Introduction to Number Theory

Math 110 | Winter 2023

Xu Gao

February 13, 2023

What we have seen last week

- Dirichlet's approximation theorem.
- Higher Diophantine equations, rational pts on curves
- Modular arithmetic
- Modular dynamic
    - Additive dynamic
    - Multiplicative dynamic $\times a$ $a \in \mathbb{Z}(m)$
    - Euler's totient φ
    - Euler-Fermat theorem

$$a^{\varphi(m)} \equiv 1 \mod m$$

Today's topics

- Primality testing
- Modular exponential
- Primitive roots
- Discrete logarithm
- Some cryptography

Primality testing

Question

Given a positive integer N, determine whether N is a prime number.

- Test each $1 < x < N$. If none of them divides N, then N is prime.
- (***Trial division method***) Just test $1 < x \leq \sqrt{N}$.

$x \mid N$ $\quad N = xy \quad$ saying $x \leq y$

smaller one

$x^2 \leq xy = N$

Definition 14.1 (Fermat's primality testing)

N is prime

$\Rightarrow a^{N-1} \equiv 1 \mod N$

$0 < a < N$

If you can find an integer $1 < x < N$ such that

$$x^{N-1} \not\equiv 1 \pmod{N}.$$

Then N cannot be prime (by Fermat's little theorem, **??**). Such an integer x is called a ***Fermat witness*** for the compositeness of N.

Note that, even N is composite, it is still possible that

$$x^{N-1} \equiv 1 \pmod{N}.$$

If this is the case, we say x is a ***Fermat liar***.

Primality testing

To disprove N is prime, we only need one Fermat witness

- Divisors are Fermat witness $\because$ $d \mid N \Rightarrow \gcd(d, N) \neq 1 \Rightarrow d$ not invertible $\Rightarrow d^{N-1} \not\equiv 1 \bmod N$.

At first glance, it does not make the primality testing any easier:

- We need to compute an exponential, which seems not easy.
- There are Fermat liars. Hence, applying the testing to only one integer $1 < x < N$ maybe not enough. (Clearly, if x is not coprime to N, then it is a Fermat witness, but it is possible that all integers that are coprime to N are Fermat liars. Such a composite N is called a ***Carmicheal numbers***.)

for which, Fermat witness = divisors so are rare.

Primality testing

At first glance, it does not make the primality testing any easier:

- We need to compute an exponential, which seems not easy.
- There are Fermat liars. Hence, applying the testing to only one integer $1 < x < N$ maybe not enough. (Clearly, if x is not coprime to N, then it is a Fermat witness, but it is possible that all integers that are coprime to N are Fermat liars. Such a composite N is called a ***Carmicheal numbers***.)

But it is in fact way faster than the trial division method, which has time complexity $O(\sqrt{N})$. While the Fermat's primality testing has time complexity $O(K \cdot \log(N))$ (K is the number of x you used in the testing).

Theorem 14.2

If there is a Fermat witness in $\Phi(N)$ for the compositeness of N, then at least half of the numbers in $\Phi(N)$ are Fermat witnesses.

Proof. Let a be a Fermat witness. If there is no Fermat liar, we are done. Otherwise, if there is a Fermat liar b, then $ab \pmod{N}$ is a Fermat witness:

$b^{N-1} \equiv 1$

$$(ab)^{N-1} = a^{N-1}b^{N-1} \equiv a^{N-1} \not\equiv 1 \pmod{N}.$$

Moreover, since $a \in \Phi(N)$, $\boxed{\cdot a \pmod{\cancel{N}}}$ is invertible. Hence, we get a injective map from Fermat liars to Fermat witnesses in $\Phi(N)$. Consequently, at least half of $\Phi(N)$ are Fermat witnesses. $\square$

$|\cdot\cdot| \leq |\cdot\cdot|$

Primality testing

So if we know the composite N is not a Carmicheal number**, then the chance for it to pass K Fermat's primality testing is less than $(\frac{1}{2})^K$. So we don't need many K in general.

The time complexity $O(\log N)$ for exponential computation can be achieved by *binary exponentiation algorithms*.

**We don't know N a priori. But we can take the distribution of Carmicheal numbers into account. For instance, there are only 8220777 Carmicheal numbers under 10^{20}.

Question (Modular exponential)

Fix the modulus m and the base b, effectively compute the natural representative of b^x modulo m.

