

# Unit 5

## Modular Arithmetic

## 4-Digit Combination Lock

Any two kids together can open the lock, but any single kid obtains no information (meaning that he/she needs to try all 10,000 combinations).



# How can it be done?

# Outline of Unit 5

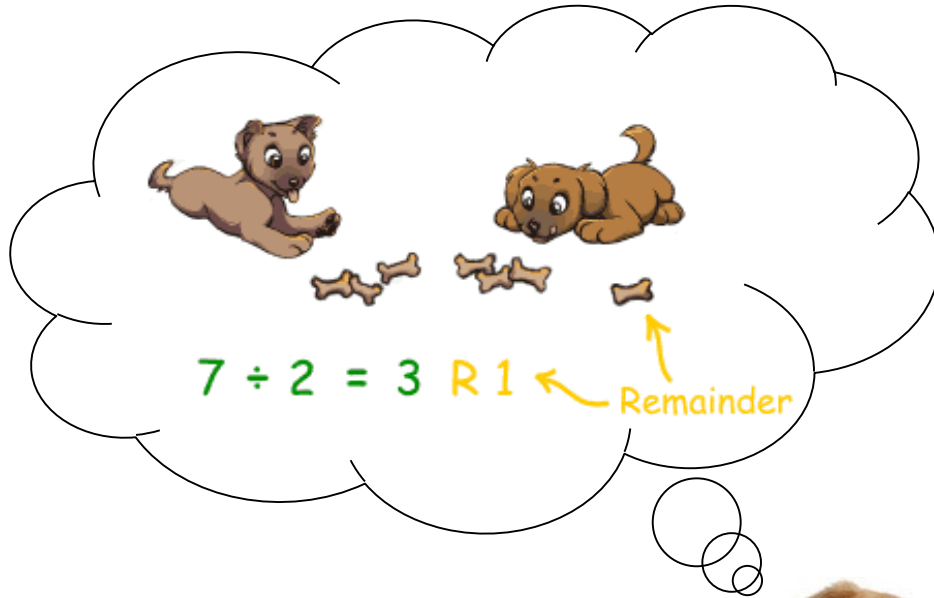
- ❑ 5.1 Modular Arithmetic
- ❑ 5.2 Diophantine Equations
- ❑ 5.3 Modular Division
- ❑ 5.4 Modular Exponentiation
- ❑ 5.5 Secret Sharing
- ❑ 5.6 SageMath: a free math software

Modular arithmetic plays an important role  
in cryptography.

# Unit 5.1

## Modular Arithmetic

# How Much will be Left?



What is the remainder of  
 $10 \times 16 \times 17 +$   
 $25 \times 5 - 37$   
when divided by  
3?

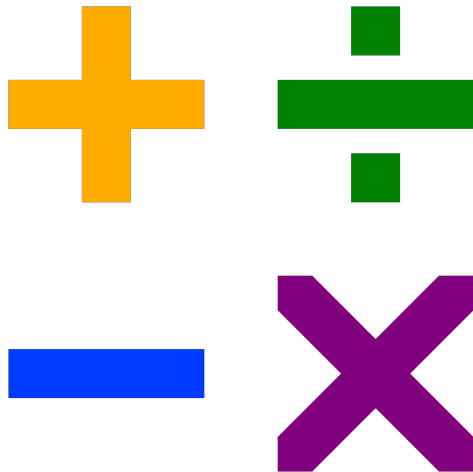


# Modulo Arithmetic

□ **Definition:** We say that two numbers  $a$  and  $b$  are **congruent modulo  $n$**  if they have the same remainder when divided by  $n$ . We write

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

We discussed before that it is an equivalence relation. Now we study it from another perspective.



Arithmetic is all about addition, subtraction, multiplication and division.

# Modular Arithmetic

□ Suppose  $a, b, c, d \in \mathbf{Z}$ ,  $n > 1$ ,  
 $a \equiv c \pmod{n}$  and  $b \equiv d \pmod{n}$ .

□ Are the following statement true?

- a)  $a + b \equiv c + d \pmod{n}$       (Addition)
- b)  $a - b \equiv c - d \pmod{n}$       (Subtraction)
- c)  $ab \equiv cd \pmod{n}$       (Multiplication)

# Nice Properties

- Congruence is **preserved** under addition, subtraction, and multiplication.
- The dog is now ready to solve its problem:
  - What is the remainder of  $10 \times 16 \times 17 + 25 \times 5 - 37$  when divided by 3?

$$\begin{aligned} 10 \times 16 \times 17 + 25 \times 5 - 38 \\ \equiv 1 \times 1 \times 2 + 1 \times 2 - 2 \equiv 2 \pmod{3} \end{aligned}$$



# Modular Division?

- Suppose we have non-zero number  $a$  and another number  $b$ .
- Is there a number  $x$  such that  $ax \equiv b \pmod{7}$ ?
- If so,  $x$  can be regarded as  $b$  divided by  $a$  modulo 7.

