

ทฤษฎีบทของแฟร์มา  
Fermat's Little Theorem

RSA

# 01204211 Discrete Mathematics

## Lecture 9a: Fermat's Little Theorem

Jittat Fakcharoenphol

October 4, 2022

## Quick recap

For any integer  $x$  and  $y$ , there exist a pair of integers  $a$  and  $b$  such that

$$\underbrace{a \cdot \underbrace{x}_{\text{red circle}} + b \cdot \underbrace{y}_{\text{red circle}}}_{\text{red bracket}} = \underline{\gcd(x, y)}.$$

## Quick recap

For any integer  $x$  and  $y$ , there exist a pair of integers  $a$  and  $b$  such that

$$a \cdot x + b \cdot y = \gcd(x, y).$$

How to find  $a$  and  $b$ ? Use the extended GCD algorithm.

# Finding $a$ and $b$ : Extended Euclid Algorithm

We will modify the Euclid algorithm so that it also returns  $a$  and  $b$  together with  $\text{gcd}(x, y)$ .

```
Algorithm Euclid(x,y):
```

```
  if  $x \bmod y == 0$ :
```

```
    return  $y, 0, 1$ 
```

```
  else:
```

```
     $g, a', b' = \text{Euclid}(y, x \bmod y)$ 
```

```
     $a = b'$ 
```

```
     $b = a' - b' \cdot \text{floor}(x / y)$ 
```

```
    return  $g, a, b$ 
```

$$a'y + b'(x \bmod y) = g$$

$$ax + by = g$$

$$\left\lfloor \frac{x}{y} \right\rfloor$$

# Recap: Congruences

## Definition (congruences)

For an integer  $m > 0$ , if integers  $a$  and  $b$  are such that

$$a \bmod m = b \bmod m,$$

we write

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

We also have that

$$a \equiv b \pmod{m} \iff m \mid (a - b)$$

## Recap: Multiplicative inverse modulo $m$

### Definition

The multiplicative inverse modulo  $m$  of  $a$ , denoted by  $a^{-1}$ , is an integer such that

$$a \cdot a^{-1} \equiv 1 \pmod{m}.$$

### Theorem 1

An integer  $a$  has a multiplicative inverse modulo  $m$  iff  $\gcd(a, m) = 1$ .

extend gcd  $um$   
 $x \geq y$

$$x \cdot a + y \cdot m = 1 \quad \forall a$$
$$\boxed{x} \cdot a + \cancel{y \cdot m} \pmod{m} = 1 \pmod{m}$$

$=$

How to test if an integer  $n$  is prime

$$5x \equiv 12 \pmod{25}$$

$$\cancel{5^{-1} \pmod{25}}$$

$$5 \cdot 5 = 25 \equiv 0 \pmod{25}$$

$$5 \cdot 10 = 50 \equiv 0 \pmod{25}$$

► Try to find factors of  $n$ . (Takes time  $\sqrt{n}$ )

$$5x \equiv 7 \pmod{19}$$

$$5^{-1} \cdot 5x \cdot 5^{-1} \quad 5 \cdot 5^{-1} \equiv 1 \pmod{19}$$

$$\cancel{5^{-1} \cdot 5x} \equiv \boxed{5^{-1} \cdot 7} \pmod{19}$$

# How to test if an integer $n$ is prime

$n$

- ▶ Try to find factors of  $n$ . (Takes time  $\sqrt{n}$ )
- ▶ If there is a property that holds iff  $n$  is prime, we can check that property. If we can check that quickly, we can test if  $n$  is prime.



# How to test if an integer $n$ is prime

- ▶ Try to find factors of  $n$ . (Takes time  $\sqrt{n}$ )
- ▶ If there is a property that holds **iff**  $n$  is prime, we can check that property. If we can check that quickly, we can test if  $n$  is prime.
- ▶ If there is a **property** that holds **if**  $n$  is prime, how can we make use of that property?