The basic idea of binary exponentiation algorithms is:

$n \approx \log_2 x$

1. Write the exponent in binary digits: $x = \sum_{i=0}^{n-1} \underbrace{a_i}_{0 \text{ or } 1} 2^i$
2. Then we have
$$b^x = b^{\sum_{i=0}^{n-1} a_i 2^i} = \prod_{i=0}^{n-1} (b^{2^i})^{a_i}.$$
a_i: 0 or 1 $\Leftrightarrow$ no effect or has a factor
3. The natural representative of b^{2^i} can be computed by iterating squares:
$$\underbrace{b \longmapsto b^2 \longmapsto (b^2)^2 = b^{2^2} \longmapsto \cdots \longmapsto (b^{2^{i-1}})^2 = b^{2^i}}_{n \text{ times}}$$

Example 14.3

Apply Fermat's primality testing to 91 with the base 2.

We first write the exponent $91 - 1 = 90$ into binary digits:
$90 = 2^6 + 2^4 + 2^3 + 2.$ $(1011010)_2$

We can compute natural representatives of 2^{2^i} as follows:

	2	2^2	2^{2^2}	2^{2^3}	2^{2^4}	2^{2^5}	2^{2^6}
modulo 91	2	4	16	74	16	74	16

$\equiv -17$

Then we have

$$2^{90} = 2^{2^6} \cdot 2^{2^4} \cdot 2^{2^3} \cdot \cancel{2^{2^3}} \cdot 2^2 \equiv 16 \cdot 16 \; 74 \cdot 4 \equiv 64 \pmod{91}$$

$74 \to 16$ $\not\equiv 1$

So 2 witness 91 being a composite.

Some remarks for binary exponentiation algorithms:

- We do not need natural representatives of b^{2^i}. Instead, using *minimal representatives*[††] maybe more effective.
- The dynamic of $\boxed{(\,\cdot\,)^2 \pmod{m}}$ will eventually fall in a circle since $\mathbb{Z}/m$ is finite. So we only need a finite step to generating all the natural representatives of b^{2^i}.
- We still need to do the multiplication of n congruence classes, but we may do it in a clever way (such as: pairing a square).

[††]The ***minimal representative*** of a congruence class α (modulo m) is the representative a of α such that $-\frac{m}{2} < a \leqslant \frac{m}{2}$.

Relation between additive and multiplicative dynamics

Corollary 14.4 (Of Euler-Fermat, ??)

Let m be a modulus and $a \in \Phi(m)$. Then for any integers b, c such that $b \equiv c \pmod{\varphi(m)}$, we have $a^b = a^{c + k \cdot \varphi(m)}$ $a^{\varphi(m)} \equiv 1$

$$a^b \equiv a^c \pmod{m}.$$

N.B. It is NOT TRUE that $b \equiv c \pmod{m} \Rightarrow a^b \equiv a^c \pmod{m}$ even given $a \in \Phi(m)$. E.g. $2 \in \Phi(7)$. $10 \equiv 3 \pmod{7}$ but $2^{10} \not\equiv 2^3 \pmod{7}$.

1024 8

3 1

?

Relation between additive and multiplicative dynamics

The corollary **??** relates the additive dynamics on $\mathbb{Z}/\varphi(m)$ and the multiplicative dynamics on $\Phi(m)$:

$$\begin{aligned}\exp_{a \pmod m} : \mathbb{Z}/\varphi(m) &\longrightarrow \Phi(m)\\ \bar{x} &\longmapsto a^x \pmod m.\end{aligned}$$

Moreover, this map is a *homomorphism* from the abelian group $(\mathbb{Z}/\varphi(m), +, \mathbf{0})$ to the abelian group $(\Phi(m), \cdot, 1)$.

addition → multiplication

$\bar{0} \to \bar{1}$

Relation between additive and multiplicative dynamics

The corollary **??** relates the additive dynamics on $\mathbb{Z}/\varphi(m)$ and the multiplicative dynamics on $\Phi(m)$:

$$\begin{aligned} \exp_{a \pmod{m}} : \mathbb{Z}/\varphi(m) &\longrightarrow \Phi(m) \\ \bar{x} &\longmapsto a^x \pmod{m}. \end{aligned}$$

Moreover, this map is a *homomorphism* from the abelian group $(\mathbb{Z}/\varphi(m), +, \mathbf{0})$ to the abelian group $(\Phi(m), \cdot, 1)$.

But it may not be bijective! E.g. Let 14 be the modulus and consider the base 9. Then $\Phi(14) = \{1, 3, 5, 9, 11, 13\}$ and hence, $\varphi(14) = 6$. However, although $[1]_6$ and $[4]_6$ are different classes in $\mathbb{Z}/\varphi(14)$, 9^1 and 9^4 have the same natural representative in $\Phi(14)$.

Just as in $\mathbb{Z}/m$

(a, m) coprime $\Rightarrow$ $\mathbb{Z}/m = \{\text{multiples of } [a]\}$ ← generator

$\exp_{a \bmod m}$ is bijective!