# $ax \equiv b \pmod{7}$ ?

Multiplication  
Table

*a*

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

If

$$2x \equiv 6 \pmod{7},$$

then

$$x \equiv 3 \pmod{7}.$$

Each non-zero row contains all possible remainders!

# Another View

$x$

$a$

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

$$2 \times 4 \equiv 1 \pmod{7}$$

4 is said to be the **multiplicative inverse** of 2.

If

$$2x \equiv 6 \pmod{7},$$

then

$$4(2x) \equiv 4 \times 6 \pmod{7}$$

$$x \equiv 24 \pmod{7}$$

$$x \equiv 3 \pmod{7}$$

# Modulo 7

- ❑ Given  $a \neq 0$  and  $b$ , consider  $ax \equiv b \pmod{7}$ .
- ❑ We have seen that  $x$  always exists.
  - Equivalently, the multiplicative inverse of  $a$  always exists.
- ❑  $x$  plays the role of modulo division  $b/a$ .
- ❑ Everything is good? What if modulo 6?

# $ax \equiv b \pmod{6}?$

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Consider  $2x \equiv 5 \pmod{6}$ .

What is the value of  $x$ ?

**No solution!**

The multiplicative inverse of 2 does not exist.

**The story has not ended!**

## Unit 5.2

### Diophantine Equations

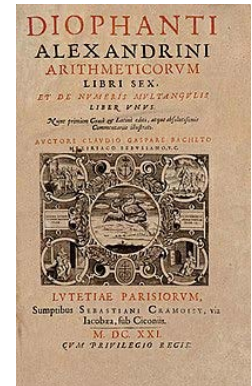
# Diophantine Equations

□ Diophantine equation is a polynomial equation whose solutions are **restricted to be integers**.

□ In this section, we consider **linear** Diophantine equation in **two unknowns**:

$$ax + by = c.$$

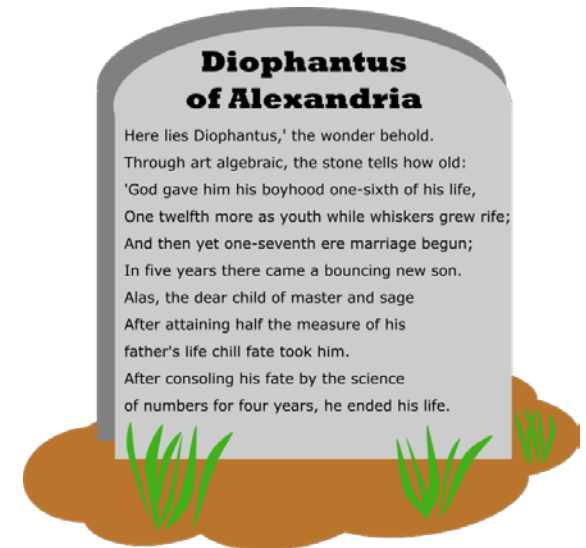
- It is useful when we consider modular division.



Diophantus of Alexandria, the father of algebra. (200-284 AD) He has written a series of books called the *Arithmetica*.

# Diophantus Puzzle (optional, just for fun)

- ❑ Diophantus passed one sixth of his life in childhood, one twelfth in youth, and one seventh more as a bachelor;
- ❑ Five years after his marriage a son was born who died four years before his father at half his final age.
- ❑ How old did Diophantus die?



The puzzle is  
an epitaph of  
Diophantus.



# Example

- ❑ You want to buy a book that costs \$230.
- ❑ You only have \$20 notes.
- ❑ The bookseller only has \$50 notes.
- ❑ Can you pay the exact price of the book?



$x =$



$y +$



Can you solve the equation?

# More Examples

□  $187x + 55y = 121$ , where  $x, y$  are integers.

- $x = 3, y = -8$

- $x = -2, y = 9$

- Infinitely many solutions!

□  $187x + 55y = 45$ , where  $x, y$  are integers.

- No solutions!

□ When does a Diophantine equation have solutions?

# Existence of Solutions

□ **Theorem:** Given integers  $a, b, c$  (at least one of  $a$  and  $b$  is nonzero), the Diophantine equation

$$ax + by = c$$

has a solution if and only if

$$\gcd(a, b) \mid c.$$

## Proof (for self study)

Let  $d = \gcd(a, b)$ .

