

# Number Theory

## ITT9131 Konkreetne Matemaatika

### Chapter Four

Divisibility

Primes

Prime examples

Factorial Factors

Relative primality

'MOD': the Congruence Relation

Independent Residues

Additional Applications

Phi and Mu



# Contents

## 1 Modular arithmetic

## 2 Primality test

- Fermat' theorem
- Fermat' test
- Rabin-Miller test

## 3 Phi and Mu



# Next section

## 1 Modular arithmetic

## 2 Primality test

- Fermat' theorem
- Fermat' test
- Rabin-Miller test

## 3 Phi and Mu



# Congruences

## Definition

Integer  $a$  is **congruent** to integer  $b$  modulo  $m > 0$ , if  $a$  and  $b$  give the same remainder when divided by  $m$ . Notation  $a \equiv b \pmod{m}$ .

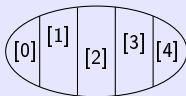
**Alternative definition:**  $a \equiv b \pmod{m}$  iff  $m \mid (b - a)$ . Congruence is

a *equivalence relation*:

**Reflectivity:**  $a \equiv a \pmod{m}$

**Symmetry:**  $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$

**Transitivity:**  $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$



# Properties of the congruence relation

- If  $a \equiv b \pmod{m}$  and  $d|m$ , then  $a \equiv b \pmod{d}$
- If  $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \dots, a \equiv b \pmod{m_k}$ , then  $a \equiv b \pmod{\text{lcm}(m_1, m_2, \dots, m_k)}$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a + c \equiv b + d \pmod{m}$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $ac \equiv bd \pmod{m}$
- If  $a \equiv b \pmod{m}$ , then  $ak \equiv bk \pmod{m}$  for any integer  $k$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a - c \equiv b - d \pmod{m}$
- If  $a \equiv b \pmod{m}$ , then  $a + um \equiv b + vm \pmod{m}$  for every integers  $u$  and  $v$
- If  $ka \equiv kb \pmod{m}$  and  $\gcd(k, m) = 1$ , then  $a \equiv b \pmod{m}$
- $a \equiv b \pmod{m}$  iff  $ak \equiv bk \pmod{mk}$  for any natural number  $k$ .



# Properties of the congruence relation

- If  $a \equiv b \pmod{m}$  and  $d|m$ , then  $a \equiv b \pmod{d}$
- If  $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \dots, a \equiv b \pmod{m_k}$ , then  $a \equiv b \pmod{\text{lcm}(m_1, m_2, \dots, m_k)}$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a + c \equiv b + d \pmod{m}$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $ac \equiv bd \pmod{m}$
- If  $a \equiv b \pmod{m}$ , then  $ak \equiv bk \pmod{m}$  for any integer  $k$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a - c \equiv b - d \pmod{m}$
- If  $a \equiv b \pmod{m}$ , then  $a + um \equiv b + vm \pmod{m}$  for every integers  $u$  and  $v$
- If  $ka \equiv kb \pmod{m}$  and  $\gcd(k, m) = 1$ , then  $a \equiv b \pmod{m}$
- $a \equiv b \pmod{m}$  iff  $ak \equiv bk \pmod{mk}$  for any natural number  $k$ .



# Properties of the congruence relation

- If  $a \equiv b \pmod{m}$  and  $d|m$ , then  $a \equiv b \pmod{d}$
- If  $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \dots, a \equiv b \pmod{m_k}$ , then  $a \equiv b \pmod{\text{lcm}(m_1, m_2, \dots, m_k)}$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a + c \equiv b + d \pmod{m}$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $ac \equiv bd \pmod{m}$
- If  $a \equiv b \pmod{m}$ , then  $ak \equiv bk \pmod{m}$  for any integer  $k$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a - c \equiv b - d \pmod{m}$
- If  $a \equiv b \pmod{m}$ , then  $a + um \equiv b + vm \pmod{m}$  for every integers  $u$  and  $v$
- If  $ka \equiv kb \pmod{m}$  and  $\gcd(k, m) = 1$ , then  $a \equiv b \pmod{m}$
- $a \equiv b \pmod{m}$  iff  $ak \equiv bk \pmod{mk}$  for any natural number  $k$ .



# Properties of the congruence relation

- If  $a \equiv b \pmod{m}$  and  $d|m$ , then  $a \equiv b \pmod{d}$
- If  $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \dots, a \equiv b \pmod{m_k}$ , then  $a \equiv b \pmod{\text{lcm}(m_1, m_2, \dots, m_k)}$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a + c \equiv b + d \pmod{m}$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $ac \equiv bd \pmod{m}$
- If  $a \equiv b \pmod{m}$ , then  $ak \equiv bk \pmod{m}$  for any integer  $k$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a - c \equiv b - d \pmod{m}$
- If  $a \equiv b \pmod{m}$ , then  $a + um \equiv b + vm \pmod{m}$  for every integers  $u$  and  $v$
- If  $ka \equiv kb \pmod{m}$  and  $\gcd(k, m) = 1$ , then  $a \equiv b \pmod{m}$
- $a \equiv b \pmod{m}$  iff  $ak \equiv bk \pmod{mk}$  for any natural number  $k$ .





# Properties of the congruence relation

- If  $a \equiv b \pmod{m}$  and  $d|m$ , then  $a \equiv b \pmod{d}$
- If  $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \dots, a \equiv b \pmod{m_k}$ , then  $a \equiv b \pmod{\text{lcm}(m_1, m_2, \dots, m_k)}$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a + c \equiv b + d \pmod{m}$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $ac \equiv bd \pmod{m}$
- If  $a \equiv b \pmod{m}$ , then  $ak \equiv bk \pmod{m}$  for any integer  $k$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a - c \equiv b - d \pmod{m}$
- If  $a \equiv b \pmod{m}$ , then  $a + um \equiv b + vm \pmod{m}$  for every integers  $u$  and  $v$
- If  $ka \equiv kb \pmod{m}$  and  $\gcd(k, m) = 1$ , then  $a \equiv b \pmod{m}$
- $a \equiv b \pmod{m}$  iff  $ak \equiv bk \pmod{mk}$  for any natural number  $k$ .



# Properties of the congruence relation

- If  $a \equiv b \pmod{m}$  and  $d|m$ , then  $a \equiv b \pmod{d}$
- If  $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \dots, a \equiv b \pmod{m_k}$ , then  $a \equiv b \pmod{\text{lcm}(m_1, m_2, \dots, m_k)}$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a + c \equiv b + d \pmod{m}$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $ac \equiv bd \pmod{m}$
- If  $a \equiv b \pmod{m}$ , then  $ak \equiv bk \pmod{m}$  for any integer  $k$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a - c \equiv b - d \pmod{m}$
- If  $a \equiv b \pmod{m}$ , then  $a + um \equiv b + vm \pmod{m}$  for every integers  $u$  and  $v$
- If  $ka \equiv kb \pmod{m}$  and  $\gcd(k, m) = 1$ , then  $a \equiv b \pmod{m}$
- $a \equiv b \pmod{m}$  iff  $ak \equiv bk \pmod{mk}$  for any natural number  $k$ .