## Theorem 2 (Fermat's Little Theorem)

*If  $p$  is prime and  $a$  is an integer such that  $\gcd(a, p) = 1$ ,*

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

## Theorem 2 (Fermat's Little Theorem)

*If  $p$  is prime and  $a$  is an integer such that  $\gcd(a, p) = 1$ ,*

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

*How can we use Fermat's Little Theorem to check if integer  $n$  is prime?*

# Fermat test

```
Algorithm CheckPrime(n):  
  pick integer a from 2,...,n-1  
  
  if gcd(a,n) != 1:  
    return False  
  
  if power(a,n-1,n) != 1:  
    return False  
  else:  
    return True
```

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

ถ้า n เป็น p.p. แล้ว

# How good is the Fermat test?

When you call `CheckPrime(n)`:

- ▶ If  $n$  is prime,

# How good is the Fermat test?

When you call `CheckPrime(n)`:

- ▶ If  $n$  is prime, `CheckPrime` always return `True`.
- ▶ If  $n$  is composite,

# How good is the Fermat test?

When you call `CheckPrime(n)`:

- ▶ If  $n$  is prime, `CheckPrime` always return `True`.
- ▶ If  $n$  is composite, you want `CheckPrime` to return `False`, but **FLT does not guarantee that.**

## Fermat test - when $n$ is composite

```
Algorithm CheckPrime(n):  
    pick integer a from 2,...,n-1  
  
    if gcd(a,n) != 1:  
        return False  
  
    if power(a,n-1,n) != 1:  
        return False  
    else:  
        return True
```

If  $n$  is composite, the algorithm returns False when



## Fermat test - when $n$ is composite

```
Algorithm CheckPrime(n):  
    pick integer  $a$  from  $2, \dots, n-1$   
  
    if  $\gcd(a, n) \neq 1$ :  
        return False  
  
    if  $a^{n-1} \not\equiv 1 \pmod{n}$ :  
        return False  
    else:  
        return True
```

If  $n$  is composite, the algorithm returns False when

- ▶  $\gcd(a, n) \neq 1$ , i.e., when you pick  $a$  with common factor with  $n$ .

## Fermat test - when $n$ is composite

```
Algorithm CheckPrime(n):  
    pick integer  $a$  from  $2, \dots, n-1$   
  
    if  $\gcd(a, n) \neq 1$ :  
        return False  
  
    if  $a^{n-1} \bmod n \neq 1$ :  
        return False  
    else:  
        return True
```

If  $n$  is composite, the algorithm returns False when

- ▶  $\gcd(a, n) \neq 1$ , i.e., when you pick  $a$  with common factor with  $n$ .
- ▶  $a^{n-1} \bmod n \neq 1$ , i.e., when you find  $a$  that violates the property. We want to be in this case. How likely?

# Proof of FLT: Idea

Let  $p = 7$  and  $a = 5$ . Consider set

$$B = \{1, 2, 3, \dots, p-1\} = \{1, 2, 3, 4, 5, 6\}$$

Also consider set

$$C = \{1 \cdot 5 \bmod 7, 2 \cdot 5 \bmod 7, 3 \cdot 5 \bmod 7, \dots, 6 \cdot 5 \bmod 7\},$$

which is

$$\underline{5, 3, 1, 6, 4, 2}$$



# Proof of FLT: Idea

Let  $p = 7$  and  $a = 5$ . Consider set

$$B = \{1, 2, 3, \dots, p-1\} = \{1, 2, 3, 4, 5, 6\}$$

Also consider set

$$C = \{1 \cdot 5 \bmod 7, 2 \cdot 5 \bmod 7, 3 \cdot 5 \bmod 7, \dots, 6 \cdot 5 \bmod 7\},$$

