 2048)$$

Now, use repeated squaring method(leave to you), we find

$$2023^{24} \equiv 1857(mod \;\; 2048)$$

Then, use extended Euclidean Algorithm to solve congruence equation $1857x \equiv 1(mod \ \ 2048)$(leave to you), we find $x \equiv 193(mod \ \ 2048)$.

So $2023^{1000}(mod 2048) = 193$.

Wilson's theorem

If p is a prime, then $(p-1)! \equiv -1(mod\ \ p)$.

Example:

$p = 7$

$6! \equiv 720 \equiv -1(mod\ \ 7)$.

$6! \equiv 1 \cdot (2 \cdot 4) \cdot (3 \cdot 5) \cdot 6 \equiv -1(mod\ \ 7)$.

Proof of Wilson's theorem

If $p = 2$, then $(p-1)! \equiv 1 \equiv -1 (mod \ \ 2)$.

Now, we can assume $p \geq 3$.

Claim 1: If a is an integer with $1 < a < p-1$, then there exists a unique integer b, s.t. $1 < b < p-1$, $b \neq a$, $ab \equiv 1(mod \ \ p)$.

Since a coprime to b, the congruence equation $ax \equiv 1(modp)$ has a unique solution $x \equiv b(mod \ \ p)$ with $1 \leq b \leq p-1$.

If $b = 1$, then $a \equiv ab \equiv 1(mod \ \ p)$, $a = 1$, a contradiction.

If $b = p-1$, then $a \equiv ab \equiv -1(mod \ \ p)$, $a = p-1$, also a contradiction.

Therefore, we can group the integers from 2 to $p-2$ into $\frac{p-3}{2}$ pairs of integers, such that the product of each pair congruent to 1 modulo p.

Thus

$$2 \cdot 3 \cdot \cdots \cdot (p-3) \cdot (p-2) \equiv 1 (mod p)$$

Hence,

$$(p-1)! \equiv 1 \cdot (2 \cdot 3 \cdot \cdots \cdot (p-3) \cdot (p-2)) \cdot (p-1) \equiv 1 \cdot 1 \cdot (-1) \equiv -1 (mod \ \ p)$$

$\square$

The converse of of Wilson's theorem is also true:

Theorem

If n is an integer greater than 2, and $(n-1)! \equiv -1(mod \;\; n)$, Then n is a prime.

Proof

Assume n is a composite and $(n-1)! \equiv -1(mod \;\; n)$.

Since n is a composite, we have:

$$n = ab, \quad 2 \leq a, b \leq n-1$$

Thus $a|(n-1)!$ since a is a factor of $(n-1)!$.

On the other hand, $a|(n-1)!+1$ since $n|(n-1)!+1$.

It follows that $a|1$, a contradiction. $\square$

Example:

$n = 18 = 2 \times 9$

$17! \equiv 1 \cdot 2 \cdot \cdots \cdot 9 \cdots 17 \equiv 0(mod \;\; 2 \times 9).$

In fact, if n is a composite greater than 5, then $(n-1)! \equiv 0(mod \;\; n)(3! \equiv 2(mod \;\; 4))$.

Theorem

n is a composite greater than 5, then $(n-1)! \equiv 0 (mod \ \ n)$.

Proof

Since n is a composite, we have:

$$n = ab, \ \ 2 \leq a \leq b \leq n-1$$

If $a \neq b$, then $(n-1)! = 1 \cdot 2 \cdots a \cdots b \cdots (n-1)$, thus $n = ab|(n-1)!$.

If $a = b$, since $n > 5$, so $a > 2$, $2a < a^2 = n$, thus $2a \leq n-1$.

Hence $(n-1)! = 1 \cdot 2 \cdots a \cdots 2a \cdots (n-1)$, thus $(a \cdot 2a)|(n-1)!$. We also have $n = a^2|(n-1)!$. $\square$

Remark

Wilson's theorem and its converse suggests us a primality Test:

Input: $n \gg 1$, n odd

Step 1: Calculate $(n-1)!(mod n)$;

If it equals to 0, then Output "n is a composite";

If it equals to $n-1$, then Output "n is a prime".

This is correct but inefficient since we don't have an efficient way to calculate $(n-1)!(mod n)$.

RSA cryptosystem

The most commonly used public key cryptosystem is the RSA cryptosystem (named after Ronald Rivest, Adi Shamir, and Leonard Adleman). The following is the principle:

Assume n is the product of two large primes p, q, e is a positive integer coprime to $\phi(n)$. Alice first translate the letters of her message into their numerical equivalents(00= blank, 01="A",02="B",03="C"...,26="Z".) and then form a block P. She then calculate $P^e(modn)$ to get a ciphertext block C and sends C to Bob. Now Bob has to decrypt the ciphertext block C to the block P and then get Alice's original message.

Principle of RSA cryptosystem:

For simplicity, assume P is coprime to n.

By Euler's theorem, we have:

$$P^{\phi(n)} \equiv 1(mod \ \ n)$$

Now, if we can find an integer d s.t. $ed \equiv 1(mod \ \ \phi(n))$, then

$$C^d \equiv P^{ed} \equiv P(mod \ \ n)$$

Example:

Let's try a naive example to illustrate how the RSA cryptosystem works:

Let $n = 2759 = 31 \times 89$ be the product of two primes, $e = 227$, and Bob receives the ciphertext block $C = 1207$. Please find Alice's original message.

Solution:

Step 1. Calculate $\phi(n)$:

$$\phi(n) = 30 \times 88 = 2640.$$

Step 2. Find d, such that $ed \equiv 1(mod\phi(n))$:

Use Extended Euclidean Algorithm(leave to you), we find $d \equiv 1163(mod 2640)$.

Step 3. Calculate $C^d(mod n)$, the result is block P :

Use Repeated Squaring Method(leave to you), we get $1207^{1163}(mod 2759) = 1511$, so $P = 1511$.

Step 4. Translate P into original message:

15="O", 11="K" So Alice's original message is "OK".

Suggest Reading

- （英）西蒙·辛格著，刘燕芬译，《The Code Book（码书）》，江西人民出版社，2018

谢谢！