# Properties of the congruence relation

- If  $a \equiv b \pmod{m}$  and  $d|m$ , then  $a \equiv b \pmod{d}$
- If  $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \dots, a \equiv b \pmod{m_k}$ , then  $a \equiv b \pmod{\text{lcm}(m_1, m_2, \dots, m_k)}$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a + c \equiv b + d \pmod{m}$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $ac \equiv bd \pmod{m}$
- If  $a \equiv b \pmod{m}$ , then  $ak \equiv bk \pmod{m}$  for any integer  $k$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a - c \equiv b - d \pmod{m}$
- If  $a \equiv b \pmod{m}$ , then  $a + um \equiv b + vm \pmod{m}$  for every integers  $u$  and  $v$
- If  $ka \equiv kb \pmod{m}$  and  $\gcd(k, m) = 1$ , then  $a \equiv b \pmod{m}$
- $a \equiv b \pmod{m}$  iff  $ak \equiv bk \pmod{mk}$  for any natural number  $k$ .



# Properties of the congruence relation

- If  $a \equiv b \pmod{m}$  and  $d|m$ , then  $a \equiv b \pmod{d}$
- If  $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \dots, a \equiv b \pmod{m_k}$ , then  $a \equiv b \pmod{\text{lcm}(m_1, m_2, \dots, m_k)}$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a + c \equiv b + d \pmod{m}$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $ac \equiv bd \pmod{m}$
- If  $a \equiv b \pmod{m}$ , then  $ak \equiv bk \pmod{m}$  for any integer  $k$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a - c \equiv b - d \pmod{m}$
- If  $a \equiv b \pmod{m}$ , then  $a + um \equiv b + vm \pmod{m}$  for every integers  $u$  and  $v$
- If  $ka \equiv kb \pmod{m}$  and  $\gcd(k, m) = 1$ , then  $a \equiv b \pmod{m}$
- $a \equiv b \pmod{m}$  iff  $ak \equiv bk \pmod{mk}$  for any natural number  $k$ .



# Properties of the congruence relation

- If  $a \equiv b \pmod{m}$  and  $d|m$ , then  $a \equiv b \pmod{d}$
- If  $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \dots, a \equiv b \pmod{m_k}$ , then  $a \equiv b \pmod{\text{lcm}(m_1, m_2, \dots, m_k)}$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a + c \equiv b + d \pmod{m}$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $ac \equiv bd \pmod{m}$
- If  $a \equiv b \pmod{m}$ , then  $ak \equiv bk \pmod{m}$  for any integer  $k$
- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a - c \equiv b - d \pmod{m}$
- If  $a \equiv b \pmod{m}$ , then  $a + um \equiv b + vm \pmod{m}$  for every integers  $u$  and  $v$
- If  $ka \equiv kb \pmod{m}$  and  $\gcd(k, m) = 1$ , then  $a \equiv b \pmod{m}$
- $a \equiv b \pmod{m}$  iff  $ak \equiv bk \pmod{mk}$  for any natural number  $k$ .



# Warmup: An impossible Josephus problem

## The problem

Ten people are sitting in circle, and every  $m$ th person is executed.

Prove that, for every  $k \geq 1$ , the first, second, and third person executed *cannot* be 10,  $k$ , and  $k+1$ , in this order.



# Warmup: An impossible Josephus problem

## The problem

Ten people are sitting in circle, and every  $m$ th person is executed.

Prove that, for every  $k \geq 1$ , the first, second, and third person executed *cannot* be 10,  $k$ , and  $k+1$ , in this order.

## Solution

- If 10 is the first to be executed, then  $10|m$ .
- If  $k$  is the second to be executed, then  $m \equiv k \pmod{9}$ .
- If  $k+1$  is the third to be executed, then  $m \equiv 1 \pmod{8}$ , because  $k+1$  is the first one after  $k$ .

But if  $10|m$ , then  $m$  is even, and if  $m \equiv 1 \pmod{8}$ , then  $m$  is odd: it cannot be both at the same time.



# Application of congruence relation

Example 1: Find the remainder of the division of  $a = 1395^4 \cdot 675^3 + 12 \cdot 17 \cdot 22$  by 7.

As  $1395 \equiv 2 \pmod{7}$ ,  $675 \equiv 3 \pmod{7}$ ,  $12 \equiv 5 \pmod{7}$ ,  $17 \equiv 3 \pmod{7}$  and  $22 \equiv 1 \pmod{7}$ , then

$$a \equiv 2^4 \cdot 3^3 + 5 \cdot 3 \cdot 1 \pmod{7}$$

As  $2^4 = 16 \equiv 2 \pmod{7}$ ,  $3^3 = 27 \equiv 6 \pmod{7}$ , and  $5 \cdot 3 \cdot 1 = 15 \equiv 1 \pmod{7}$  it follows

$$a \equiv 2 \cdot 6 + 1 = 13 \equiv 6 \pmod{7}$$





# Application of congruence relation

Example 2: Find the remainder of the division of  $a = 53 \cdot 47 \cdot 51 \cdot 43$  by 56.

- A. As  $53 \cdot 47 = 2491 \equiv 27 \pmod{56}$  and  $51 \cdot 43 = 2193 \equiv 9 \pmod{56}$ , then

$$a \equiv 27 \cdot 9 = 243 \equiv 19 \pmod{56}$$

- B. As  $53 \equiv -3 \pmod{56}$ ,  $47 \equiv -9 \pmod{56}$ ,  $51 \equiv -5 \pmod{56}$  and  $43 \equiv -13 \pmod{56}$ , then

$$a \equiv (-3) \cdot (-9) \cdot (-5) \cdot (-13) = 1755 \equiv 19 \pmod{56}$$



# Application of congruence relation

Example 3: Find a remainder of dividing  $45^{69}$  by 89

Make use of so called *method of squares*:

$$45 \equiv 45 \pmod{89}$$

$$45^2 = 2025 \equiv 67 \pmod{89}$$

$$45^4 = (45^2)^2 \equiv 67^2 = 4489 \equiv 39 \pmod{89}$$

$$45^8 = (45^4)^2 \equiv 39^2 = 1521 \equiv 8 \pmod{89}$$

$$45^{16} = (45^8)^2 \equiv 8^2 = 64 \equiv 64 \pmod{89}$$

$$45^{32} = (45^{16})^2 \equiv 64^2 = 4096 \equiv 2 \pmod{89}$$

$$45^{64} = (45^{32})^2 \equiv 2^2 = 4 \equiv 4 \pmod{89}$$

As  $69 = 64 + 4 + 1$ , then

$$45^{69} = 45^{64} \cdot 45^4 \cdot 45^1 \equiv 4 \cdot 39 \cdot 45 \equiv 7020 \equiv 78 \pmod{89}$$



# Application of congruence relation

Let  $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0$ , where  $a_i \in \{0, 1, \dots, 9\}$  are digits of its decimal representation.

