

# Exam 2

1.  $6x \equiv -x \equiv 1 \pmod{7}$  (given)

$\therefore x \equiv -1$

$\therefore \exists x \in \{0, 1, \dots, 6\}$ ,  $\boxed{x = 6}$

2. (a)  $324^{123} \equiv 4^{123} \pmod{10}$

But,  $4^2 = 16 \equiv 6 \equiv -4 \pmod{10}$

$\therefore 4^4 \equiv (-4)^2 = 16 \equiv 6 \equiv -4 \pmod{10}$

$\therefore 4^5 \equiv (-4) \cdot 4 = -16 \equiv 4 \pmod{10}$

$\therefore 4^{10} \equiv 4^2 \equiv -4 \pmod{10}$

$\therefore (4^{10})^{10} \equiv (-4)^{10} = 4^{10} \equiv -4 \pmod{10}$

$\therefore 4^{123} \equiv 4^{100} \cdot (4^{10})^2 \cdot 4^3 \pmod{10}$

$\equiv (-4) \cdot (-4) \cdot 4^3 = 4^5 \pmod{10}$

b) Let  $P(k) : 4^{2k-1} \equiv 4 \pmod{10}$

$k=1 : 4 \equiv 4 \pmod{10} \checkmark$

$\{ 4^{2k-1} \equiv 4 \pmod{10}$

Then,  $4^{2(k+1)-1} = 4^{2k-1} \cdot 4 \equiv 4 \cdot 16 \equiv 4 \cdot (-4) \pmod{10}$

$\equiv -16 \equiv 4 \pmod{10} \quad \square$

Second argument (without induction.)

$4^{2k-1} \equiv 0 \equiv 4 \pmod{2}$

$4^{2k-1} \equiv 4^{2(k-1)+1} \pmod{5}$

$\equiv (4^2)^{k-1} \cdot 4$

$\equiv 1^{k-1} \cdot 4 \equiv 4$

Hence, 2 and 5 are relatively prime since they are relatively prime.

$\left. \begin{array}{l} 2 \\ 5 \end{array} \right\} \begin{array}{l} 4^{2k-1} \\ 4^{2k-1} \\ 4^{2k-1} \end{array}$

$$(c) \quad 324 \stackrel{123}{=} 2 \stackrel{123}{=} 2 \pmod{7}$$

$$\text{But } 2^3 = 8 \equiv 1 \pmod{7}$$

$$\therefore 2^{123} \equiv (2^3)^{40} \equiv 1 \pmod{7}$$

$$3. (a) \quad 377 = 2 \cdot (127) + 23$$

$$127 = 1 \cdot (123) + 4$$

$$123 = 30 \cdot (4) + 3$$

$$4 = 1 \cdot (3) + 1$$

$$3 = 3 \cdot (1) + 0$$

$$\therefore \gcd(377, 127) = 1$$

(b)

$$1 = 4 - 1 \cdot 3 = 4 - 1 \cdot (123 - 30 \cdot 4)$$

$$= 31 \cdot (4) - 1 \cdot (123)$$

$$= 31 \cdot (127 - 1 \cdot 123) - 1 \cdot (123)$$

$$= 31 \cdot (127) - 32 \cdot (123)$$

$$= 31 \cdot (127) - 32 \cdot (377 - 2 \cdot 127)$$

$$= 95 \cdot (127) - 32 \cdot (377)$$

$$\therefore x = -32$$

$$y = 95$$

works

4. ~~(a)~~ Induction.

$$k=1. \quad n^p \equiv n \pmod{p} \quad \text{by FLT.}$$

$$\& \quad n^{pk} \equiv n \pmod{p}$$

$$\text{Show } n^{p^{k+1}} \equiv n \pmod{p}$$

$$\text{But, } n^{p^{k+1}} \equiv n^{p^k \cdot p} \equiv (n^{p^k})^p \stackrel{IH}{=} (n)^p \stackrel{FLT}{=} n \quad \square$$

5. We know  $n^p \equiv n \pmod{p}$ , In other words  
 $p$  divides  $n^p - n = n(n^{p-1} - 1)$   
Since  $\gcd(p, n) = 1$ ,  $p$  divides  $n^{p-1} - 1$ . Hence,  
 $n^{p-1} \equiv 1 \pmod{p}$

---

6.  $\S$   $f$  1-1. Fix  $A, B \subseteq X$ . By definition

$f(A \cap B) \subseteq f(A)$   
and  $f(A \cap B) \subseteq f(B)$ , since  $A \cap B \subseteq A$  and  $A \cap B \subseteq B$ .

$\therefore f(A \cap B) \subseteq f(A) \cap f(B)$ .

For the other direction, let  $y \in f(A) \cap f(B)$

$\therefore y \in f(A) = \{f(a) : a \in A\}$ .

$\therefore y = f(a)$  for some  $a \in A$ .

Similarly,

$y \in f(B)$ , so  $y = f(b)$  for some  $b \in B$ .

$\therefore f(a) = y = f(b)$ .  $\therefore f(a) = f(b)$ . Since  $f$  is 1-1  
 $a = b$ .  $\therefore a \in A$  and  $a = b \in B$ . So,  $a \in A \cap B$ .

$\therefore y = f(a)$ ,  $a \in A \cap B$ . So,  $y \in f(A \cap B)$ .

---

7.  $\S$   $f$  is onto. Show  $F$  is 1-1.

$\S$   $F(y_1) = F(y_2)$  or (by the definition of  $F$ )

$f^{-1}(\{y_1\}) = f^{-1}(\{y_2\})$

Since  $f$  is onto,  $\exists x_1 \in X$  s.t.  $f(x_1) = y_1$ .

$\therefore x_1 \in f^{-1}(\{y_1\}) = f^{-1}(\{y_2\})$ .  $\therefore f(x_1) \in \{y_2\}$

$\therefore f(x_1) = y_2$   $\therefore y_1 = f(x_1) = y_2$ .  $\therefore y_1 = y_2$

$\therefore F$  is 1-1.