Definition 14.5

Let m be a modulus. Then a ***primitive root modulo*** m is an element a in $\Phi(m)$ such that the dynamic of $\boxed{\cdot a \pmod{m}}$ consists of only one circle. Namely, any element of $\Phi(m)$ can be expressed as a power of a modulo m.

Example 14.6

3 is a primitive root modulo 14.

$\Phi(14) = \{1, 3, 5, 9, 11, 13\} \approx \mathbb{Z}/6$ ← $\varphi(14)$

$$\begin{array}{ccccccccccccc} 1 & \to & 3 & \to & 9 & \to & 13 & \to & 11 & \to & 5 & \to & 1 \\ \parallel & & \parallel & & \parallel & & \parallel & & \parallel & & \parallel & & \\ 3^0 & & 3^1 & & 3^2 & & 3^3 & & 3^4 & & 3^5 & & \end{array}$$

Relation between additive and multiplicative dynamics

However, primitive roots do not always exist.

Example 14.7

There is no primitive root modulo 12.

First, $\Phi(12) = \{1, 5, 7, 11\}$. For each of them, we investigate the multiplicative dynamic.

- $\ell_{12}(1) = 1$. $a \mapsto a$
- $\ell_{12}(5) = 2$. $1 \mapsto 5 \to 1 \quad 7 \mapsto 11 \to 7$
- $\ell_{12}(7) = 2$. $1 \to 7 \to 1 \quad 5 \to 11 \to 5$
- $\ell_{12}(11) = 2$. $1 \to 11 \to 1 \quad 5 \to 7 \to 5$

Relation between additive and multiplicative dynamics

When a primitive root g modulo m exists, we have an *isomorphism* between abelian groups:

$$\begin{aligned} \exp_{g \pmod{m}} : \mathbb{Z}/\varphi(m) &\longrightarrow \Phi(m) \\ \bar{x} &\longmapsto g^x \pmod{m}. \end{aligned}$$

In particular, any element a of $\Phi(m)$ can be expressed as a power of g modulo m. Then exponent, which is a congruence class modulo $\varphi(m)$, is called the ***discrete logarithm of a to the base g modulo $\varphi(m)$***. Notation: $\log_{g \pmod{m}}(a)$.

After Class Work

Pingala's algorithm on computing modular exponential $b^x \pmod{m}$:

1. Write the exponent in binary digits: $x = \sum_{i=0}^{n-1} a_i 2^i$
2. Instead of think b^x as $\prod_{i=0}^{n-1} (b^{2^i})^{a_i}$, we think it as

$$b^x = (((b^2 \cdot b^{a_{n-2}})^2 \cdot b^{a_{n-3}})^2 \cdots)^2 \cdot b^{a_0}.$$

3. Then the algorithm can be understood as:
   - Start with b;
   - In each step k, take square (modulo m) of the previous one and then multiply it with $b^{a_{n-k}}$ (namely, multiply it with b if $a_{n-k} = 1$ and do nothing if not).

Example 14.8

Find the natural representative of 2^{90} modulo 91.

divided by 2 | minus 1 divided by 2 | divided by 2 | minus 1 divided by 2 | minus 1 divided by 2 | divided by 2

exponent e	90	45	22	11	5	2	1
Binary	1011010 $\xrightarrow{\text{Erase}}$	101101 $\xrightarrow{\text{Erase}}$	10110 $\xrightarrow{\text{Erase}}$	1011 $\xrightarrow{\text{Erase}}$	101 $\xrightarrow{\text{Erase}}$	10 $\xrightarrow{\text{Erase}}$	1
$2^2 \pmod{91}$	64	57	23	46	32	4	2

Square | Square & multi by 2 | Square | Square & multi by 2 | Square & multi by 2 | Square

Exercise 14.1

Is 119 a prime number?

Terminology

Terminology

A group $(G, *, e)$ is called a ***cyclic group*** if it is isomorphic to $(\mathbb{Z}/m, +, \mathbf{0})$ for some m (called its ***order***). The name comes from the fact that you can arrange elements in G in a single cycle $e \mapsto g \mapsto g^2 \mapsto \cdots \mapsto g^m = e$ under the function "$- * g$". Such an element g is called a ***primitive root*** of the cyclic group G.

Terminology

A congruence class $\overline{a} \in \mathbb{Z}/m$ is a primitive root of the additive group $(\mathbb{Z}/m, +, \mathbf{0})$ if and only if a coprime to m. (by theorem **??**)

An element $a \in \Phi(m)$ is a primitive root of the multiplicative group $(\Phi(m), \cdot, 1)$ if and only if a is a primitive root modulo m.