**Theorem:** An integer  $n$  is divisible by 11 iff the difference of the sums of the odd numbered digits and the even numbered digits is divisible by 11 :

$$11 \mid (a_0 + a_2 + \dots) - (a_1 + a_3 + \dots)$$

*Proof.*

Note, that  $10 \equiv -1 \pmod{11}$ . Then  $10^i \equiv (-1)^i \pmod{11}$  for any  $i$ . Hence,

$$\begin{aligned} n &\equiv a_k(-1)^k + a_{k-1}(-1)^{k-1} + \dots - a_1 + a_0 = \\ &= (a_0 + a_2 + \dots) - (a_1 + a_3 + \dots) \pmod{11} \end{aligned} \quad \text{Q.E.D.}$$

**Example 4:** 34425730438 is divisible by 11

Indeed, due to the following expression is divisible by 11:

$$(8 + 4 + 3 + 5 + 4 + 3) - (3 + 0 + 7 + 2 + 4) = 27 - 16 = 11$$



# Strange numbers: “arithmetic of days of the week”

Addition:

$\oplus$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Mo	Tu	We	Th	Fr	Sa
Mo	Mo	Tu	We	Th	Fr	Sa	Su
Tu	Tu	We	Th	Fr	Sa	Su	Mo
We	We	Th	Fr	Sa	Su	Mo	Tu
Th	Th	Fr	Sa	Su	Mo	Tu	We
Fr	Fr	Sa	Su	Mo	Tu	We	Th
Sa	Sa	Su	Mo	Tu	We	Th	Fr

Multiplication:

$\odot$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Su	Su	Su	Su	Su	Su
Mo	Su	Mo	Tu	We	Th	Fr	Sa
Tu	Su	Tu	Th	Sa	Mo	We	Fr
We	Su	We	Sa	Tu	Fr	Mo	Th
Th	Su	Th	Mo	Fr	Tu	Sa	We
Fr	Su	Fr	We	Mo	Sa	Th	Tu
Sa	Su	Sa	Fr	Th	We	Tu	Mo



# Strange numbers: “arithmetic of days of the week”

Addition:

$\oplus$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Mo	Tu	We	Th	Fr	Sa
Mo	Mo	Tu	We	Th	Fr	Sa	Su
Tu	Tu	We	Th	Fr	Sa	Su	Mo
We	We	Th	Fr	Sa	Su	Mo	Tu
Th	Th	Fr	Sa	Su	Mo	Tu	We
Fr	Fr	Sa	Su	Mo	Tu	We	Th
Sa	Sa	Su	Mo	Tu	We	Th	Fr

Multiplication:

$\odot$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Su	Su	Su	Su	Su	Su
Mo	Su	Mo	Tu	We	Th	Fr	Sa
Tu	Su	Tu	Th	Sa	Mo	We	Fr
We	Su	We	Sa	Tu	Fr	Mo	Th
Th	Su	Th	Mo	Fr	Tu	Sa	We
Fr	Su	Fr	We	Mo	Sa	Th	Tu
Sa	Su	Sa	Fr	Th	We	Tu	Mo

Commutativity:

$$Tu + Fr = Fr + Tu$$

$$Tu \cdot Fr = Fr \cdot Tu$$



# Strange numbers: “arithmetic of days of the week”

Addition:

$\oplus$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Mo	Tu	We	Th	Fr	Sa
Mo	Mo	Tu	We	Th	Fr	Sa	Su
Tu	Tu	We	Th	Fr	Sa	Su	Mo
We	We	Th	Fr	Sa	Su	Mo	Tu
Th	Th	Fr	Sa	Su	Mo	Tu	We
Fr	Fr	Sa	Su	Mo	Tu	We	Th
Sa	Sa	Su	Mo	Tu	We	Th	Fr

Multiplication:

$\odot$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Su	Su	Su	Su	Su	Su
Mo	Su	Mo	Tu	We	Th	Fr	Sa
Tu	Su	Tu	Th	Sa	Mo	We	Fr
We	Su	We	Sa	Tu	Fr	Mo	Th
Th	Su	Th	Mo	Fr	Tu	Sa	We
Fr	Su	Fr	We	Mo	Sa	Th	Tu
Sa	Su	Sa	Fr	Th	We	Tu	Mo

Associativity:

$$(Mo + We) + Fr = Mo + (We + Fr) \quad (Mo \cdot We) \cdot Fr = Mo \cdot (We \cdot Fr)$$



# Strange numbers: “arithmetic of days of the week”

Addition:

$\oplus$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Mo	Tu	We	Th	Fr	Sa
Mo	Mo	Tu	We	Th	Fr	Sa	Su
Tu	Tu	We	Th	Fr	Sa	Su	Mo
We	We	Th	Fr	Sa	Su	Mo	Tu
Th	Th	Fr	Sa	Su	Mo	Tu	We
Fr	Fr	Sa	Su	Mo	Tu	We	Th
Sa	Sa	Su	Mo	Tu	We	Th	Fr

Multiplication:

$\odot$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Su	Su	Su	Su	Su	Su
Mo	Su	Mo	Tu	We	Th	Fr	Sa
Tu	Su	Tu	Th	Sa	Mo	We	Fr
We	Su	We	Sa	Tu	Fr	Mo	Th
Th	Su	Th	Mo	Fr	Tu	Sa	We
Fr	Su	Fr	We	Mo	Sa	Th	Tu
Sa	Su	Sa	Fr	Th	We	Tu	Mo

**Subtraction** is inverse operation of addition:

$$Th - We = (Mo + We) - We = Mo$$



# Strange numbers: “arithmetic of days of the week”

Addition:

$\oplus$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Mo	Tu	We	Th	Fr	Sa
Mo	Mo	Tu	We	Th	Fr	Sa	Su
Tu	Tu	We	Th	Fr	Sa	Su	Mo
We	We	Th	Fr	Sa	Su	Mo	Tu
Th	Th	Fr	Sa	Su	Mo	Tu	We
Fr	Fr	Sa	Su	Mo	Tu	We	Th
Sa	Sa	Su	Mo	Tu	We	Th	Fr

Multiplication:

$\odot$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Su	Su	Su	Su	Su	Su
Mo	Su	Mo	Tu	We	Th	Fr	Sa
Tu	Su	Tu	Th	Sa	Mo	We	Fr
We	Su	We	Sa	Tu	Fr	Mo	Th
Th	Su	Th	Mo	Fr	Tu	Sa	We
Fr	Su	Fr	We	Mo	Sa	Th	Tu
Sa	Su	Sa	Fr	Th	We	Tu	Mo

*Su* is zero element:

$$We + Su = We$$

$$We \cdot Su = Su$$





# Strange numbers: “arithmetic of days of the week”

Addition:

$\oplus$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Mo	Tu	We	Th	Fr	Sa
Mo	Mo	Tu	We	Th	Fr	Sa	Su
Tu	Tu	We	Th	Fr	Sa	Su	Mo
We	We	Th	Fr	Sa	Su	Mo	Tu
Th	Th	Fr	Sa	Su	Mo	Tu	We
Fr	Fr	Sa	Su	Mo	Tu	We	Th
Sa	Sa	Su	Mo	Tu	We	Th	Fr

Multiplication:

$\odot$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Su	Su	Su	Su	Su	Su
Mo	Su	Mo	Tu	We	Th	Fr	Sa
Tu	Su	Tu	Th	Sa	Mo	We	Fr
We	Su	We	Sa	Tu	Fr	Mo	Th
Th	Su	Th	Mo	Fr	Tu	Sa	We
Fr	Su	Fr	We	Mo	Sa	Th	Tu
Sa	Su	Sa	Fr	Th	We	Tu	Mo

*Mo* is **unit**:

$$We \cdot Mo = We$$



# Arithmetic modulo $m$

- Numbers are denoted by  $\overline{0}, \overline{1}, \dots, \overline{m-1}$ , where  $\overline{a}$  represents the class of all integers that dividing by  $m$  give remainder  $a$ .
- Operations are defined as follows

$$\overline{a} + \overline{b} = \overline{c} \quad \text{iff} \quad a + b \equiv c \pmod{m}$$

$$\overline{a} \cdot \overline{b} = \overline{c} \quad \text{iff} \quad a \cdot b \equiv c \pmod{m}$$

## Examples

- “arithmetic of days of the week”, modulus 7
- Boolean algebra, modulus 2



# Division in modular arithmetic

- Dividing  $\bar{a}$  by  $\bar{b}$  means to find a **quotient**  $x$ , such that  $\bar{b} \cdot x = \bar{a}$ , s.o.  $\bar{a}/\bar{b} = x$

In "arithmetic of days of the week":

- $Mo/Tu = Th$  ja  $Tu/Mo = Tu$ .
- We cannot divide by  $Su$ , exceptionally  $Su/Su$  could be any day.
- A quotient is well defined for  $\bar{a}/\bar{b}$  for every  $\bar{b} \neq \bar{0}$ , if the modulus is a prime number.

$\odot$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Su	Su	Su	Su	Su	Su
Mo	Su	Mo	Tu	We	Th	Fr	Sa
Tu	Su	Tu	Th	Sa	Mo	We	Fr
We	Su	We	Sa	Tu	Fr	Mo	Th
Th	Su	Th	Mo	Fr	Tu	Sa	We
Fr	Su	Fr	We	Mo	Sa	Th	Tu
Sa	Su	Sa	Fr	Th	We	Tu	Mo



# Division in modular arithmetic

- Dividing  $\bar{a}$  by  $\bar{b}$  means to find a **quotient**  $x$ , such that  $\bar{b} \cdot x = \bar{a}$ ,  
s.o.  $\bar{a}/\bar{b} = x$

In "arithmetic of days of the week":

- $Mo/Tu = Th$  ja  $Tu/Mo = Tu$ .
- We cannot divide by  $Su$ ,  
exceptionally  $Su/Su$  could be  
any day.
- A quotient is well defined for  
 $\bar{a}/\bar{b}$  for every  $\bar{b} \neq \bar{0}$ , if the  
modulus is a prime number.

$\odot$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Su	Su	Su	Su	Su	Su
Mo	Su	Mo	Tu	We	Th	Fr	Sa
Tu	Su	Tu	Th	Sa	Mo	We	Fr
We	Su	We	Sa	Tu	Fr	Mo	Th
Th	Su	Th	Mo	Fr	Tu	Sa	We
Fr	Su	Fr	We	Mo	Sa	Th	Tu
Sa	Su	Sa	Fr	Th	We	Tu	Mo



# Division in modular arithmetic

- Dividing  $\bar{a}$  by  $\bar{b}$  means to find a **quotient**  $x$ , such that  $\bar{b} \cdot x = \bar{a}$ , s.o.  $\bar{a}/\bar{b} = x$

In "arithmetic of days of the week":

- $Mo/Tu = Th$  ja  $Tu/Mo = Tu$ .
- We cannot divide by  $Su$ , exceptionally  $Su/Su$  could be any day.
- A quotient is well defined for  $\bar{a}/\bar{b}$  for every  $\bar{b} \neq \bar{0}$ , if the modulus is a prime number.

$\odot$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Su	Su	Su	Su	Su	Su
Mo	Su	Mo	Tu	We	Th	Fr	Sa
Tu	Su	Tu	Th	Sa	Mo	We	Fr
We	Su	We	Sa	Tu	Fr	Mo	Th
Th	Su	Th	Mo	Fr	Tu	Sa	We
Fr	Su	Fr	We	Mo	Sa	Th	Tu
Sa	Su	Sa	Fr	Th	We	Tu	Mo



# Division in modular arithmetic

- Dividing  $\bar{a}$  by  $\bar{b}$  means to find a **quotient**  $x$ , such that  $\bar{b} \cdot x = \bar{a}$ ,  
s.o.  $\bar{a}/\bar{b} = x$

In "arithmetic of days of the week":

- $Mo/Tu = Th$  ja  $Tu/Mo = Tu$ .
- We cannot divide by  $Su$ ,  
exceptionally  $Su/Su$  could be  
any day.
- A quotient is well defined for  
 $\bar{a}/\bar{b}$  for every  $\bar{b} \neq \bar{0}$ , if the  
modulus is a prime number.

$\odot$	Su	Mo	Tu	We	Th	Fr	Sa
Su	Su	Su	Su	Su	Su	Su	Su
Mo	Su	Mo	Tu	We	Th	Fr	Sa
Tu	Su	Tu	Th	Sa	Mo	We	Fr
We	Su	We	Sa	Tu	Fr	Mo	Th
Th	Su	Th	Mo	Fr	Tu	Sa	We
Fr	Su	Fr	We	Mo	Sa	Th	Tu
Sa	Su	Sa	Fr	Th	We	Tu	Mo



# Division modulo prime $p$

## Theorem

If  $m$  is a prime number and  $x < m$ , then the numbers

$$\bar{x} \cdot \bar{0}, \bar{x} \cdot \bar{1}, \dots, \bar{x} \cdot \overline{m-1}$$

are pairwise different.

*Proof.* Assume contrary, that the remainders of dividing  $x \cdot i$  and  $x \cdot j$ , where  $i < j$ , by  $m$  are equal. Then  $m \mid (j-i)x$ , that is impossible as  $j-i < m$  and  $\gcd(m, x) = 1$ . Hence,  $\bar{x} \cdot \bar{i} \neq \bar{x} \cdot \bar{j}$  Q.E.D.

## Corollary

If  $m$  is prime number, then the quotient of the division  $\bar{x} = \bar{a}/\bar{b}$  modulo  $m$  is well defined for every  $b \neq 0$ .