which is

$$C = \{5, 3, 1, 6, 4, 2\}$$

# Proof of FLT: Idea

Let  $p = 7$  and  $a = 5$ . Consider set

$$B = \{1, 2, 3, \dots, p-1\} = \{1, 2, 3, 4, 5, 6\}$$

Also consider set

$$C = \{1 \cdot 5 \bmod 7, 2 \cdot 5 \bmod 7, 3 \cdot 5 \bmod 7, \dots, 6 \cdot 5 \bmod 7\},$$

which is

$$C = \{5, 3, 1, 6, 4, 2\} = B.$$

# Proof of FLT: Idea

Let  $p = 7$  and  $a = 5$ . Consider set

$$B = \{1, 2, 3, \dots, p-1\} = \{1, 2, 3, 4, 5, 6\}$$

Also consider set

$$C = \{1 \cdot 5 \bmod 7, 2 \cdot 5 \bmod 7, 3 \cdot 5 \bmod 7, \dots, 6 \cdot 5 \bmod 7\},$$

which is

$$C = \{5, 3, 1, 6, 4, 2\} = B.$$

Is this coincidental?

# Proof of FLT: Idea

Let  $p = 7$  and  $a = 5$ . Consider set

$$B = \{1, 2, 3, \dots, p-1\} = \{1, 2, 3, 4, 5, 6\}$$

Also consider set

$$C = \{1 \cdot 5 \bmod 7, 2 \cdot 5 \bmod 7, 3 \cdot 5 \bmod 7, \dots, 6 \cdot 5 \bmod 7\},$$

which is

$$C = \{5, 3, 1, 6, 4, 2\} = B.$$

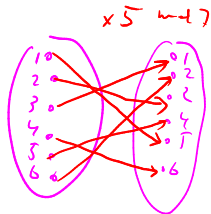
Is this coincidental? No. (We will prove that. But can you quickly tell why.)

Since  $B = C$ , the following terms are equal:

$$\left( \prod_{i \in B} i \right) \bmod 7 = \overbrace{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6}^1 \bmod 7,$$

and

$$\begin{aligned} \left( \prod_{i \in C} i \right) \bmod 7 &= 5 \cdot 3 \cdot 1 \cdot 6 \cdot 4 \cdot 2 \bmod 7 \\ &= (1a) \cdot (2a) \cdot (3a) \cdot (4a) \cdot (5a) \cdot (6a) \bmod 7 \\ &= \overbrace{(1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6)}^1 \cdot a^6 \bmod 7. \end{aligned}$$



## Proof of FLT.

Recall that  $\gcd(a, p) = 1$ , i.e., there exists a multiplicative inverse  $a^{-1}$  of  $a$  modulo  $p$ . This implies that for  $i \not\equiv j \pmod{p}$ ,  $ai \not\equiv aj \pmod{p}$ . Also note that  $a \cdot 0 \equiv 0 \pmod{p}$ .



## Proof of FLT.

Recall that  $\gcd(a, p) = 1$ , i.e., there exists a multiplicative inverse  $a^{-1}$  of  $a$  modulo  $p$ . This implies that for  $i \not\equiv j \pmod{p}$ ,  $ai \not\equiv aj \pmod{p}$ . Also note that  $a \cdot 0 \equiv 0 \pmod{p}$ .

Let  $B = \{1, 2, \dots, p-1\}$ . Let

$$C = \{a \cdot i \bmod p \mid i \in B\}.$$

## Proof of FLT.

Recall that  $\gcd(a, p) = 1$ , i.e., there exists a multiplicative inverse  $a^{-1}$  of  $a$  modulo  $p$ . This implies that for  $i \not\equiv j \pmod{p}$ ,  $ai \not\equiv aj \pmod{p}$ . Also note that  $a \cdot 0 \equiv 0 \pmod{p}$ .

