初等数论

吴 伊 涛

2021 年秋

Recall: we define ”a residue class coprime(modulo m) to m” last week.

Q: Why consider such residue class?

A: Because we can make division with these kind of residue classes.

Prop Let m be a positive integer, a be an integer coprime to m. Then there exists an integer t, s.t. $ta \equiv 1(mod m)$. In particular, if $ax \equiv ay(mod \;\; m)$, then $x \equiv y(mod \;\; m)$.

Or, in the language of residue class, there exists a residue class(modulo m) $\bar{t}$ coprime to m, s.t. $\bar{t}\bar{a} = \bar{1}$, in particular, if $\bar{a}\bar{x} = \bar{a}\bar{y}$, then $\bar{x} = \bar{y}$.

We will see the proof later.

· Euler's Thm and FLT.

Recall that we have proved (page 138):

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

If x runs through a reduced system modulo m,

then ax also runs through a reduced residue system modulo m.

So, if x runs through $\{r_1, r_2, \cdots, r_{\phi(m)}\}$,

then ax runs through $\{ar_1, ar_2, \cdots, ar_{\phi(m)}\}$

It follows that

$$\{\overline{r_1}, \overline{r_2}, \cdots, \overline{r_{\phi(m)}}\} = \{\overline{ar_1}, \overline{ar_2}, \cdots, \overline{ar_{\phi(m)}}\}.$$

$$\therefore \overline{r_1} \cdot \overline{r_2} \cdots \cdot \overline{r_{\phi(m)}} = \overline{ar_1} \cdot \overline{ar_2} \cdots \cdot \overline{ar_{\phi(m)}}$$

$$\therefore \overline{r_1 \cdot r_2 \cdots r_{\phi(m)}} = \overline{a^{\phi(m)} \cdot r_1 \cdot r_2 \cdots r_{\phi(m)}}$$

$$\therefore a^{\phi(m)} \cdot r_1 \cdot r_2 \cdots r_{\phi(m)} \equiv r_1 \cdot r_2 \cdots r_{\phi(m)} \pmod{m}.$$

$$\therefore m \mid (a^{\phi(m)} - 1) \cdot r_1 \cdot r_2 \cdots r_{\phi(m)}.$$

Since $r_1, r_2, \cdots r_{\phi(m)}$ all coprime to m, thus the product $r_1 \cdot r_2 \cdots r_{\phi(m)}$ is also coprime to m. (~~The~~ Proof is easy and leave to the reader)

So $m \mid a^{\phi(m)} - 1$, i.e. $a^{\phi(m)} \equiv 1 \pmod{m}$.

We've proved the following Euler's theorem:

Euler's Theorem:

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

Then $$a^{\phi(m)} \equiv 1 \pmod{m}$$

E.g. $m = 1001$, $a = -2$.

Since g.c.d.$(a, m) = 1$, $m = 1001 = 7 \times 11 \times 13$,

$\phi(1001) = (7-1) \times (11-1) \times (13-1) = 720$.

By Euler's theorem, we have: $(-2)^{720} \equiv 1 \pmod{1001}$.

Now, let's consider the case m is a prime, in this case, $\phi(m) = m-1$. We then get the following corollary from Euler's theorem:

Fermat's Little Theorem:

Let p be a prime, $a \in \mathbb{Z}$, $p \nmid a$.

Then $$a^{p-1} \equiv 1 \pmod{p}$$

E.g. $p = 7$, $a = 5$, then $5^6 \equiv 1 \pmod{7}$

$p = 11$, $a = 8$, then $8^{10} \equiv 1 \pmod{11}$

Example Calculate $3^{12345}(mod \ \ 7)$.

Solution

Since 7 is a prime and 3 is coprime to 7, by Fermat's little theorem,

$$3^6 \equiv 1(mod \ \ 7)$$

So

$$3^{12345} \equiv 3^{12342} \cdot 3^3 \equiv (3^6)^{2057} \cdot 3^3 \equiv 1 \cdot 27 \equiv 6(mod \ \ 7)$$

Hence $3^{12345}(mod \ \ 7) = 6$.