# If the modulus is not prime ...

The quotient is not well defined, for example:

$$\overline{1} = \overline{2}/\overline{2} = \overline{3}$$

$\odot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$





## Computing of $\bar{x} = \bar{a}/\bar{b}$ modulo $p$ (where $p$ is a prime number)

In two steps:

- 1 Compute  $\bar{y} = \bar{1}/\bar{b}$
- 2 Compute  $\bar{x} = \bar{y} \cdot \bar{a}$

How to compute  $\bar{y} = \bar{1}/\bar{b}$  i.e. find such a  $\bar{y}$ , that  $\bar{b} \cdot \bar{y} = \bar{1}$

Algorithm:

- 1 Using Euclidean algorithm, compute  $\gcd(p, b) = \dots = 1$
- 2 Find the coefficients  $s$  and  $t$ , such that  $ps + bt = 1$
- 3 if  $t \geq p$  then  $t := t \bmod p$  fi
- 4 return( $t$ )

% Property:  $\bar{t} = \bar{1}/\bar{b}$



# Division modulo $p$

Example: compute  $\overline{53}/\overline{2}$  modulo 234 527

- At first, we find  $\overline{1}/\overline{2}$ . For that we compute GCD of the divisor and modulus:

$$\gcd(234527, 2) = \gcd(2, 1) = 1$$

- The remainder can be expressed by modulus and divisor as follows:

$$\begin{aligned} 1 &= 2(-117263) + 234527 \text{ or} \\ -117263 \cdot \overline{2} &\equiv 117264 \pmod{234527} \end{aligned}$$

Thus,  $\overline{1}/\overline{2} = \overline{117264}$

- Due to  $x = 53 \cdot 117264 \equiv 117290 \pmod{234527}$ , the result is  $\overline{x} = \overline{53 \cdot 117264} = \overline{117290}$ .



# Linear equations

Solve the equation  $\overline{7}x + \overline{3} = \overline{0}$  modulo 47

Solution can be written as  $\overline{x} = -\overline{3}/\overline{7}$

- Compute GCD using Euclidean algorithm

$$\gcd(47, 7) = \gcd(7, 5) = \gcd(5, 2) = \gcd(2, 1) = 1,$$

that yields the relations

$$1 = 5 - 2 \cdot 2$$

$$2 = 7 - 5$$

$$5 = 47 - 6 \cdot 7$$

- Find coefficients of 47 and 7:

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 = \\ &= (47 - 6 \cdot 7) - 2 \cdot (7 - 5) = \\ &= 47 - 8 \cdot 7 + 2 \cdot 5 = \\ &= 47 - 8 \cdot 7 + 2 \cdot (47 - 6 \cdot 7) = \\ &= 3 \cdot 47 - 20 \cdot 7 \end{aligned}$$

*Continues on the next slide ...*



## Linear equations (2)

Solve the equation  $\overline{7}x + \overline{3} = \overline{0}$  modulo 47

- The previous expansion of the  $\gcd(47, 7)$  shows that  $-20 \cdot 7 \equiv 1 \pmod{47}$  i.e.  $27 \cdot 7 \equiv 1 \pmod{47}$   
Hence,  $\overline{1/7} = \overline{-20} = \overline{27}$
- The solution is  $\overline{x} = \overline{-3 \cdot 27} = \overline{13}$

The latter equality follows from the congruence relation  $44 \equiv -3 \pmod{47}$ , therefore  $x = 44 \cdot 27 = 1188 \equiv 13 \pmod{47}$



# Solving a system of equations using elimination method

## Example

Assuming modulus 127, find integers  $x$  and  $y$  such that:

$$\begin{cases} \overline{12}x + \overline{31}y = \overline{2} \\ \overline{2}x + \overline{89}y = \overline{23} \end{cases}$$

Accordingly to the **elimination method**, multiply the second equation by  $-\overline{6}$  and sum up the equations, we get

$$\overline{y} = \frac{\overline{2} - \overline{6} \cdot \overline{23}}{\overline{31} - \overline{6} \cdot \overline{89}}$$

Due to  $6 \cdot 23 = 138 \equiv 11 \pmod{127}$  and  $6 \cdot 89 = 534 \equiv 26 \pmod{127}$ , the latter equality can be transformed as follows:

$$\overline{y} = \frac{\overline{2} - \overline{11}}{\overline{31} - \overline{26}} = \frac{-\overline{9}}{\overline{5}}$$

Substituting  $\overline{y}$  into the second equation, express  $\overline{x}$  and transform it further considering that  $5 \cdot 23 = 115 \equiv -12 \pmod{127}$  and  $9 \cdot 89 = 801 \equiv 39 \pmod{127}$ :

$$\overline{x} = \frac{\overline{23} - \overline{89}\overline{y}}{\overline{2}} = \frac{\overline{23} \cdot \overline{5} - \overline{899}}{\overline{10}} = \frac{-\overline{12} + \overline{39}}{\overline{10}} = \frac{\overline{27}}{\overline{10}}$$



## Solving a system of equations using elimination method (2)

Continuation of the last example ...

Computing:

$$\begin{cases} \bar{x} = \overline{27/10} \\ \bar{y} = \overline{-9/5} \end{cases}$$

if the modulus is 127.

Apply the Euclidean algorithm:

$$\begin{aligned} \gcd(127, 5) &= \gcd(5, 2) = \gcd(2, 1) = 1 \\ \gcd(127, 10) &= \gcd(10, 7) = \gcd(7, 3) = \gcd(3, 1) = 1 \end{aligned}$$

That gives the equalities:

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 = 5 - 2(127 - 25 \cdot 5) = (-2)127 + 51 \cdot 5 \\ 1 &= 7 - 2 \cdot 3 = 127 - 12 \cdot 10 - 2(10 - 127 + 12 \cdot 10) = 3 \cdot 127 - 38 \cdot 10 \end{aligned}$$

Hence, division by  $\bar{5}$  is equivalent to multiplication by  $\overline{51}$  and division by  $\overline{10}$  to multiplication to  $\overline{-38}$ . Then the solution of the system is

$$\begin{cases} \bar{x} = \overline{27/10} = \overline{-27 \cdot 38} = \overline{-1026} = \overline{117} \\ \bar{y} = \overline{-9/5} = \overline{-9 \cdot 51} = \overline{-459} = \overline{49} \end{cases}$$



# Next section

1 Modular arithmetic

2 Primality test

- Fermat' theorem
- Fermat' test
- Rabin-Miller test

3 Phi and Mu



# For determining whether a number $n$ is prime.

There are alternatives:

- Try all numbers  $2, \dots, n-1$ . If  $n$  is not dividisble by none of them, then it is prime.
- Same as above, only try numbers  $2, \dots, \sqrt{n}$ .
- Probabilistic algorithms with polynomial complexity (the Fermat' test, the Miller-Rabin test, etc.).
- Deterministic primality-proving algorithm by Agrawal–Kayal–Saxena (2002).





# For determining whether a number $n$ is prime.

There are alternatives:

- Try all numbers  $2, \dots, n-1$ . If  $n$  is not dividisble by none of them, then it is prime.
- Same as above, only try numbers  $2, \dots, \sqrt{n}$ .
- Probabilistic algorithms with polynomial complexity (the Fermat' test, the Miller-Rabin test, etc.).
- Deterministic primality-proving algorithm by Agrawal–Kayal–Saxena (2002).



# For determining whether a number $n$ is prime.

There are alternatives:

- Try all numbers  $2, \dots, n-1$ . If  $n$  is not dividisble by none of them, then it is prime.
- Same as above, only try numbers  $2, \dots, \sqrt{n}$ .
- Probabilistic algorithms with polynomial complexity (the Fermat' test, the Miller-Rabin test, etc.).
- Deterministic primality-proving algorithm by Agrawal–Kayal–Saxena (2002).