Let  $B = \{1, 2, \dots, p-1\}$ . Let

$$C = \{a \cdot i \bmod p \mid i \in B\}.$$

Since for different  $i, j \in B$ , we have different  $ai \bmod p, aj \bmod p$ , we know that  $|C| = p-1$ . Also,  $C \subseteq B$  because  $0 \leq ai \bmod p \leq p-1$  and  $0 \notin C$ . Thus, we can conclude that  $C = B$ .

## Proof of FLT.

Recall that  $\gcd(a, p) = 1$ , i.e., there exists a multiplicative inverse  $a^{-1}$  of  $a$  modulo  $p$ . This implies that for  $i \not\equiv j \pmod{p}$ ,  $ai \not\equiv aj \pmod{p}$ . Also note that  $a \cdot 0 \equiv 0 \pmod{p}$ .

Let  $B = \{1, 2, \dots, p-1\}$ . Let

$$C = \{a \cdot i \bmod p \mid i \in B\}.$$

Since for different  $i, j \in B$ , we have different  $ai \bmod p, aj \bmod p$ , we know that  $|C| = p-1$ . Also,  $C \subseteq B$  because  $0 \leq ai \bmod p \leq p-1$  and  $0 \notin C$ . Thus, we can conclude that  $C = B$ .

Since  $B = C$ , we have that  $\prod_{i \in B} i \equiv \prod_{i \in C} i \pmod{p}$ , i.e.

$$\begin{aligned} 1 \cdot 2 \cdots (p-1) &\equiv (a1) \cdot (a2) \cdot (a3) \cdots (a(p-1)) \pmod{p} \\ &\equiv \cancel{1} \cdot \cancel{2} \cdots \cancel{(p-1)} \cdot a^{p-1} \pmod{p}. \end{aligned}$$

Since each of  $1, 2, \dots, p-1$  has an inverse modulo  $p$ , we can multiply both sides with  $\underbrace{1^{-1}}, \underbrace{2^{-1}}, \dots, \underbrace{(p-1)^{-1}}$  to obtain

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

as required.

## Exercise

Prove that for any integer  $a$  and prime  $p$ ,

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

How good is the Fermat test when  $n$  is composite?

To answer correctly, we want  $a$  to be such that  $\gcd(a, n) \neq 1$  or

$$a^{n-1} \not\equiv 1$$

$$\underline{a^{n-1} \not\equiv 1 \pmod{n}.$$

# How good is the Fermat test when $n$ is composite?

To answer correctly, we want  $a$  to be such that  $\gcd(a, n) \neq 1$  or

$$a^{n-1} \not\equiv 1 \pmod{n}.$$

We only consider the case where  $\gcd(a, n) = 1$  because when  $\gcd(a, n) \neq 1$ , the test works perfectly.

# How good is the Fermat test when $n$ is composite?

To answer correctly, we want  $a$  to be such that  $\gcd(a, n) \neq 1$  or

$$a^{n-1} \not\equiv 1 \pmod{n}.$$

We only consider the case where  $\gcd(a, n) = 1$  because when  $\gcd(a, n) \neq 1$ , the test works perfectly.

We refer to  $a \in \{1, 2, \dots, n-1\}$  such that  $\gcd(a, n) = 1$  and  $a^{n-1} \not\equiv 1 \pmod{n}$  as a **witness**. The other element  $b$  such that  $b^{n-1} \equiv 1 \pmod{n}$  is called a **non-witness**.

How likely that we randomly choose an element and get a witness?

## Number of witnesses

Suppose that there exists a witness  $a$ ; we know that  $a^{n-1} \not\equiv 1 \pmod{n}$ . How can we find other witnesses?



# Number of witnesses

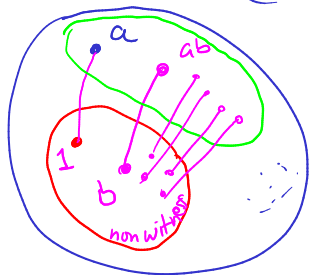
Suppose that there exists a witness  $a$ ; we know that  $a^{n-1} \not\equiv 1 \pmod{n}$ . How can we find other witnesses?