Example Calculate $2022^{12345}(mod\ \ 97)$.

Solution

Since 97 is a prime and 2022 is coprime to 97, by Fermat's little theorem,

$$2022^{96} \equiv 1(mod\ \ 97)$$

So

$$2022^{12345} \equiv 2022^{12288} \cdot 2022^{57} \equiv (2022^{96})^{128} \cdot 2022^{57} \equiv 2022^{57}(mod\ \ 97)$$

Now, use repeated squaring method,

Step1: Convert 57 to binary representation.

$$57 = (111001)_2 = 1 + 2^3 + 2^4 + 2^5$$

Step2: Calculate $2022^{2^i}(mod\ \ 97)$, where $i = 0, 1, 2, 3, 4, 5$.

$$2022^{2^0}(mod\ \ 97) = 82$$

$$2022^{2^1} \equiv 82^2 \equiv 6724 \equiv 31(mod\ \ 97)$$

$$2022^{2^2} \equiv 31^2 \equiv 961 \equiv 88(mod\ \ 97)$$

$$2022^{2^3} \equiv 88^2 \equiv 7744 \equiv 81(mod\ \ 97)$$

$$2022^{2^4} \equiv 81^2 \equiv 6561 \equiv 62(mod\ \ 97)$$

$$2022^{2^5} \equiv 62^2 \equiv 3844 \equiv 61(mod\ \ 97)$$

Step3: Calculate $2022^{57}(mod\ \ 97)$.

$2022^{57} \equiv 2022^{1+2^3+2^4+2^5} \equiv 82 \times 81 \times 62 \times 61 \equiv 51(mod\ \ 97)$.

Thus $2022^{57}(mod\ \ 97) = 51$.

Hence $2022^{12345}(mod\ \ 97) = 51$.

Example Calculate $2022^{12345}(mod\ \ 125)$.

Solution

$125 = 5^3$, $\phi(125) = 5^3 - 5^2 = 100$. Since 2022 is coprime to 125, by Euler's theorem,

$$2022^{100} \equiv 1(mod\ \ 125)$$

So

$$2022^{12345} \equiv 2022^{12300} \cdot 2022^{45} \equiv (2022^{100})^{123} \cdot 2022^{45} \equiv 2022^{45}(mod\ \ 125)$$

Now, use repeated squaring method,

Step1: Convert 45 to binary representation.

$$45 = (101101)_2 = 1 + 2^2 + 2^3 + 2^5$$

Step2: Calculate $2022^{2^i}(mod\ \ 125)$, where $i = 0, 1, 2, 3, 4, 5$.

$$2022^{2^0}(mod\ \ 125) = 22$$

$$2022^{2^1} \equiv 22^2 \equiv 484 \equiv 109(mod\ \ 125)$$

$$2022^{2^2} \equiv 109^2 \equiv 11881 \equiv 6(mod\ \ 125)$$

$$2022^{2^3} \equiv 6^2 \equiv 36(mod\ \ 125)$$

$$2022^{2^4} \equiv 36^2 \equiv 1296 \equiv 46(mod\ \ 125)$$

$$2022^{2^5} \equiv 46^2 \equiv 2116 \equiv 116(mod\ \ 97)$$

Step3: Calculate $2022^{45}(mod\ \ 125)$.

$2022^{45} \equiv 2022^{1+2^2+2^3+2^5} \equiv 22 \times 6 \times 36 \times 116 \equiv 107(mod\ \ 125)$.

Thus $2022^{45}(mod\ \ 125) = 107$.

Hence $2022^{12345}(mod\ \ 125) = 107$.

Let's see some applications of Euler's thm and Fermat's Little thm.

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

As before (page 129), $999^{1000} \pmod{1001} = 2^{1000} \pmod{1001}$.

Since g.c.d.$(2, 1001) = 1$ and $\phi(1001) = 720$, we have $2^{720} \equiv 1 \pmod{1001}$

So $2^{1000} \equiv 2^{720+280} \equiv 2^{720} \cdot 2^{280} \equiv 2^{280} \pmod{1001}$.

