Lesson 4
Powers modulo m
and
Fermat little theorem

Unit 1
The Fast Powering Algorithm

Modularity for products

EXAMPLE

Without using a calculator compute $998 \times 999 \times 1001 \times 1002[1000]$.

The naive method

THE PROBLEM

Let $g, N \in \mathbb{N}_{\geq 1}$. Compute $g^A[N]$.

THE NAIVE METHOD

Choose $|g_1|$ as small as possible

$$g \equiv g_1[N],\ g_1 \in \{-(N-1), ..., 0, ..., N-1\}$$

$$g^2 \equiv g_1 \cdot g_1 \equiv g_2[N],\ g_2 \in \{-(N-1), ..., 0, ..., N-1\}$$

$$g^3 \equiv g_2 \cdot g_1 \equiv g_3[N],\ g_3 \in \{-(N-1), ..., 0, ..., N-1\}$$

$$\cdots\cdots\cdots\cdots$$

$$g^A \equiv g_{A-1} \cdot g_1 \equiv g_A[N],\ g_A \in \{0, ..., N-1\}$$

REMARK

Requires A steps!

If $A \approx 2^{1000}$ it may become exhausting...

The naive method

EXAMPLE Compute $12^5[7]$

A smart method for powers

EXAMPLE **Find the 2 last digits of 3^{10}: $3^{10}[100]$.**

$$10 = 2 + 2^3 \qquad 3^{10} = 3^{2+2^3} = 3^2 \cdot 3^{2^3}$$

$3^2 \equiv 9[100]$

$3^{2^2} = (3^2)^2 \equiv 81[100]$

$3^{2^3} = (3^{2^2})^2 \equiv 81^2 \equiv 61[100]$

$3^{10} = 3^2 \cdot 3^{2^3} \equiv 9 \cdot 61 = 549 \equiv \boxed{49}[100]$

Check: $3^{10} = 590\boxed{49} \equiv 49[100]$

The Fast Powering Algorithm

THE FAST POWERING ALGORITHM

Let $A \geq 1$ and $A = (A_r \dots A_0)_2 = A_0 + 2A_1 + 2^2A_2 + \cdots + A_r 2^r$, with $A_i \in \{0, 1\}$, be its binary representation, $g \geq 1, N \geq 1$ (we may assume $A_r = 1$).

1. **Compute the powers $g^{2^i}[N]$, $0 \leq i \leq r$ by successive squaring:**

$$a_0 \equiv g[N]$$

$$a_1 \equiv a_0^2 \equiv g^2[N]$$

$$a_2 \equiv a_1^2 \equiv g^{2^2}[N]$$

$$a_3 \equiv a_2^2 \equiv g^{2^3}[N]$$

$$\vdots \qquad \vdots$$

$$a_r \equiv a_{r-1}^2 \equiv g^{2^r}[N]$$

2. **Compute g^A using the formula**

$$g^A = g^{A_0 + 2A_1 + 2^2A_2 + \cdots + 2^rA_r}$$

$$= g^{A_0} \cdot (g^2)^{A_1} \cdot (g^{2^2})^{A_2} \cdots (g^{2^r})^{A_r}$$

$$\equiv a_0^{A_0} \cdot a_1^{A_1} \cdot a_2^{A_2} \cdots a_r^{A_r}[N]$$

The Fast Powering Algorithm

NUMBER OF OPERATIONS

REMARK If $2^r \leq A < 2^{r+1}$: at most r divisions to write A in binary (r bits).

If $A = A_0 + 2A_1 + 2^2A_2 + \cdots + A_r2^r$, we need $2r$ multiplications to compute g^A.

Since $2^r \leq A$, then $3r \leq 3\log_2(A)$. If $A \approx 2^{1000} \sim 10^{300}$ then $3\log_2(A) \approx 3000$.

The Fast Powering Algorithm

EXAMPLE **Compute the last 3 digits of 3^{218}: $3^{218}[1000]$.**

The Fast Powering Algorithm

EXAMPLE **Compute the last 3 digits of 2^{477}.**

Unit 2
Fermat's little Theorem

Fermat's little Theorem

EXAMPLE

Table of powers $a^i[7]$, $a \in \{1, \ldots, 6\}, i = 1, \ldots, 6$.

$1^1 \equiv 1$	$1^2 \equiv 1$	$1^3 \equiv 1$	$1^4 \equiv 1$	$1^5 \equiv 1$	$1^6 \equiv 1$
$2^1 \equiv 2$	$2^2 \equiv 4$	$2^3 \equiv 1$	$2^4 \equiv 2$	$2^5 \equiv 4$	$2^6 \equiv 1$
$3^1 \equiv 3$	$3^2 \equiv 2$	$3^3 \equiv 6$	$3^4 \equiv 4$	$3^5 \equiv 5$	$3^6 \equiv 1$
$4^1 \equiv 4$	$4^2 \equiv 2$	$4^3 \equiv 1$	$4^4 \equiv 4$	$4^5 \equiv 2$	$4^6 \equiv 1$
$5^1 \equiv 5$	$5^2 \equiv 4$	$5^3 \equiv 6$	$5^4 \equiv 2$	$5^5 \equiv 3$	$5^6 \equiv 1$
$6^1 \equiv 6$	$6^2 \equiv 1$	$6^3 \equiv 6$	$6^4 \equiv 1$	$6^5 \equiv 6$	$6^6 \equiv 1$

Fermat's little Theorem

THEOREM (Fermat's little Theorem) Let p be a prime.