# For determining whether a number $n$ is prime.

There are alternatives:

- Try all numbers  $2, \dots, n-1$ . If  $n$  is not dividisble by none of them, then it is prime.
- Same as above, only try numbers  $2, \dots, \sqrt{n}$ .
- Probabilistic algorithms with polynomial complexity (the Fermat' test, the Miller-Rabin test, etc.).
- Deterministic primality-proving algorithm by Agrawal–Kayal–Saxena (2002).



# Next subsection

1 Modular arithmetic

2 Primality test

- Fermat' theorem
- Fermat' test
- Rabin-Miller test

3 Phi and Mu



# Fermat's "Little" Theorem

## Theorem

If  $p$  is prime and  $a$  is an integer not divisible by  $p$ , then

$$p \mid a^{p-1} - 1$$

## Lemma

If  $p$  is prime and  $0 < k < p$ , then  $p \mid \binom{p}{k}$

*Proof.* This follows from the equality

$$\binom{p}{k} = \frac{p^k}{k!} = \frac{p(p-1)\cdots(p-k+1)}{k(k-1)\cdots 1}$$



Pierre de  
Fermat  
(1601–1665)

# Another formulation of the theorem

## Fermat's "little" theorem

If  $p$  is prime, and  $a$  is an integer, then  $p|a^p - a$ .

*Proof.*

- If  $a$  is not divisible by  $p$ , then  $p|a^{p-1} - 1$  iff  $p|(a^{p-1} - 1)a$
- The assertion is trivially true if  $a = 0$ . To prove it for  $a > 0$  by induction, set  $a = b + 1$ . Hence,

$$\begin{aligned}a^p - a &= (b + 1)^p - (b + 1) = \\&= \binom{p}{0}b^p + \binom{p}{1}b^{p-1} + \cdots + \binom{p}{p-1}b + \binom{p}{p} - b - 1 = \\&= (b^p - b) + \binom{p}{1}b^{p-1} + \cdots + \binom{p}{p-1}b\end{aligned}$$

Here the expression  $(b^p - b)$  is divisible by  $p$  by the induction hypothesis, while other terms are divisible by  $p$  by the Lemma. Q.E.D.



# Application of the Fermat' theorem

**Example:** Find a remainder of division the integer  $3^{4565}$  by 13.

Fermat' theorem gives  $3^{12} \equiv 1 \pmod{13}$ . Let's divide 4565 by 12 and compute the remainder:  $4565 = 380 \cdot 12 + 5$ . Then

$$3^{4565} = (3^{12})^{380} 3^5 \equiv 1^{380} 3^5 = 81 \cdot 3 \equiv 3 \cdot 3 = 9 \pmod{13}$$



## Application of the Fermat' theorem (2)

Prove that  $n^{18} + n^{17} - n^2 - n$  is divisible by 51 for any positive integer  $n$ .

Let's factorize

$$\begin{aligned}A &= n^{18} + n^{17} - n^2 - n = \\&= n(n^{17} - n) + n^{17} - n = \\&= (n+1)(n^{17} - n) = & \% \text{ From Fermat' theorem } \Rightarrow 17|A \\&= (n+1)n(n^{16} - 1) = \\&= (n+1)n(n^8 - 1)(n^8 + 1) = \\&= (n+1)n(n^4 - 1)(n^4 + 1)(n^8 + 1) = \\&= (n+1)n(n^2 - 1)(n^2 + 1)(n^4 + 1)(n^8 + 1) = \\&= \underbrace{(n+1)n(n-1)(n+1)}_{\text{divisible by 3}}(n^2 + 1)(n^4 + 1)(n^8 + 1)\end{aligned}$$

Hence,  $A$  is divisible by  $17 \cdot 3 = 51$ .





# Pseudoprimes

A **pseudoprime** is a probable prime (an integer that shares a property common to all prime numbers) that is not actually prime.

- The assertion of the Fermat' theorem is valid also for some composite numbers.
- For instance, if  $p = 341 = 11 \cdot 31$  and  $a = 2$ , then dividing

$$2^{340} = (2^{10})^{34} = 1024^{34}$$

by 341 yields the remainder 1, because of dividing 1024 gives the remainder 1.

- Integer 341 is a **Fermat' pseudoprime** to base 2.
- However, 341 the assertion of Fermat' theorem is not satisfied for the base 3. Dividing  $3^{340}$  by 341 results in the remainder 56.



# Carmichael numbers

## Definition

An integer  $n$  that is a Fermat pseudoprime for every base  $a$  that are coprime to  $n$  is called a **Carmichael number**.

Example: let  $p = 561 = 3 \cdot 11 \cdot 17$  and  $\gcd(a, p) = 1$ .

$a^{560} = (a^2)^{280}$  gives the remainder 1, if divided by 3

$a^{560} = (a^{10})^{56}$  gives the remainder 1, if divided by 11

$a^{560} = (a^{16})^{35}$  gives the remainder 1, if divided by 17

Thus  $a^{560} - 1$  is divisible by 3, by 11 and by 17.

# Next subsection

1 Modular arithmetic

2 Primality test

- Fermat' theorem

- Fermat' test

- Rabin-Miller test

3 Phi and Mu



# Fermat' test

**Fermat' theorem:** If  $p$  is prime and integer  $a$  is such that  $1 \leq a < p$ , then

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

To test, whether  $n$  is prime or composite number:

- Check validity of  $a^{n-1} \equiv 1 \pmod{n}$  for every  $a = 2, 3, \dots, n-1$ .
- If the condition is not satisfiable for one or more value of  $a$ , then  $n$  is composite, otherwise prime.

Example: is 221 prime?

$$\begin{aligned} 2^{220} &= (2^{11})^{20} \equiv 59^{20} = (59^4)^5 \equiv 152^5 = \\ &= 152 \cdot (152^2)^2 \equiv 152 \cdot 120^2 \equiv 152 \cdot 35 = 5320 \equiv 16 \pmod{221} \end{aligned}$$

Hence, 221 is a composite number. Indeed,  $221 = 13 \cdot 17$



# Fermat' test

**Fermat' theorem:** If  $p$  is prime and integer  $a$  is such that  $1 \leq a < p$ , then

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

To test, whether  $n$  is prime or composite number:

- Check validity of  $a^{n-1} \equiv 1 \pmod{n}$  for every  $a = 2, 3, \dots, n-1$ .
- If the condition is not satisfiable for one or more value of  $a$ , then  $n$  is composite, otherwise prime.