Thus $999^{1000} \pmod{1001} = 2^{280} \pmod{1001}$, and we can use "repeated squaring method" to calculate the latter.

But the above method does NOT make full use of the factorization of $1001 = 7 \times 11 \times 13$.

Sol: Since $1001 = 7 \times 11 \times 13$, and $7 \nmid 2$, $11 \nmid 2$, $13 \nmid 2$.

By Fermat's Little thm:

$2^{7-1} \equiv 1 \pmod 7$, $2^{11-1} \equiv 1 \pmod{11}$, $2^{13-1} \equiv 1 \pmod{13}$.

Thus:

$$2^{60} \equiv (2^6)^{10} \equiv 1^{10} \equiv 1 \pmod 7$$

$$2^{60} \equiv (2^{10})^6 \equiv 1^6 \equiv 1 \pmod{11}$$

$$2^{60} \equiv (2^{12})^5 \equiv 1^5 \equiv 1 \pmod{13}$$

$\therefore$ $7 \mid 2^{60} - 1$, $11 \mid 2^{60} - 1$, $13 \mid 2^{60} - 1$.

$\therefore$ $1001 = 7 \times 11 \times 13 \mid 2^{60} - 1$. $\therefore$ $2^{60} \equiv 1 \pmod{1001}$.

$$\therefore\ 999^{1000} \equiv 2^{1000} \equiv 2^{60\times 16+40} \equiv (2^{60})^{16}\cdot 2^{40} \equiv 1^{60}\cdot 2^{40} \equiv 2^{40} \pmod{1001}$$

i.e. $999^{1000} \pmod{1001} = 2^{40} \pmod{1001}$.

And we can use "repeated squaring method" to calculate $2^{40} \pmod{1001}$. (See page 129 for $2^{2^i} \pmod{1001}$).

$$\begin{aligned} 2^{40} \pmod{1001} &= 2^{2^5}\cdot 2^{2^3} \pmod{1001} \\ &= 620 \times 256 \pmod{1001} \\ &= 562. \end{aligned}$$

□

So we give a simplification of the "repeated squaring method" for the calculation of $a^b \pmod{m}$ when $g.c.d.(a, m) = 1$ and we know the factorization (or, part of the factorization) of m. We will generalize these when we introduce the concept of the order of a modulo m later.

Example Calculate $1235^{888888} (mod \ \ 528)$.

Solution

$528 = 2^4 \times 3 \times 11.$

Since 1235 is coprime to 2^4 and $\phi(2^4) = 2^4 - 2^3 = 8$, by Euler's theorem

$$1235^8 \equiv 1 (mod \ \ 2^4)$$

Since By 1235 is coprime to 3 and 11, By Fermat's Little Theorem,

$$1235^2 \equiv 1 (mod \ \ 3)$$

$$1235^{10} \equiv 1 (mod \ \ 11)$$

$lcm(8,2,10) = 40$, thus

$$1235^{40} \equiv (1235^8)^5 \equiv 1^5 \equiv 1(mod\ \ 2^4)$$

$$1235^{40} \equiv (1235^2)^{20} \equiv 1^{20} \equiv 1(mod\ \ 3)$$

$$1235^{40} \equiv (1235^{10})^4 \equiv 1^4 \equiv 1(mod\ \ 11)$$

So $2^4|(1235^{40}-1)$, $3|(1235^{40}-1)$, $11|(1235^{40}-1)$, Thus

$$528 = 2^4 \times 3 \times 11|(1235^{40}-1)$$

$$1235^{40} \equiv 1(mod\ \ 528)$$

Hence

$$1235^{888888} \equiv 1235^{888880} \cdot 1235^8 \equiv (1235^{40})^{22222} \cdot 1235^8 \equiv 1235^8(mod\ \ 528)$$

Use repeated squaring method, we can find$1235^8 \equiv 49(mod\ \ 528)$.

Hence $1235^{888888}(mod\ \ 528) = 49$.

