

## 5.5: Congruences

### Congruences and their properties

Discuss the following problem:

EXAMPLE 1. *Are there any integers  $x$  and  $y$  such that  $x^2 = 4y + 3$ ?*

Recall that congruence mod  $n$  is an equivalence relation on  $\mathbf{Z}$ , i.e.

- 1.
- 2.
- 3.

PROPOSITION 2. *Let  $a, b, c, d \in \mathbf{Z}$  and let  $n \in \mathbf{Z}^+$ . Then*

1. *If  $a \equiv b \pmod{n}$  and  $c \equiv d \pmod{n}$  then  $a + c \equiv b + d \pmod{n}$ .*
2. *If  $a \equiv b \pmod{n}$  and  $c \equiv d \pmod{n}$  then  $ac \equiv bd \pmod{n}$ .*
3. *If  $ab \equiv ac \pmod{n}$  and  $\gcd(a, n) = 1$  then  $b \equiv c \pmod{n}$ .*

*Proof.*

REMARK 3. If  $\gcd(a, n) \neq 1$ , then (3) maybe false.

COROLLARY 4. *If  $a \equiv b \pmod{n}$  then  $a^k \equiv b^k \pmod{n}$  for every  $k \in \mathbf{Z}^+$ .*

EXAMPLE 5. *Prove that  $7|6^{1000} - 1$  and  $7|6^{1001} + 1$ .*

EXAMPLE 6. *What is the last digit of  $7^{1258}$ ?*

PROPOSITION 7. Let  $n \in \mathbf{Z}$ ,  $n > 1$ . If  $a \in \mathbf{Z}$ , then  $a$  is congruent modulo  $n$  to exactly one of the integers  $0, 1, 2, \dots, n - 1$ .

EXAMPLE 8. Show that square of any integer is congruent to 0 or to 1 (modulo 4). Then derive another proof of Example 1.

Recall the definition of **congruence class** of  $a$  modulo  $n$ :

$$[a] = \{x \in \mathbf{Z} \mid x \equiv a \pmod{n}\}.$$

Note that

1. For any integer  $a$ ,  $[a]$  is a set, not an integer.
2. If  $0 \leq a < n$ , then  $[a]$  can be described as the set of integers that give a remainder of  $a$  when divided by  $n$ . (In this case we call  $a$  a standard representative of  $[a]$ .)
3. If  $[a] = [b]$ , it does not mean  $a = b$ , only that  $a \equiv b \pmod{n}$  or that  $a$  and  $b$  give the same remainder when divided by  $n$ .

### The set of congruence classes. Modular Arithmetic

Consider the following partition of  $\mathbf{Z}$  by set of congruence classes:

$$\mathbf{Z}_n = \{[0], [1], [2], \dots, [n-1]\}$$

**Addition on  $\mathbf{Z}_n$  :**  $[a] + [b] = [a + b]$

**Multiplication on  $\mathbf{Z}_n$  :**  $[a][b] = [ab]$

EXAMPLE 9. Give addition and multiplication tables for  $\mathbf{Z}_n$  for  $n = 2, 3$ .

$n = 2$	+	[0]	[1]
	[0]		
	[1]		

·	[0]	[1]
[0]		
[1]		

$n = 3$	+	[0]	[1]	[2]
	[0]			
	[1]			
	[2]			

·	[0]	[1]	[2]
[0]			
[1]			
[2]			

EXAMPLE 10. Compute

(a) in  $\mathbf{Z}_6$ ,

$$[2][3] =$$

$$[2][4] =$$

(b) in  $\mathbf{Z}_{11}$ ,

$$[6][7] =$$

$$[25] + [22] =$$

THEOREM 11. Let  $n \in \mathbf{Z}$ ,  $n > 1$ .

1. Addition in  $\mathbf{Z}_n$  is commutative

2. Addition in  $\mathbf{Z}_n$  is associative

3.  $[0]$  is the multiplicative identity of  $\mathbf{Z}_n$  w.r.t. addition:

4. Every element of  $\mathbf{Z}_n$  has an inverse w.r.t. addition. Namely, for every  $a \in \mathbf{Z}$  the additive inverse of  $[a]$  is  $[-a]$ .

THEOREM 12. Let  $n \in \mathbf{Z}$ ,  $n > 1$ .

1. Multiplication in  $\mathbf{Z}_n$  is commutative
2. Multiplication in  $\mathbf{Z}_n$  is associative
3.  $[1]$  is the multiplicative identity of  $\mathbf{Z}_n$ :
4. The following distributive laws hold:

$$[a]([b] + [c]) =$$

$$([a] + [b])[c] =$$

DEFINITION 13. An element  $[a] \in \mathbf{Z}_n$  has an inverse w.r.t. multiplication if there exists  $[x] \in \mathbf{Z}_n$  such that  $[a][x] = [1]$ .

EXAMPLE 14.  $[5]$  is invertible in  $\mathbf{Z}_9$  because

However,  $[3]$  and  $[6]$  are not invertible in  $\mathbf{Z}_9$  because

THEOREM 15. Let  $[a] \in \mathbf{Z}_n$ . Then  $[a]$  has a multiplicative inverse if and only if  $a$  and  $n$  are relatively prime, i.e.  $\gcd(a, n) = 1$ .

*Proof.*

EXAMPLE 16. Is  $[51]$  invertible in  $\mathbf{Z}_{65}$  w.r.t. multiplication? If yes, find its inverse.

### Fermat's Little Theorem

Question: Which of the following are true for any integer  $a$ ?

- $2|a^2 - a$
  
- $3|a^3 - a$
  
- $4|a^4 - a$
  
- $5|a^5 - a$

What is wrong with number 4?

**Fermat's Little Theorem.** For any prime integer  $p$  and  $a \in \mathbf{Z}$ ,

$$p|a^p - a.$$

Equivalently

**Alternative version of Fermat's Little Theorem.** For any prime integer  $p$  and  $a \in \mathbf{Z}$  such that  $a$  and  $p$  are relatively prime, i.e.  $\gcd(a, p) = 1$ , one has

$$p|a^{p-1} - 1 \quad \text{or} \quad a^{p-1} \equiv 1 \pmod{p}.$$

EXAMPLE 17. Find the remainder if  $7^{985}$  is divided by 13.