1. Let $a \in (\mathbb{Z}/p\mathbb{Z})^*$. Then $a^{p-1} = 1$.
2. If $a \in \mathbb{Z}$ and $p \nmid a$ then $a^{p-1} \equiv 1[p]$.
3. If $a \in \mathbb{Z}$ then $a^p \equiv a[p]$.

$(1) \Leftrightarrow (2) \Leftrightarrow (3)$

REMARK If $p \mid a$ then $a^{p-1} \equiv 0[p]$.

EXAMPLE Compute $2^{104}[101]$

101 is prime (no prime divisors $\leq \sqrt{101}$).

Fermat: $2^{100} \equiv 1[101] \Rightarrow 2^{104} = 2^{100} \cdot 2^4 \equiv 1 \cdot 2^4 = 16[101]$

EXAMPLE The claim is false if p is not prime:

Fermat's little Theorem: examples

EXAMPLE Compute $3^{28}[5]$.

EXAMPLE Divide 23 into 7^{200}. What is the remainder?

Fermat's little Theorem

EXAMPLE

1299709 is prime (believe it).
What is the remainder of the division of $124^{1299708}$ by 1299709?

Try…it has about 1 million digits

Why little? A word about Fermat's (big) Theorem

THEOREM **Let $n > 2$ in $\mathbb{N}$.**

There are no integer solutions (x, y, z) apart the trivial ones (x or y or $z = 0$) of

$$x^n + y^n = z^n$$

"j'en ai découvert une démonstration véritablement merveilleuse que cette marge est trop étroite pour contenir" - Fermat 1647

For this I have discovered a truly wonderful proof, but the margin is too small to contain it" - Fermat 1647

It was proved by A. Wiles in 1994

Fermat's little Theorem: proof

THEOREM (Fermat's little Theorem) **Let p be a prime. If $a \in (\mathbb{Z}/p\mathbb{Z})^*$ then $a^{p-1} = 1$.**

Proof.

UNIT 3
Fermat's Little Theorem: Applications

Fermat's little Theorem: exponents mod. (p-1)

COROLLARY **Let p prime, $a \in \mathbb{Z}$. If $x \equiv y\,[p-1]$ then $a^x \equiv a^y\,[p]$.**

What counts is the exponent mod. (*p-1*)

WARNING **We wrote $x \equiv y\,[p-1]$ NOT $x \equiv y\,[p]$. $6 \equiv 1[5]$ but $2^6 = 64 \not\equiv 2^1[5]$!**

Proof.

REMARK **The converse is false.**

Fermat's little Theorem: exponents mod. (p-1)

COROLLARY **Let p prime, $a \in \mathbb{Z}$. The map**

$$\begin{aligned} \mathbb{Z}/(p-1)\mathbb{Z} &\longrightarrow \mathbb{Z}/p\mathbb{Z} \\ \forall x \in \mathbb{Z} \quad (x)_{p-1} &\longmapsto (a^x)_p \end{aligned}$$

is well defined.

Proof.

Fermat's little Theorem: find the inverse

COROLLARY **Let p be a prime and $a \in (\mathbb{Z}/p\mathbb{Z})^*$. Then $a^{-1} = a^{p-2}$.**

Proof. $a \cdot a^{p-2} = a^{p-1} = 1$. $\square$

EXAMPLE **145441 is prime (admitted). What is the inverse of 4560 in $\mathbb{Z}/145441\mathbb{Z}$?**

Fermat (non) primality test

COROLLARY **Let $p \geq 2$ in $\mathbb{N}$ and $p \nmid a \in \mathbb{Z}$. If $a^{p-1} \not\equiv 1[p]$ then p is not prime.**

EXAMPLE **6 is not prime!**

$$5^5 \equiv 5^{2^2+1}[6] \equiv 1 \cdot 5 \neq 1[6]$$

FPA

WARNING **It may happen that $m \nmid a$ and $a^{m-1} \equiv 1[m]$ and m is not prime.**

For instance $8^8 \equiv (-1)^8 \equiv 1[9]$ but 9 is not prime.

If this happens then m is called pseudoprime relative to base a.

Fermat (non) primality test

EXAMPLE Compute $2^{76}[77]$ with the Fast Powering Algorithm. $p = 77$ is prime?

Fermat (non) primality test

EXAMPLE **Is $m = 15485207$ a prime number?**

Fermat (non) primality test

0	2
1	4
2	16
3	256
4	65 536
5	5 564 957
6	4 814 205
7	15 317 195
8	13 984 990
9	91 295
10	3 735 659
11	3 497 537
12	9 003 821
13	2 020 154
14	4 275 315
15	13 592 221
16	10 699 947
17	9 871 971
18	1 844 895
19	4 547 632
20	13 787 921
21	4 766 758
22	11 102 426
23	4 903 948

End of Lesson 4
Powers modulo m