Aaron Hong
EE418 HW1
10/19/23

1) a) $a = 30,\ b = 236,\ m = 10$

i) $(30+236) \bmod 10 = 266 \bmod 10 = 6 \bmod 10$

ii) $30 \bmod 10 + 236 \bmod 10 = 0 + 6 \bmod 10 = 6 \bmod 10$

b) $a = -310,\ b = -95,\ m = 26$

i) $(-310 + -95) \bmod 26 = -405 \bmod 26 = 11 \bmod 26$

ii) $-310 \bmod 26 - 95 \bmod (26) = 2 \bmod 26 + 9 \bmod 26 = 11 \bmod 26$

c) $a = 1036,\ b = -5219,\ m = 256$

i) $(1036 - 5219) \bmod 256 = -4183 \bmod 256 = 169 \bmod 256$

ii) $1036 \bmod 256 - 5219 \bmod 256 = 12 \bmod 256 + 157 \bmod 256 = 169 \bmod 256$

d) $a = 770,\ b = 40375,\ m = 1024$

i) $(770 + 40375) \bmod 1024 = 41145 \bmod 1024 = 185 \bmod 1024$

ii) $770 \bmod (1024) + 40375 \bmod 1024 = 770 \bmod 1024 + 439 \bmod 1024 = 1209 \bmod 1024 = 185 \bmod 1024$

e) $a = -37348,\ b = 519,\ m = 4096$

i) $(-37348 + 519) \bmod 4096 = -36829 \bmod 4096 = 35 \bmod 4096$

ii) $-37348 \bmod 4096 + 519 \bmod 4096 = 3612 \bmod 4096 + 519 \bmod 4096 = 4131 \bmod 4096 = 35 \bmod 4096$

f) $a = -25778,\ b = -895732,\ m = 33558$

i) $(-25778 - 895732) \bmod 33558 = -921510 \bmod 33558 = 18114 \bmod 33558$

ii) $-25778 \bmod 33558 - 895732 \bmod 33558 = 7780 \bmod 33558 + 10334 \bmod 33558 = 18114 \bmod 33558$

2) a) $a = 442,\ b = 153,\ m = 12$

i) $(442 \cdot 153) \bmod 12 = 67626 \bmod 12 = 6 \bmod 12$

ii) $442 \bmod 12 \cdot 153 \bmod 12 = 10 \bmod 12 \cdot 9 \bmod 12 = 90 \bmod 12 = 6 \bmod 12$

b) $a = -532,\ b = -415,\ m = 26$

i) $(-532 \cdot -415) \bmod 26 = 220780 \bmod 26 = 14 \bmod 26$

ii) $-532 \bmod 26 \cdot -415 \bmod 26 = 14 \bmod 26 \cdot 1 \bmod 26 = 14 \bmod 26$

c) $a = -2475,\ b = 8426,\ m = 512$

i) $(-2475 \cdot 8426) \bmod 512 = -20854350 \bmod 512 = 434 \bmod 512$

ii) $-2475 \bmod 512 \cdot 8426 \bmod 512 = 85 \bmod 512 \cdot 234 \bmod 512 = 19890 \bmod 512 = 434 \bmod 512$

d) $a = 1014,\ b = 401375,\ m = 2048$

i) $(1014 \cdot 401375) \bmod 2048 = 406994250 \bmod 2048 = 1354 \bmod 2048$

ii) $1014 \bmod 2048 \cdot 401375 \bmod 2048 = 1014 \bmod 2048 \cdot 2015 \bmod 2048 = 2043210 \bmod 2048 = 1354 \bmod 2048$

e) $a = -46589,\ b = 7898,\ m = 8192$

i) $(-46589 \cdot 7898) \bmod 8192 = -367959922 \bmod 8192 = 142 \bmod 8192$

ii) $-46589 \bmod 8192 \cdot 7898 \bmod 8192 = 2563 \bmod 8192 \cdot 7898 \bmod 8192 = 20242574 \bmod 8192 = 142 \bmod 8192$

f) $a = -4556883,\ b = -87631,\ m = 47384$

i) $(-4556883 \cdot -87631) \bmod 47384 = 171480064173 \bmod 47384 = 21677 \bmod 47384$

ii) $-455683 \bmod 47384 \cdot -87631 \bmod 47384 = 89365 \bmod 47384 \cdot 9753 \bmod 47384 = 883926845 \bmod 47384 = 21677 \bmod 47384$