Remark

When we use Euler' theorem and Fermat's Little theorem to calculate $a^b(mod\ \ m)$(directly or simplify the repeated squaring method), we always need a, m coprime. When $gcd(a, m) \neq 1$, we need other methods to simplify the repeated squaring method.

Remark

- Euler' theorem can be generalized to the following Lagrange's theorem:

  Let G be a finite group, H be a subgroup of G, then $|H|$ is a divisor of $|G|$. In particular, $\forall a \in G$, the order of a is a divisor of $|G|$.

· Primary Test and Carmichael Number.

In ancient times, people believe that the inverse of Fermat's Little Theorem is also correct, i.e. :

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

$$a^{m-1} \equiv 1 \pmod{m} \implies m \text{ is a prime.}$$

In fact, there is an "ancient Chinese theorem", saying that:

If $2^n \equiv 2 \pmod{n}$ $(*)$, then n is a prime.

Even Leibniz believed this is a theorem!

But this is indeed wrong, we give a composite number follows which satisfing $(*)$.

E.g. $341 = 11 \times 31$ is a composite number.

Since $11 \nmid 2$, $31 \nmid 2$, by Fermat's Little Thm:

$$2^{10} \equiv 1 \pmod{11}, \quad 2^{30} \equiv 1 \pmod{31}.$$

$$\therefore 2^{340} \equiv (2^{10})^{34} \equiv 1^{34} \equiv 1 \pmod{11}$$

$$2^{340} \equiv (2^{30})^{11} \cdot 2^{10} \equiv 1^{11} \times 1024 \equiv 1 \pmod{31}$$

$$\therefore 11 \mid 2^{340} - 1, \quad 31 \mid 2^{340} - 1 \implies 341 = 11 \times 31 \mid 2^{340} - 1.$$

$$\therefore 2^{340} \equiv 1 \pmod{341}, \quad 2^{341} \equiv 2 \pmod{341}.$$

A composite number n satisfing $(*)$ (i.e. $2^n \equiv 2 \pmod{n}$). is called a pseudo prime. The above example shows that 341 is a pseudo prime.

In fact, we can prove that there are infinitely many pseudo primes.

Prop (Malo, 1903) If n is a pseudo prime, then 2^n-1 is also a pseudo prime.

Proof:

If $n = a\cdot b$, $2 \leq a, b \leq n-1$

Then $2^a-1 \mid 2^n-1$, 2^n-1 is a composite.

Also, $(2^n-1) = (2^a-1)\cdot\left(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1\right)$

Since $n \mid 2^n-2$, a similar identity tells us $2^n-1 \mid 2^{2^n-2}-1$. Thus $2^{2^n-1} \equiv 2 \pmod{2^n-1}$, thus 2^n-1 is a pseudo prime. □

Cor. There are infinitely many pseudo primes.

We have seen that the "ancient Chinese theorem" is incorrect, How about the inverse of Fermat's Little theorem?

Def: Let $b \in \mathbb{Z}^+$, $n \in \mathbb{Z}^+$ and g.c.d. $(b, n) = 1$.

If $b^{n-1} \equiv 1 \pmod{n}$, then n is called a pseudo prime under base b (or base b - pseudo prime).

E.g. 341 is a base 2 - pseudo prime.

91 is a base 3 - pseudo prime since $3^{90} \equiv 1 \pmod{91}$, but not a base 2 - pseudo prime since $2^{90} \equiv 64 \pmod{91}$.

One can prove that: if the inverse of Fermat's Little thm is true, thenfor at least half of the integers $b \in \{1, 2, \cdots, n-1\}$, $b^{n-1} \not\equiv 1 \pmod{n}$. (If n is a composite)

This suggests us the following algorithm for primary test (under the hypothesis: the inverse of Fermat's Little thm is true).

```
Input:  n >> 1 and n is odd.

Step 1:  Choose $b \in \{1, 2, \cdots, n-1\}$ randomly.

Step 2:  Use Euclidean algorithm to calculate g.c.d.(b, n).
         If g.c.d.(b, n) ≠ 1, then output "n is a composite."

Step 3:  Now, g.c.d.(b, n) = 1, use "repeated squaring method"
         to calculate $b^{n-1} \pmod{n}$.
         If ~~g.c.d.~~ $b^{n-1} \pmod{n} \neq 1$, then output "n is a composite".
         Otherwise, goto Step 1 and choose another b ...
```

