

Khoa Tran

1. a. $a = 35, b = 256, m = 10$

i. $(35 + 256) \pmod{10} = 291 \pmod{10} = 1 \pmod{10}$

ii. $35 \pmod{10} + 256 \pmod{10} = 5 \pmod{10} + 6 \pmod{10} = 11 \pmod{10} = 1 \pmod{10}$

b. $a = -300, b = -93, m = 26$

i. $(-300 + -93) \pmod{26} = -393 \pmod{26} = -3 \pmod{26} = 23 \pmod{26}$

ii. $-300 \pmod{26} + (-93 \pmod{26}) = -14 \pmod{26} + (-15 \pmod{26}) = -29 \pmod{26} = -3 \pmod{26} = 23 \pmod{26}$

c. $a = 10496, b = -5899, m = 256$

i. $(10496 - 5899) \pmod{256} = 4597 \pmod{256} = 245 \pmod{256} = -11 \pmod{256}$

ii. $10496 \pmod{256} + (-5899 \pmod{256}) = 0 \pmod{256} - 11 \pmod{256} = -11 \pmod{256} = 245 \pmod{256}$

d. $a = 771, b = 400375, m = 1024$

i. $(771 + 400375) \pmod{1024} = 401146 \pmod{1024} = 762 \pmod{1024} = -262 \pmod{1024}$

$$\begin{aligned} 771 \pmod{1024} + 400375 \pmod{1024} &= 771 \pmod{1024} + 1015 \pmod{1024} = 1786 \pmod{1024} \\ &= 762 \pmod{1024} = -262 \pmod{1024} \end{aligned}$$

e. $a = -37388, b = 509, m = 4096$

i. $(-37388 + 509) \pmod{4096} = -36879 \pmod{4096} = -15 \pmod{4096} = 4081 \pmod{4096}$

ii. $(-37388 \pmod{4096}) + 509 \pmod{4096} = -524 \pmod{4096} + 509 \pmod{4096} = -15 \pmod{4096} = 4081 \pmod{4096}$

f. $a = -25678, b = -895632, m = 33558$

i. $(-25678 - 895632) \pmod{33558} = -921310 \pmod{33558} = -15244 \pmod{33558} = 18314 \pmod{33558}$

ii. $-25678 \pmod{33558} - 895632 \pmod{33558} = 1880 \pmod{33558} - 23124 \pmod{33558}$

$$= -15244 \pmod{33558} = 18314 \pmod{33558}$$

2. a. $a = 432, b = 163, m = 12$

i. $(432 \cdot 163) \pmod{12} = 70416 \pmod{12} = 0 \pmod{12}$

ii. $432 \pmod{12} \cdot 163 \pmod{12} = 0 \pmod{12} \cdot 7 \pmod{12} = 0 \pmod{12}$

b. $a = -531, b = -435, m = 26$

i. $(-531 \cdot -435) \pmod{26} = 230985 \pmod{26} = 1 \pmod{26}$

ii. $-531 \pmod{26} \cdot -435 \pmod{26} = -11 \pmod{26} \cdot -9 \pmod{26} = 209 \pmod{26} = 1 \pmod{26}$

c. $a = -2465, b = 8526, m = 512$

i. $(-2465 \cdot 8526) \pmod{512} = -21016590 \pmod{512} = -14 \pmod{512} = 498 \pmod{512}$

ii. $-2465 \pmod{512} \cdot 8526 \pmod{512} = -417 \pmod{512} \cdot 334 \pmod{512}$

$$= -139278 \pmod{512} = -14 \pmod{512} = 498 \pmod{512}$$

d. $a = 1024, b = 400375, m = 2048$

i. $(1024 \cdot 400375) \pmod{2048} = 409984000 \pmod{2048}$

$$= 1024 \pmod{2048}$$

ii. $1024 \pmod{2048} \cdot 400375 \pmod{2048} = 1024 \pmod{2048} \cdot 1015 \pmod{2048}$

$$= 1039360 \pmod{2048}$$

$$= 1024 \pmod{2048}$$

e. $a = -45599, b = 7999, m = 8192$

i. $(-45599 \cdot 7999) \pmod{8192} = -364746401 \pmod{8192} = -5793 \pmod{8192}$

$$= 2399 \pmod{8192}$$

ii. $-45599 \pmod{8192} \cdot 7999 \pmod{8192} = -4639 \pmod{8192} \cdot 7999 \pmod{8192}$

$$= -37107361 \pmod{8192} = -5793 \pmod{8192}$$

$$= 2399 \pmod{8192}$$

f. $a = -4536783, b = -39632, m = 47384$

i. $(-4536783 \cdot -39632) \pmod{47384} = 21172 \pmod{47384}$

ii. $-4536783 \pmod{47384} \cdot -39632 \pmod{47384} = -35303 \pmod{47384} \cdot -39632 \pmod{47384}$

$$= 1399128496 \pmod{47384}$$

$$= 21128 \pmod{47384}$$

3c. a. $a = 777, m = 26$

$$\gcd(777, 26) = 1 \text{ so } 777^{-1} \pmod{26} \text{ exist}$$

i. $777^{-1} \pmod{26} = 17 \pmod{26} = -9 \pmod{26}$

ii. $(777 \pmod{26})^{-1} \pmod{26} = 23^{-1} \pmod{26} = -9 \pmod{26} = 17 \pmod{26}$