**Example:** is 221 prime?

$$\begin{aligned} 2^{220} &= (2^{11})^{20} \equiv 59^{20} = (59^4)^5 \equiv 152^5 = \\ &= 152 \cdot (152^2)^2 \equiv 152 \cdot 120^2 \equiv 152 \cdot 35 = 5320 \equiv 16 \pmod{221} \end{aligned}$$

Hence, 221 is a composite number. Indeed,  $221 = 13 \cdot 17$



# Problems of the Fermat' test

- Computing of LARGE powers  $\rightsquigarrow$  *method of squares*
- Computing with LARGE numbers  $\rightsquigarrow$  *modular arithmetic*
- $n$  is a pseudoprime  $\rightsquigarrow$  choose  $a$  *randomly* and repeat
- $n$  is a Carmichael number  $\rightsquigarrow$  use better methods, for example *Rabin-Miller test*



# Modified Fermat' test

**Input:**  $n$  – a value to test for primality  
 $k$  – the number of times to test for primality

**Output:** " $n$  is composite" or " $n$  is probably prime"

- **for**  $i := 0$  **step** 1 **to**  $k$ 
  - do**
    - 1 pick  $a$  randomly, such that  $1 < a < n$
    - 2 **if**  $a^{n-1} \not\equiv 1 \pmod{n}$  **return**(" $n$  is composite"); **exit**
  - od**
- **return**(" $n$  is probably prime")

Example,  $n = 221$ , randomly picked values for  $a$  are 38 ja 26

$$a^{n-1} = 38^{220} \equiv 1 \pmod{221} \quad \rightsquigarrow 38 \text{ is pseudoprime}$$

$$a^{n-1} = 26^{220} \equiv 169 \not\equiv 1 \pmod{221} \quad \rightsquigarrow 221 \text{ is composite number}$$

Does not work, if  $n$  is a Carmichael number: 561, 1105, 1729, 2465, 2821, 6601, 8911, ...



# Modified Fermat' test

**Input:**  $n$  – a value to test for primality  
 $k$  – the number of times to test for primality

**Output:** " $n$  is composite" or " $n$  is probably prime"

- **for**  $i := 0$  **step** 1 **to**  $k$ 
  - do**
    - 1** pick  $a$  randomly, such that  $1 < a < n$
    - 2** **if**  $a^{n-1} \not\equiv 1 \pmod{n}$  **return**(" $n$  is composite"); **exit**
  - od**
- **return**(" $n$  is probably prime")

Example,  $n = 221$ , randomly picked values for  $a$  are 38 ja 26

$$a^{n-1} = 38^{220} \equiv 1 \pmod{221} \quad \rightsquigarrow 38 \text{ is pseudoprime}$$

$$a^{n-1} = 26^{220} \equiv 169 \not\equiv 1 \pmod{221} \quad \rightsquigarrow 221 \text{ is composite number}$$

Does not work, if  $n$  is a Carmichael number: 561, 1105, 1729, 2465, 2821, 6601, 8911, ...





# Next subsection

1 Modular arithmetic

2 Primality test

- Fermat' theorem
- Fermat' test
- Rabin-Miller test

3 Phi and Mu



# An idea, how to battle against Carmichael numbers

- Let  $n$  be an odd positive integer to be tested against primality
- Randomly pick an integer  $a$  from the interval  $0 \leq a \leq n-1$ .
- Consider the expression  $a^n - a = a(a^{n-1} - 1)$  and until possible, transform it applying the identity  $x^2 - 1 = (x-1)(x+1)$
- If the expression  $a^n - a$  is not divisible by  $n$ , then all its divisors are also not divisible by  $n$ .
- If at least one factor is divisible by  $n$ , then  $n$  is probably prime. To increase this probability, it is need to repeat with another randomly chosen value of  $a$ .



## Example: $n = 221$

- Let's factorize:

$$\begin{aligned}a^{221} - a &= a(a^{220} - 1) = \\&= a(a^{110} - 1)(a^{110} + 1) = \\&= a(a^{55} - 1)(a^{55} + 1)(a^{110} + 1)\end{aligned}$$

- If  $a = 174$ , then  
 $174^{110} = (174^2)^{55} \equiv (220)^{55} = 220 \cdot (220^2)^{27} \equiv 220 \cdot 1^{27} \equiv 220 \equiv -1 \pmod{221}$ .  
Thus 221 is either prime or pseudoprime to the base 174.
- If  $a = 137$ , then  $221 \nmid a$ ,  $221 \nmid (a^{55} - 1)$ ,  $221 \nmid (a^{55} + 1)$ ,  $221 \nmid (a^{110} + 1)$ .  
Consequently, 221 is a composite number



# Rabin-Miller test

**Input:**  $n > 3$  – a value to test for primality  
 $k$  – the number of times to test for primality

**Output:** " $n$  is composite" or " $n$  is probably prime"

- Factorize  $n - 1 = 2^s \cdot d$ , where  $d$  is an odd number
- **for**  $i := 0$  **step** 1 **to**  $k$ 
  - {
  - 1 Randomly pick value for  $a \in \{2, 3, \dots, n-1\}$ ;
  - 2  $x := a^d \bmod n$ ;
  - 3 **if**  $x = 1$  **or**  $x = n-1$  **then** { **continue**; }
  - 4 **for**  $r := 1$  **step** 1 **to**  $s-1$ 
    - {
    - 1  $x := x^2 \bmod n$
    - 2 **if**  $x = 1$  **then** { **return**(" $n$  is composite"); **exit**; }
    - 3 **if**  $x = n-1$  **then** { **break**; }
    - }
  - 5 **return**(" $n$  is composite"); **exit**;
  - }
- **return**(" $n$  is probably prime");

Complexity of the algorithm is  $\mathcal{O}(k \log_2^3 n)$



# Next section

## 1 Modular arithmetic

## 2 Primality test

- Fermat' theorem
- Fermat' test
- Rabin-Miller test

## 3 Phi and Mu



# Euler's totient function $\phi$

## Euler's totient function

Euler's totient function  $\phi$  is defined for  $m \geq 2$  as

$$\phi(m) = |\{n \in \{0, \dots, m-1\} \mid \gcd(m, n) = 1\}|$$

$n$	2	3	4	5	6	7	8	9	10	11	12	13
$\phi(n)$	1	2	2	4	2	6	4	6	4	10	4	12



# Computing Euler's function

## Theorem

- 1 If  $p \geq 2$  is prime and  $k \geq 1$ , then  $\phi(p^k) = p^{k-1} \cdot (p - 1)$ .
- 2 If  $m, n \geq 1$  are relatively prime, then  $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$ .

## Proof

- 1 Exactly every  $p$ th number  $n$ , starting with 0, has  $\gcd(p^k, n) \geq p > 1$ .  
Then  $\phi(p^k) = p^k - p^k/p = p^{k-1} \cdot (p - 1)$ .
- 2 If  $m \perp n$ , then for every  $k \geq 1$  it is  $k \perp mn$  if and only if **both**  $m \perp k$  and  $n \perp k$ .



# Multiplicative functions

## Definition

$f : \mathbb{N}^+ \rightarrow \mathbb{N}^+$  is *multiplicative* if it satisfies the following condition:  
For every  $m, n \geq 1$ , if  $m \perp n$ , then  $f(m \cdot n) = f(m) \cdot f(n)$

## Theorem

If  $g(m) = \sum_{d|m} f(d)$  is multiplicative, then so is  $f$ .

