# Lecture - 3

compute $a^b \bmod n$

Brute force | Square & multiply
---|---
multiplication : $b-1$ | $\log_2(b)$

★ Square & multiply [Fast Exponentiation]

Algo: $a^b \bmod n$

I/P : binary of b : $b_k b_{k-1} \ldots b_0$

Steps : $z = 1$

```
for i = k down to 0
{
    z = z^2 mod n
    if (bi == 1)
    {
        z = (z x a) mod n
    }
}
```

Ex: $7^{100} \bmod 15$

Binary of 100

| 64 | 32 | 16 | 8 | 4 | 2 | 1 |
|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 1 | 0 | 0 |

initially $z=1$

| bit value | square | multiply |
|---|---|---|
| 1 | $1^2 \bmod 15$<br>$z = 1$ | $1 \times 7 \bmod 15$<br>$z = 7$ |
| 1 | $7^2 \bmod 15$<br>$z = 4$ | $4 \times 7 \bmod 15$<br>$z = 13$ |
| 0 | $13^2 \bmod 15$<br>$z = 4$ | X |
| 0 | $4^2 \bmod 15$<br>$z = 1$ | X |

| | | |
|---|---|---|
| 1 | $1^2 \bmod 15$ <br> $z = 1$ | $1 \times 7 \bmod 15$ <br> $= 7$ |
| 0 | $7^2 \bmod 15$ <br> $z = 4$ | X |
| 0 | $4^2 \bmod 15$ <br> $z = 1$ | X |

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 1 | 0 | 0 |
| 7 | 13 | 4 | 1 | 7 | 4 | 1 |

↑ Ans is last entry in table

* Two theorems that play important roles in public-key cryptography

1) Fermat's Theorem

- Fermat's theorem states the following : If $p$ is prime and $a$ is a positive integer not divisible by $p$ then

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

$$\Downarrow$$

$$a^{p-1} \bmod p = 1$$

suppose $a = 3$, $p = 23$

$p = 23$ prime

$a = 3 > 0$

$a \% p = 3 \% 23 = 3 \neq 0$

according to fermat's theorem

$a^{p-1} \bmod p = 1$

$\therefore 3^{23-1} \bmod 23 = 1$

$\therefore \boxed{3^{22} \bmod 23 = 1}$

$3^{22} \bmod 23 = [(3^3)^7 \times 3^1] \bmod 23$

$= [(3^3 \times 3^3 \times 3^3 \times 3^3 \times 3^3 \times 3^3 \times 3^3) \times 3] \bmod 23$

$= (4 \times 4 \times 4 \times 4 \times 4 \times 4 \times 4 \times 3) \bmod 23$

$= (4^7 \times 3) \bmod 23$

$= (4^3 \times 4^3 \times 4 \times 3) \bmod 23$

$= (18 \times 18 \times 12) \bmod 23$

$= (3^2 \times 2 \times 3^2 \times 2 \times 12) \bmod 23$

$= (12 \times 2) \bmod 23$

$= 24 \bmod 23 = 1$

Ex-2 $7^{100} \bmod 15 \rightarrow 7^{101-1} \bmod 15$

$P = 101$ is prime

$a = 7 > 0$ is ~~prime~~

$a \% P = 7 \% 101 \neq 0$

$$101 \overline{)\,7\,}$$
$0$
$7 \neq 0$

According to Fermat's theorem

$$\boxed{7^{101-1} \bmod 15 = 1}$$

→ An alternative form of Fermat's theorem is also useful

If $p$ is prime and $a$ is positive integer then

$$a^{p} \equiv a \pmod{p}$$

→ Note that first form of the theorem requires that $a$ be relatively prime to $p$ but this form does not

Ex: $p=5, a=3$

$$a^{p} = 3^{5} = 243 \equiv 3 \pmod{5}$$

$5 \overline{)\,243\,}$ = 48, $243 - 20 = 43$, $43 - 40 = 3$

Ex: $p=5, a=10$

$$a^{p} = 10^{5} = 100000 \equiv 10 \pmod{5} \equiv 0 \pmod{5}$$

↳ Here $a$ & $p$ are not relatively prime

# Euler's Theorem

→ Euler's theorem states that for every a & n that are relatively prime

$$a^{\phi(n)} \equiv 1 \pmod n \Rightarrow a^{\phi(n)} \bmod n = 1$$

Ex: $7^{100} \bmod 15$

∴ $a = 7$, $n = 15$ that are relatively prime

so, apply Euler's theorem

$\phi(n) = \phi(15)$

$= \cancel{\phi(3)\times}\ \phi(3 \times 5)$

$= \phi(3) \times \phi(5)$

$= 2 \times 4$

$$\boxed{\phi(15) = 8}$$

According Euler's theorem

$$\boxed{7^8 \bmod 15 = 1}$$

**Note:** →

★ $(a+b) \bmod n$

$= (a \bmod n + b \bmod n) \bmod n$

DATE:

* $a^b \bmod n = [(a \bmod n)^b] \bmod n$

* $(a \bmod n) \bmod n = a \bmod n$

$7^{100} \bmod 15$

$= (7^{96} \times 7^4) \bmod 15$

$= ((7^8)^{12} \times 7^4) \bmod 15$

$= (\underbrace{(7^8)}_{a}{}^{12 \to b} \bmod 15 \times 7^4 \bmod 15) \bmod 15$

$= ((7^8 \bmod 15)^{12}_{\bmod 15} \times 7^4 \bmod 15) \bmod 15$

$= (1^{12})_{\bmod 15} \times (7^4 \bmod 15) \bmod 15$

$= 7^4 \bmod 15$

$= 2401 \bmod 15$

$= \boxed{1}$

$$\begin{array}{r|l} & 16 \\ \hline 15 & 2401 \\ & 15 \\ \hline & 90 \\ & 90 \\ \hline & 1 \end{array}$$