b. $a = -37, m = 512$

$$\gcd(-37, 512) = 1 \text{ so } -37^{-1} \pmod{512} \text{ exist}$$

i. $-37^{-1} \pmod{512} = 83 \pmod{512}$

ii. $(-37 \pmod{512})^{-1} \pmod{512} = 475^{-1} \pmod{512} = 83 \pmod{512}$

c. $a = 24865, m = 4096$

$$\gcd(24865, 4096) = 1 \text{ so } 24865^{-1} \pmod{4096} \text{ exist}$$

i. $24865^{-1} \pmod{4096} = 737 \pmod{4096}$

ii. $(24865 \pmod{4096})^{-1} \pmod{4096} = 289^{-1} \pmod{4096} = 737 \pmod{4096}$

d. $a = -256789, m = 56789$

$$\gcd(-256789, 56789) = 1 \text{ so } -256789^{-1} \pmod{56789} \text{ exist}$$

i. $-256789^{-1} \pmod{56789} = 25586 \pmod{56789}$

ii. $(-256789 \pmod{56789})^{-1} \pmod{56789} = (27156)^{-1} \pmod{56789}$

$$= 25586 \pmod{56789}$$

e. $a = -1900757, m = 770077$

i. $\gcd(-1900757, 770077) = 1 \text{ so } -1900757^{-1} \pmod{770077} \text{ exist}$

i. $-1900757^{-1} \pmod{770077} = 237731 \pmod{770077}$

ii. $((-1900757) \pmod{770077})^{-1} \pmod{770077} = 409474^{-1} \pmod{770077} = 237731 \pmod{770077}$

e. As the value of the module gets bigger, the time it takes to compute the modular inverse increases as it starts from 0s and increases to 0.026 seconds. As module value increases, time increases as well.

4a. $(32 \cdot (-71) + 782) \pmod{7} =$

$$(32 \pmod{7} \cdot (-71) \pmod{7} + 782 \pmod{7}) =$$

$$4 \pmod{7} \cdot -1 \pmod{7} + 5 \pmod{7} =$$

$$-4 \pmod{7} + 5 \pmod{7} = 1 \pmod{7}$$

b. $(-534 \cdot (90 + 4382)) \pmod{26} =$

$$-534 \pmod{26} \cdot (90 \pmod{26} + 4382 \pmod{26}) =$$

$$12 \pmod{26} \cdot (12 \pmod{26} + 14 \pmod{26})$$

$$12 \pmod{26} \cdot 26 \pmod{26} = 12 \pmod{26} \cdot 0 \pmod{26} = 0 \pmod{26}$$

c. $((-543 - 4652) \cdot (-75 + 976)) \pmod{256} =$

$$((-543 \pmod{256} - 4652 \pmod{256}) \cdot (-75 \pmod{256} + 976 \pmod{256})) =$$

$$(-31 \pmod{256} - 44 \pmod{256}) \cdot (-75 \pmod{256} + 208 \pmod{256})$$

$$(-75 \pmod{256}) \cdot (133 \pmod{256}) = -9975 \pmod{256} = 9 \pmod{256}$$

d. $((313^2 \cdot (-782)) \pmod{2048})$

$$((313 \pmod{2048})^2 \cdot (-782 \pmod{2048})) =$$

$$(1065^2 \pmod{2048}) \cdot (1266 \pmod{2048}) =$$

$$1134225 \pmod{2048} \cdot 1266 \pmod{2048} =$$

$$1681 \pmod{2048} \cdot 1266 \pmod{2048} =$$

$$2128146 \pmod{2048} = 274 \pmod{2048}$$

e. $((-5)^4 \cdot 2153^{-3}) \pmod{4096}$

$$((-5 \pmod{4096})^4 \cdot (2153 \pmod{4096})^{-3})$$

$$(625 \pmod{4096} \cdot (2153 \pmod{4096})^3)^{-1} \pmod{4096} =$$

$$((625 \pmod{4096}) \cdot (2009 \pmod{4096})^3)^{-1} =$$

$$625 \pmod{4096} \cdot 8108486729 \pmod{4096} =$$

$$625 \pmod{4096} \cdot 73 \pmod{4096} = 45625 \pmod{4096} = 569 \pmod{4096}$$

f. $((635 \cdot 3 + 7762)^7 \cdot ((-5462)^2 - (216)^{-1})^5 \pmod{12235})$

$$(((635 \pmod{12235} \cdot 3 \pmod{12235} + 7762 \pmod{12235})^7 \pmod{12235}) \cdot ((-5462 \pmod{12235})^2 - (216)^{-1} \pmod{12235})^5 \pmod{12235} =$$

$$((-105 \pmod{12235} + 7762 \pmod{12235})^7 \pmod{12235}) \cdot ((-5462 \pmod{12235})^2 - (216)^{-1} \pmod{12235})^5 \pmod{12235} =$$

$$(7657^{-1} \pmod{12235})^7 \pmod{12235}$$

$$(-302 \pmod{12235})^7 \pmod{12235}$$

$$3270 \pmod{1$$