**Solution exists  $\Rightarrow d|c$**

Assume there exists integers  $x, y$  such that

$$c = ax + by.$$

Write  $a = dp$  and  $b = dq$ ,  
(where  $p$  and  $q$  are integers).

Then  $c = d(px + qy)$ .

Hence,  $d|c$ .

**Solution exists  $\Leftarrow d|c$**

Assume  $d|c$ .

Write  $c = td$ .

Bézout's identity (in Unit 4):

$$ax' + by' = d$$

Multiply both sides by  $t$ ;

$$a(tx') + b(ty') = c$$

Hence,  $(tx', ty')$  is a solution.

*Q.E.D.*

# A Particular Solution

□  $391x + 299y = -69$

- Extended Euclidean Algorithm gives

$$391(-3) + 299(4) = \gcd(391, 299) = 23$$

Multiplying the whole equation by  $-3$ ,

$$391(9) + 299(-12) = -69$$

- Hence,  $x = 9, y = -12$  is a solution.

Extended Euclidean algorithm can find a particular solution.

- But  $x = -4, y = 5$  is also a solution.

- How do we find **all** solutions?

## Example: From one solution to many...

**Q:** Solve  $2x + 3y = 7$ .

Clearly,  $x = 2, y = 1$  is a solution.

Consider  $x = 2 + 3t, y = 1 - 2t$ , where  $t \in \mathbb{Z}$ .

Substituting them into the given equation,

$$2(2 + 3t) + 3(1 - 2t) = 7.$$

Since  $t$  can be any integer, a particular solution gives rise to an infinite number of solutions.

# General Solution (proof omitted)

□ **Theorem:** If  $(x_0, y_0)$  is any particular solution to the Diophantine equation

$$ax + by = c$$

then all the solutions have the form

$$a \left( x_0 + t \frac{b}{d} \right) + b \left( y_0 - t \frac{a}{d} \right) = c,$$

where  $d = \gcd(a, b)$  and  $t$  is an arbitrary integer.

# Example (revisited)



- The equation is  $20x - 50y = 230$ .
- Dividing it by  $\gcd(20, 50) = 10$ , we obtain
$$2x - 5y = 23.$$
- We have seen that  $x_0 = 14, y_0 = 1$  is a particular solution.
- Therefore,  $2(14 - 5t) - 5(1 - 2t) = 23$ .
  - This result can also be obtained directly by the formula in the previous slide.



## Unit 5.3

### Modular Division

# Multiplicative Inverse

- $a^{-1}$  is said to be a **multiplicative inverse** of  $a \pmod{n}$  if

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

- If  $a$  has an inverse, then we can “divide by  $a$ ”.

$$\text{Divide by } a \triangleq \text{Multiply by } a^{-1}$$

# Uniqueness of Inverses

**Lemma:** If  $a$  has a multiplicative inverse modulo  $n$ , then it is unique modulo  $n$ .

**Proof:**

Suppose  $x$  and  $y$  are both inverses of  $a$ .

$$x \equiv x(ay) \equiv (xa)y \equiv y \pmod{n}.$$

$$\because ay = 1$$

$$\because xa = 1$$

*Q.E.D.*

# Existence of Inverses

**Theorem:**  $a$  has a multiplicative inverse modulo  $n$  iff

$$\gcd(a, n) = 1.$$

i.e.  $a$  and  $n$   
are co-prime

**Proof:**

- $ax \equiv 1 \pmod{n}$  iff  $ax + kn = 1$  for some integer  $k$ .
- For fixed  $a$  and  $n$ , this Diophantine equation has an integer solution for  $x$  iff  $\gcd(a, n) \mid 1$ .

*Q.E.D.*

# Modular Division

- If  $\gcd(a, n) = 1$ , then we can perform “division by  $a$  modulo  $n$ ”.
  - i.e., multiply by  $a^{-1}$ .
  
- How to find  $a^{-1}$ ?
  - i. Use extended Euclidean algorithm to find  $s$  and  $t$  such that  $as + nt = 1$ .
  - ii. Then  $a^{-1} = s$ .

# Classwork

□ Find the value of  $3^{-1} \bmod 11$ .