Consider a non-witness  $b$  such that  $b^{n-1} \equiv 1 \pmod{n}$ . *(warning)*

$ab$  witness?

$$(ab)^{n-1} \equiv a^{n-1} \cdot b^{n-1}$$

$$\equiv a^{n-1} \not\equiv 1$$



either witness or non 1 in  
or. witness  $\geq \frac{1}{2}(n-1)$

# Carmichael Number

A **Carmicheal number** is a composite number  $n$  where

$$b^{n-1} \equiv 1 \pmod{n},$$

for every  $b$  which are relatively prime to  $n$ .

$$\text{gcd}(b, n) = 1$$

Carmicheal numbers are rare. The smallest is  $561 = 3 \cdot 11 \cdot 17$ . The next ones are 1105, 1729, and 2465. There are 20, 138, 200 Carmicheal numbers between 1 and  $10^{21}$ .

So, if we ignore Carmicheal numbers, the Fermat test is very good.

There are other probabilistic tests (e.g. Miller-Rabin test) that uses other properties that works for all numbers and there are deterministic algorithms for testing primes.

## Lemma 3

*If  $n$  is not a Carmicheal number, the Fermat test returns that  $n$  is a composite with probability at least  $1/2$ .*

Note that if you repeat the test for  $k$  times, the probability that it gives the wrong answer is at most  $1/2^k$ .

# Running time

$$\sqrt{n}$$

```
Algorithm CheckPrime(n):  
    pick integer a from 2,...,n-1
```

```
    if gcd(a,n) != 1:  
        return False
```

```
    if power(a,n-1,n) != 1:  
        return False
```

```
    else:  
        return True
```

$\log n$

$\log^2 n$

$O(\log^2 n)$

## Special case of Euler's theorem

### Theorem 4 (Euler's theorem)

*If  $p$  and  $q$  are different primes, for  $a$  such that  $\gcd(a, pq) = 1$ , we have*

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

# Special case of Euler's theorem

## Theorem 4 (Euler's theorem)

*If  $p$  and  $q$  are different primes, for  $a$  such that  $\gcd(a, pq) = 1$ , we have*

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

*Is this useful?*

## Special case of Euler's theorem

### Theorem 4 (Euler's theorem)

*If  $p$  and  $q$  are different primes, for  $a$  such that  $\gcd(a, pq) = 1$ , we have*

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

*Is this useful?* Yes! In the RSA algorithm.

# RSA

- ▶ Private key:  $(e, n)$ ,    Public key:  $(d, n)$
- ▶ Encryption  $E(m) = m^e \bmod n$ ,    Decryption:  
 $D(w) = w^d \bmod n$ .
- ▶ Goal: Select  $e, d, n$  such that  $D(E(m)) = m^{ed} \bmod n = m$ .

# RSA

- ▶ Private key:  $(e, n)$ , Public key:  $(d, n)$
- ▶ Encryption  $E(m) = m^e \bmod n$ , Decryption:  $D(w) = w^d \bmod n$ .
- ▶ Goal: Select  $e, d, n$  such that  $D(E(m)) = m^{ed} \bmod n = m$ .

- ▶ Pick two primes  $p$  and  $q$ . Let  $n = pq$ .
- ▶ Pick  $e$  (usually a small number)
- ▶ Pick  $d$  such that  $d = e^{-1} \pmod{(p-1)(q-1)}$ , i.e.,  $ed \equiv 1 \pmod{(p-1)(q-1)}$ , or  $ed = k \cdot (p-1)(q-1) + 1$ , for some integer  $k$ .
- ▶ What is  $m^{ed} \bmod n$ ?

$$\begin{aligned} (m^{ed}) &= m^{k \cdot (p-1)(q-1) + 1} \\ &= \cancel{m^{k(p-1)(q-1)}} \cdot m^1 \end{aligned}$$



# RSA

- ▶ Private key:  $(e, n)$ , Public key:  $(d, n)$
- ▶ Encryption  $E(m) = m^e \bmod n$ , Decryption:  $D(w) = w^d \bmod n$ .
- ▶ Goal: Select  $e, d, n$  such that  $D(E(m)) = m^{ed} \bmod n = m$ .