- $g(1) = g(1) \cdot g(1) = f(1)$  must be either 0 or 1.
- If  $m = m_1 m_2$  with  $m_1 \perp m_2$ , then by induction

$$\begin{aligned} g(m_1 m_2) &= \sum_{d_1 d_2 | m_1 m_2} f(d_1 d_2) \\ &= \left( \sum_{d_1 | m_1} f(d_1) \right) \left( \sum_{d_2 | m_2} f(d_2) \right) - f(m_1) f(m_2) + f(m_1 m_2) \\ &\quad \text{with } d_1 \perp d_2 \\ &= g(m_1) g(m_2) - f(m_1) f(m_2) + f(m_1 m_2) : \end{aligned}$$

whence  $f(m_1 m_2) = f(m_1) f(m_2)$  as  $g(m_1 m_2) = g(m_1) g(m_2)$ .





## $\sum_{d|m} \phi(d) = m$ : Example

The fractions

$$\frac{0}{12}, \frac{1}{12}, \frac{2}{12}, \frac{3}{12}, \frac{4}{12}, \frac{5}{12}, \frac{6}{12}, \frac{7}{12}, \frac{8}{12}, \frac{9}{12}, \frac{10}{12}, \frac{11}{12}$$

are simplified into:

$$\frac{0}{1}, \frac{1}{12}, \frac{1}{6}, \frac{1}{4}, \frac{1}{3}, \frac{5}{12}, \frac{1}{2}, \frac{7}{12}, \frac{2}{3}, \frac{3}{4}, \frac{5}{6}, \frac{11}{12}.$$

The divisors of 12 are 1, 2, 3, 4, 6, and 12. Of these:

- The denominator 1 appears  $\phi(1) = 1$  time:  $0/1$ .
- The denominator 2 appears  $\phi(2) = 1$  time:  $1/2$ .
- The denominator 3 appears  $\phi(3) = 2$  times:  $1/3, 2/3$ .
- The denominator 4 appears  $\phi(4) = 2$  times:  $1/4, 3/4$ .
- The denominator 6 appears  $\phi(6) = 2$  times:  $1/6, 5/6$ .
- The denominator 12 appears  $\phi(12) = 4$  times:  $1/12, 5/12, 7/12, 11/12$ .

We have thus found:  $\phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) = 12$ .



# $\sum_{d|m} \phi(d) = m$ : Proof

Call a fraction  $a/b$  **basic** if  $0 \leq a < b$ .

After simplifying any of the  $m$  basic fractions with denominator  $m$ , the denominator  $d$  of the resulting fraction must be a divisor of  $m$ .

## Lemma

In the simplification of the  $m$  basic fractions with denominator  $m$ , for every divisor  $d$  of  $m$ , the denominator  $d$  appears exactly  $\phi(d)$  times.

It follows immediately that  $\sum_{d|m} \phi(d) = m$ .

## Proof

- After simplification, the fraction  $k/d$  only appears if  $\gcd(k, d) = 1$ : for every  $d$  there are at most  $\phi(d)$  such  $k$ .
- But each such  $k$  appears in the fraction  $kh/n$ , where  $h \cdot d = n$ .



# Euler's theorem

## Statement

If  $m$  and  $n$  are positive integers and  $n \perp m$ , then  $n^{\phi(m)} \equiv 1 \pmod{m}$ .

Note: Fermat's little theorem is a special case of Euler's theorem for  $m = p$  prime.



# Euler's theorem

## Statement

If  $m$  and  $n$  are positive integers and  $n \perp m$ , then  $n^{\phi(m)} \equiv 1 \pmod{m}$ .

Note: Fermat's little theorem is a special case of Euler's theorem for  $m = p$  prime.

## Proof with $m \geq 2$ (cf. Exercise 4.32)

Let  $U_m = \{0 \leq a < m \mid a \perp m\} = \{a_1, \dots, a_{\phi(m)}\}$  in increasing order.

- The function  $f(a) = na \pmod{m}$  is a permutation of  $U_m$ :  
If  $f(a_i) = f(a_j)$ , then  $m \mid n(a_i - a_j)$ , which is only possible if  $a_i = a_j$ .
- Consequently,

$$n^{\phi(m)} \prod_{i=1}^{\phi(m)} a_i \equiv \prod_{i=1}^{\phi(m)} a_i \pmod{m}$$

- But by construction,  $\prod_{i=1}^{\phi(m)} a_i \perp m$ : we can thus simplify and obtain the thesis.



# Möbius function $\mu$

## Mobius function

Mobius' function  $\mu$  is defined for  $m \geq 1$  by the formula

$$\sum_{d|m} \mu(d) = [m = 1]$$

$m$	1	2	3	4	5	6	7	8	9	10	11	12	13
$\mu(m)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0	-1



# Möbius function $\mu$

## Mobius function

Mobius' function  $\mu$  is defined for  $m \geq 1$  by the formula

$$\sum_{d|m} \mu(d) = [m = 1]$$

$m$	1	2	3	4	5	6	7	8	9	10	11	12	13
$\mu(m)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0	-1

As  $[m = 1]$  is clearly multiplicative, so is  $\mu$ !



# Computing the Möbius function

## Theorem

For every  $m \geq 1$ ,

$$\mu(m) = \begin{cases} (-1)^k & \text{if } m = p_1 p_2 \cdots p_k \text{ distinct primes,} \\ 0 & \text{if } p^2 \mid m \text{ for some prime } p. \end{cases}$$

Indeed, let  $p$  be prime. Then, as  $\mu(1) = 1$ :

- $\mu(1) + \mu(p) = 0$ , hence  $\mu(p) = -1$ .

The first formula then follows by multiplicativity.

- $\mu(1) + \mu(p) + \mu(p^2) = 0$ , hence  $\mu(p^2) = 0$ .

The second formula then follows, again by multiplicativity.



# Möbius inversion formula

## Theorem

Let  $f, g : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ . The following are equivalent:

- 1 For every  $m \geq 1$ ,  $g(m) = \sum_{d|m} f(d)$ .
- 2 For every  $m \geq 1$ ,  $f(m) = \sum_{d|m} \mu(d) g\left(\frac{m}{d}\right)$ .

## Corollary

For every  $m \geq 1$ ,

$$\phi(m) = \sum_{d|m} \mu(d) \cdot \frac{m}{d} :$$

because we know that  $\sum_{d|m} \phi(d) = m$ .





# Proof of Möbius inversion formula

Suppose  $g(m) = \sum_{d|m} f(d)$  for every  $m \geq 1$ . Then for every  $m \geq 1$ :

$$\begin{aligned}\sum_{d|m} \mu(d) g\left(\frac{m}{d}\right) &= \sum_{d|m} \mu\left(\frac{m}{d}\right) g(d) \\&= \sum_{d|m} \mu\left(\frac{m}{d}\right) \sum_{k|d} f(k) \\&= \sum_{k|m} \left( \sum_{d|(m/k)} \mu\left(\frac{m}{kd}\right) \right) f(k) \\&= \sum_{k|m} \left( \sum_{d|(m/k)} \mu(d) \right) f(k) \\&= \sum_{k|m} \left[ \frac{m}{k} = 1 \right] f(k) \\&= f(m).\end{aligned}$$

The converse implication is proved similarly.