□ Solution:

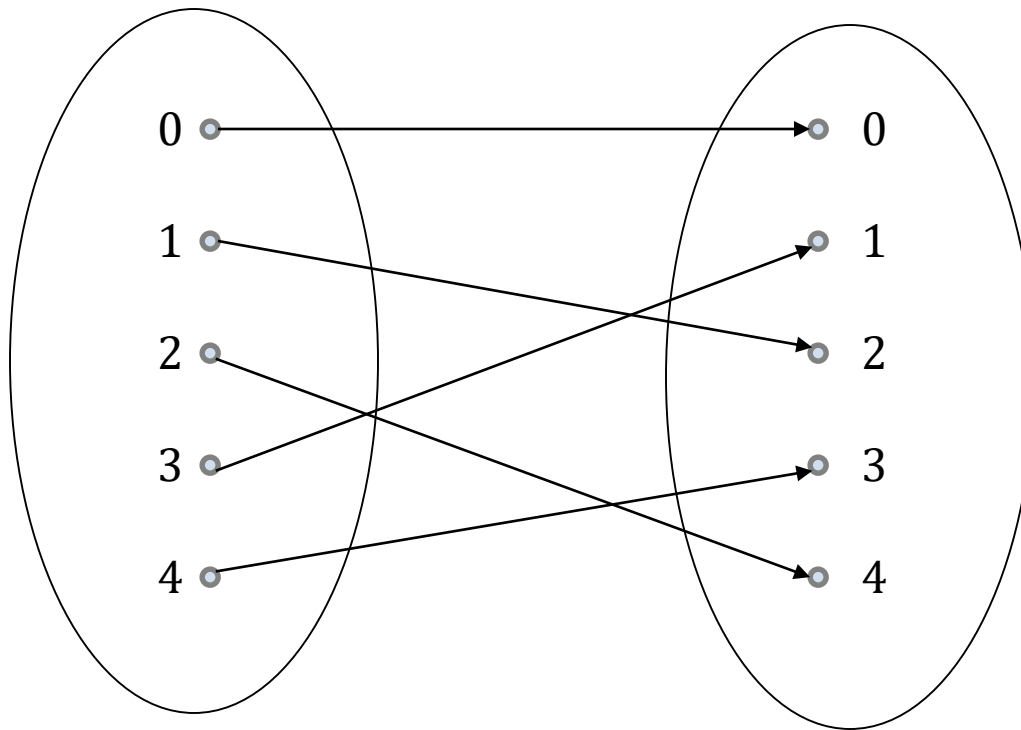
# Modulo $p$

- ❑ If  $p$  is a prime number and  $a \neq 0$ , then  $\gcd(a, p) = 1$ .
- ❑ Hence,  $a$  has multiplicative inverse modulo  $p$ .
- ❑ Division (mod  $p$ ) can be performed for all **non-zero** elements.
  
- ❑ In fact, multiplication (mod  $p$ ) is a bijection.
  - Division is the inverse function.

# Multiplication (mod $p$ ) is a Bijection

□ Example:  $f(x) = 2x \pmod{5}$

Five possible  
remainders:  
0, 1, 2, 3, 4



Bijection!

Division  
is just the  
inverse  
function.



## Unit 5.4

### Modular Exponentiation

# Modular Exponentiation

- ❑ How to compute  $m^e \bmod n$ ?
- ❑ Straightforward?
  - First, compute  $m^e$ .
  - Next, divide it by  $n$  and obtain the remainder.
- ❑ How about  $17^{29} \bmod 35$ ?
  - For cryptography,  $m$ ,  $e$ , and  $n$  may have 1000 digits.
  - A fast method is needed.

# Square-and-Multiply Method

First, note the following:

- $17 \bmod 35 = 17$
- $17^2 \bmod 35 = 289 \bmod 35$   
 $= 9$
- $17^4 \bmod 35 = (17^2)^2 \bmod 35$   
 $= 9^2 \bmod 35$   
 $= 11$
- $17^8 \bmod 35 = 11^2 \bmod 35$   
 $= 16$
- $17^{16} \bmod 35 = 16^2 \bmod 35$   
 $= 11$

Second, do the calculation:

- $17^{29} \bmod 35$   
 $= 17^{16} 17^8 17^4 17 \bmod 35$   
 $= (11) (16) (11) (17) \bmod 35$   
 $= 32912 \bmod 35$   
 $= 12$

# Fermat's Little Theorem

**Theorem:** If  $p$  is prime and  $p \nmid a$   
(which means  $p$  does not divide  $a$ ), then

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

- ❑ It can be used to calculate modular exponentiation if  $p$  is a **prime**.
- ❑ Example: Compute  $2^{35} \pmod{7}$ .
  - i.  $2^{35} = (2^6)^5 \cdot 2^5$
  - ii.  $2^{35} \equiv 2^5 \equiv 32 \equiv 4 \pmod{7}$

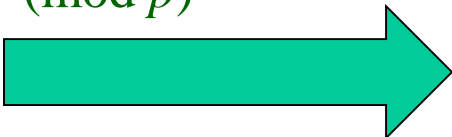


Pierre de Fermat (1607-1665), the father of modern number theory. Watch this 5-min video to learn more:

<https://www.youtube.com/watch?v=Ij01HGgxnkA>

# Proof

Since it is a bijection, these numbers are just permutation of the original  $p - 1$  numbers.