- ▶ Pick two primes  $p$  and  $q$ . Let  $n = pq$ .
- ▶ Pick  $e$  (usually a small number)
- ▶ Pick  $d$  such that  $d = e^{-1} \pmod{(p-1)(q-1)}$ , i.e.,  $ed \equiv 1 \pmod{(p-1)(q-1)}$ , or  $ed = k \cdot (p-1)(q-1) + 1$ , for some integer  $k$ .
- ▶ What is  $m^{ed} \bmod n$ ?

$$\begin{aligned} m^{ed} &\equiv m^{k(p-1)(q-1)+1} \pmod{n} \\ &\equiv (m^{(p-1)(q-1)})^k \cdot m \pmod{n} \\ &\equiv 1^k \cdot m \pmod{n} \\ &\equiv m \pmod{n} \\ &\quad \underline{\underline{=}} \end{aligned}$$

$$\gcd(m, n) = 1$$

# RSA

- ▶ Private key:  $(e, n)$ , Public key:  $(d, n)$
- ▶ Encryption  $E(m) = m^e \bmod n$ , Decryption:  $D(w) = w^d \bmod n$ .
- ▶ Goal: Select  $e, d, n$  such that  $D(E(m)) = m^{ed} \bmod n = m$ .

- ▶ Pick two primes  $p$  and  $q$ . Let  $n = pq$ .
- ▶ Pick  $e$  (usually a small number)
- ▶ Pick  $d$  such that  $d = e^{-1} \pmod{(p-1)(q-1)}$ , i.e.,  $ed \equiv 1 \pmod{(p-1)(q-1)}$ , or  $ed = k \cdot (p-1)(q-1) + 1$ , for some integer  $k$ .
- ▶ What is  $m^{ed} \bmod n$ ?

$$\begin{aligned} m^{ed} &\equiv m^{k(p-1)(q-1)+1} \pmod{n} \\ &\equiv (m^{(p-1)(q-1)})^k \cdot m \pmod{n} \\ &\equiv 1^k \cdot m \pmod{n} \\ &\equiv m \pmod{n} \end{aligned}$$

$$g_w(m, pq) \neq 1$$

What is the requirement for  $m$ ?

# RSA

- ▶ Private key:  $(e, n)$ , Public key:  $(d, n)$
- ▶ Encryption  $E(m) = m^e \bmod n$ , Decryption:  $D(w) = w^d \bmod n$ .
- ▶ Goal: Select  $e, d, n$  such that  $D(E(m)) = m^{ed} \bmod n = m$ .

- ▶ Pick two primes  $p$  and  $q$ . Let  $n = pq$ .
- ▶ Pick  $e$  (usually a small number)
- ▶ Pick  $d$  such that  $d = e^{-1} \pmod{(p-1)(q-1)}$ , i.e.,  $ed \equiv 1 \pmod{(p-1)(q-1)}$ , or  $ed = k \cdot (p-1)(q-1) + 1$ , for some integer  $k$ .
- ▶ What is  $m^{ed} \bmod n$ ?

$$\begin{aligned} m^{ed} &\equiv m^{k(p-1)(q-1)+1} \pmod{n} \\ &\equiv (m^{(p-1)(q-1)})^k \cdot m \pmod{n} \\ &\equiv 1^k \cdot m \pmod{n} \\ &\equiv m \pmod{n} \end{aligned}$$

What is the requirement for  $m$ ?  $\gcd(m, n) = 1$ , otherwise you can use the message to factor  $n$ .