

## 1

(a) **Claim:** If  $d|a$  and  $d|b$  then  $d|ax + by$  for all  $x, y \in \mathbb{Z}$ .

**Proof:**  $d|a \Rightarrow \exists k_1 \in \mathbb{Z}, a = k_1d, d|b \Rightarrow \exists k_2 \in \mathbb{Z}, b = k_2d, ax + by = k_1xd + k_2yd = (k_1x + k_2y)d$  with  $k_1x + k_2y$  for all  $x, y \in \mathbb{Z}$ , so  $d|ax + by$  for all  $x, y \in \mathbb{Z}$ . ■

(b) **Claim:** If  $a|b$  and  $c|d$ , then  $ac|bd$ .

**Proof:**  $a|b \Rightarrow \exists k_1 \in \mathbb{Z}, b = k_1a, c|d \Rightarrow \exists k_2 \in \mathbb{Z}, d = k_2c$ , then  $bd = k_1ak_2c = k_1k_2ac$  with  $k_1k_2 \in \mathbb{Z}$  by closure. So if  $a|b$  and  $c|d$ , then  $ac|bd$ . ■

(c) **Claim:** If  $a|b$  and  $c|d$ , then  $(a + c)|(b + d)$ .

**Proof:**  $a|b \Rightarrow \exists k_1 \in \mathbb{Z}, b = k_1a, c|d \Rightarrow \exists k_2 \in \mathbb{Z}, d = k_2c$ , then  $b + d = (k_1 + k_2)c$  with  $k_1 + k_2 \in \mathbb{Z}$ .

## 2

(a) **Claim:** If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $ac \equiv bd \pmod{m}$ .

**Proof:**  $a \equiv b \pmod{m} \Rightarrow \exists k_1 \in \mathbb{Z}, (a - b) = k_1m, c \equiv d \pmod{m} \Rightarrow \exists k_2 \in \mathbb{Z}, (c - d) = k_2m, ac - bd = (b + k_1m)(d + k_2m) - bd = bd + k_1md + k_2mb + k_1k_2m^2 - bd = k_1md + k_2mb + k_1k_2m^2 = m(k_1d + k_2b + k_1k_2m)$ .

Thus,  $ac \equiv bd \pmod{m}$ . ■

(b) **Claim:** If  $a \equiv b \pmod{m}$ , then for any  $k \in \mathbb{N}$ ,  $a^k \equiv b^k \pmod{m}$ .

**Proof:** Base case, let  $c = a, d = b$ , we have statement to be true when  $k = 1$ .

Suppose, the statement is true when  $k = n$ ,  $a^n \equiv b^n \pmod{m}$ . Then when  $k = n + 1$ , let  $a = b + tm$ ,  $a^{n+1} - b^{n+1} = (b + tm)^{n+1} - b^{n+1} = \sum_{i=0}^n \binom{n+1}{i} b^{n+1-i} y^i - b^{n+1}$ , which is a multiple of  $m$ , so  $m|(a^{n+1} - b^{n+1}) \Rightarrow a^{n+1} \equiv b^{n+1} \pmod{m}$ .

As a result, if  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $ac \equiv bd \pmod{m}$ . ■

## 3

(a) Since  $347 \equiv 7 \pmod{10} \Rightarrow 347^4 \equiv 1 \pmod{10} \Rightarrow 347^{100} \equiv 1 \pmod{10} \Rightarrow 347^{101} \equiv 7 \pmod{10}$ , so the last decimal digit is 7.

(b) According to Fermat's Little Theorem,  $347^{101} \equiv 347 \pmod{101} = 44$  since 101 is a prime.

(c) According to Fermat's Little Theorem,  $2^{13} \equiv 2 \pmod{13}$ , then  $2^{100} \equiv 2^{12 \cdot 8 + 4} \equiv (2^{12})^8 \cdot 2^4 \equiv 3 \pmod{13}$ .

(d)

(i) Since  $9 = 11_8$ ,  $11^2 = 121$ ,  $11^3 = 1331 \dots$ , so  $9^{1000} = (11_8)^{1000}$  ends with 1.

(ii) Since  $10 = 12_8$ ,  $12^2 = 144$ ,  $12^3 = 1750 \dots$ ,  $10^{1000}$  ends with 0.

(iii) Since  $11 = 13_8$ , then  $13 = 13$ ,  $13^2 = 171 \dots$ , so  $11^{1000}$  ends with 1.