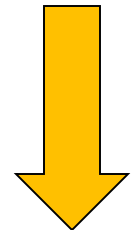
$1, 2, \dots, p - 1$    $a, 2a, \dots, (p - 1)a.$

Multiply each of them by  $a \neq 0 \pmod{p}$

 Multiply altogether

 Multiply altogether

$$[1 \times 2 \times \dots \times (p - 1)] \equiv a^{p-1} [1 \times 2 \times \dots \times (p - 1)]$$

 Divide both sides by  $[1 \times 2 \times \dots \times (p - 1)] \pmod{p}$

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

*Q.E.D.*

# Euler's Theorem

## **Theorem:**

If  $a$  is co-prime with  $n$ , then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

## **Proof:**

Same as in previous slide, except that we start with the  $\phi(n)$  numbers that are co-prime with  $n$ .

# Unit 5.5

## Secret Sharing

# 4-Digit Combination Lock

Key Idea: Two points determine a line.



Suppose the lock's combination is 6965.

slope = 6965, y-intercept (generated randomly)



# Secret Sharing Scheme

- ❑ Let  $p = 10007$  (a prime number greater than 10,000)
- ❑ Pick a random number (mod  $p$ ), say 30.
- ❑ Define the line  $L$  by
$$y \equiv 6965x + 30 \pmod{10007}$$

- ❑ Give the kids the following points on  $L$ :
  - Alice: (1, 6995)
  - Bob: (2, 3953)
  - Claire: (3, 911)
  - Daniel: (4, 7876)

# How to Open the Lock?

□ Suppose Alice and Claire want to open the lock.

○ Alice: (1, 6995), Claire: (3, 911)

□ The slope of the line through their point is

$$\frac{911 - 6995}{3 - 1} \equiv \frac{-6084}{2} \pmod{10007}$$

□ Note that  $2^{-1} \equiv 5004 \pmod{10007}$ .

□ Hence,

$$-6084 \times 5004 \equiv 6965 \pmod{10007}$$

They can open the lock!

## Unit 5.6

SageMath: a free math software

# SageMath

- ❑ A free open-source mathematics software system
  - alternative to Magma, Maple, Mathematica and Matlab.
  - <http://www.sagemath.org/>
- ❑ Built on top of Python
  - You can use python commands in Sage.
- ❑ There is a web interface called SageMathCell
  - <http://sagecell.sagemath.org/>
  - Powerful programmable calculator online
    - Great for small (or even medium-sized) tasks.
    - Accessible by desktop/mobile.
- ❑ For large projects, switch to SageMathCloud.
  - You need to open an account (which is free).



Type some Sage code below and press Evaluate.

```
1 euler_phi(10000)
2
```



Evaluate

Language: Sage ▼

Share

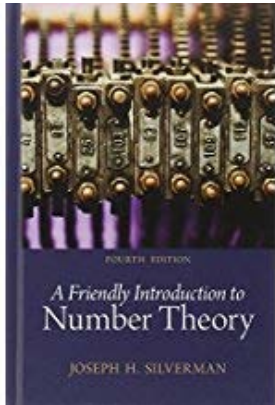
4000

[Help](#) | Powered by [SageMath](#)

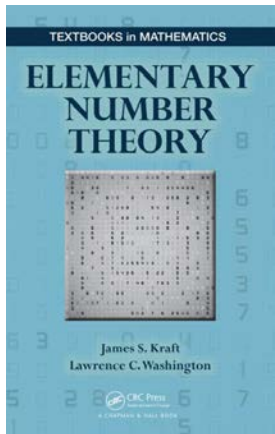
# Some Useful Commands

- ❑ `factor( $x$ )` // factorize  $x$
- ❑ `nth_prime( $n$ )` // return the  $n$ -th prime
- ❑ `gcd( $a, b$ )`
- ❑ `xgcd( $a, b$ )` // extended Euclidean alg.
- ❑ `euler_phi( $x$ )`
- ❑ `mod( $a, n$ )` (or  $a \% n$ )

# Recommended Reading



- Chapters 6 and 8 – 10, J. H. Silverman, *A Friendly Introduction to Number Theory*, 4<sup>th</sup> ed., Pearson, 2013.



- Chapters 2, 5 and Section 7.8, J. S. Kraft and L. C. Washington, *Elementary Number Theory*, CRC Press, 2015.