Since for at least half of the integers $b \in \{1, 2, \cdots, n-1\}$, $b^{n-1} \pmod{n} \neq 1$ if n is a composite, So for each test, we have at least 50% chance to find out n is a composite if it is indeed a composite. Thus if an integer n passes 10 rounds test without (any) output "n is a composite", then the probability that n is still a composite is less than $(\frac{1}{2})^{10} \approx 1‰$.

The above is a probability primality test. Since the calculations of g.c.d.(b, n) and $b^{n-1} \pmod{n}$ are easy, this algorithm is far more efficient than "Eratosthenes Sieve" and Fermat factorization. Unfortunately, the hypothesis: "the inverse of Fermat's Little Theorem is true" does NOT hold.

E.g. $n = 561 = 3 \times 11 \times 17$, for any $b \in \mathbb{Z}$ s.t. g.c.d.$(b, 561) = 1$

we have $b^{560} \equiv 1 \pmod{561}$

In fact, since g.c.d.$(b, 561) = 1$, by Fermat's Little Thm:

$$b^2 \equiv 1 \pmod{3}, \quad b^{10} \equiv 1 \pmod{11}, \quad b^{16} \equiv 1 \pmod{17}$$

$$\therefore b^{560} \equiv (b^2)^{280} \equiv 1^{280} \equiv 1 \pmod{3}$$

$$b^{560} \equiv (b^{10})^{56} \equiv 1^{56} \equiv 1 \pmod{11}$$

$$b^{560} \equiv (b^{16})^{35} \equiv 1^{35} \equiv 1 \pmod{17}$$

$$\therefore 11, 17, 3 \mid b^{560} - 1, \quad \therefore 3 \times 11 \times 17 = 561 \mid b^{560} - 1$$

Thus $b^{560} \equiv 1 \pmod{561}$

So, the above algorithm can not get out whether 561 is a prime or not unless you are lucky —— when you choose b from $\{1, 2, \cdots, 560\}$, your choice b has a factor 3 (11, 17), thus g.c.d.$(b, 561) \neq 1$ —— whose probability is $1 - (1 - \frac{1}{3}) \cdot (1 - \frac{1}{11}) \cdot (1 - \frac{1}{17}) \approx 43\%$.

Def: Let n be a composite number, if for any integer a coprime to n, we always have $a^{n-1} \equiv 1 \pmod{n}$, then n is called a <u>Carmichael Number</u>.

The above example shows that 561 is a Carmichael Number, in fact, 561 is the least Carmichael Number.

Use the same method, one can show that 1105, 1729, 2465, 2821, 6601, 8911 are also Carmichael Numbers, and they are all Carmichael Numbers smaller than 10000.

It seems that there are not so many Carmichael Numbers, in fact, there are just 255 Carmichael Numbers less than 10^8.

However, we have the following results:

Thm (Alford, Granville, Pomerance 1992)

There are infinitely many Carmichael Numbers.

In fact, if we denote $C(X)$ ~~as~~ as the number of Carmichael Numbers not exceeding X, then in Alford, Granville, Pomerance's paper (published in 1994), they showed that:

$$C(X) > X^{\frac{2}{7}} \quad \text{for } X \gg 1.$$

Remark

In 2002, Agrawal, Kayal, and Saxena found an unconditional deterministic polynomial-time algorithm that determines whether an input number is prime or composite.

Suggest Reading

- Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, PRIMES is in P, Annals of Mathematics, 160 (2004), 781 - 793
- Ehrhard Behrends, Peter Gritzmann, G*ü*nter M.Ziegler编，邱予嘉译，《来自德国的数学盛宴》（第8章一个给“所有人”的突破），高等教育出版社，2017

谢谢！