EE418 HW1 cont

3) c) $a = 777,\ m = 26 \rightarrow gcd = 1$

i) $777^{-1} \bmod 26 = 17 \bmod 26$

ii) $777 \bmod 26^{-1} \bmod 26 = 23^{-1} \bmod 26 = 17 \bmod 26$

$a = -37,\ m = 512 \rightarrow gcd = 1$

i) $-37^{-1} \bmod 512 = 83 \bmod 512$

ii) $-37 \bmod 512^{-1} \bmod 512 = 475^{-1} \bmod 512 = 83 \bmod 512$

$a = 24865,\ m = 4096 \rightarrow gcd = 1$

i) $24865^{-1} \bmod 4096 = 737 \bmod 4096$

ii) $24865 \bmod 4096^{-1} \bmod 4096 = 289^{-1} \bmod 4096 = 737 \bmod 4096$

$a = -256789,\ m = 56789 \rightarrow gcd = 1$

i) $-256789 \bmod 56789 = 25586 \bmod 56789$

ii) $-256789 \bmod 56789^{-1} \bmod 56789 = 27156^{-1} \bmod 56789 = 25586 \bmod 56789$

$a = -1900757,\ m = 770077 \rightarrow gcd = 1$

i) $-1900757^{-1} \bmod 770077 = 237731 \bmod 770077$

d) 0.0 sec, 0.0 sec, 0.0 sec, 0.006 sec, 0.6 sec

e) as the numbers get bigger, the runtime increases. This is because there are more calculations to be done with larger numbers.

3b) 6, 243, 1

5a)

x	1	2	3	4	5	6	7	8
$\pi^{-1}(x)$	2	4	6	1	8	3	5	7

4) a) $82 \bmod 7 \cdot -71 \bmod 7 + 782 \bmod 7 = 4 \bmod 7 \cdot 6 \bmod 7 + 5 \bmod 7$

$= 29 \bmod 7 = 1 \bmod 7$

b) $-534 \bmod 26 \cdot (90 \bmod 26 + 4382 \bmod 26) = -14 \bmod 26 \cdot (12 \bmod 26 + 14 \bmod 26)$

$= 12 \bmod 26 \cdot (26 \bmod 26) \rightarrow 0 = 0$

c) $(-543 \bmod 256 - 4652 \bmod 26) \cdot (-75 \bmod 256 + 976 \bmod 256)$

$= (225 \bmod 256 - 44 \bmod 26) \cdot (181 \bmod 256 + 208 \bmod 256)$

$= 181 \bmod 256 \cdot 389 \bmod 256 = 181 \bmod 256 \cdot 133 \bmod 256$

$= 24073 \bmod 256 = 9 \bmod 256$

d) $8113^2 \bmod 2048 \cdot -782 \bmod 2048 = 1065^2 \bmod 2048 \cdot 1266 \bmod 2048$

$= 1134225 \bmod 2048 \cdot 1266 \bmod 2048 = (1681 \cdot 1266) \bmod 2048$

$= 2128146 \bmod 2048 = 274 \bmod 2048$

e) $-5^4 \bmod 4096 \cdot (2153^{-1})^3 \bmod 4096 = 625 \bmod 4096 \cdot 2009^3 \bmod 4096$

$= 625 \bmod 4096 \cdot 8108486729 \bmod 4096 = 625 \bmod 4096 \cdot 73 \bmod 4096$

$= 45625 \bmod 4096 = 569 \bmod 4096$

f) $-35 \cdot 8 = -105,\ -105 + 7762 = 7657,\ -5462^2 = 29833444$

$= ((7657)^{-1})^7 \bmod 12235 \cdot (29833444 \bmod 12235 - (2161)^{-1} \bmod 12235)^5$

$= 11933^7 \bmod 12235 \cdot (4514 \bmod 12235 - 4971 \bmod 12235)^5$

$= 3445462158071773219982259067 \bmod 12235 \cdot (-457)^5 \bmod 12235$

$= 9917 \bmod 12235 \cdot -19933382494057 \bmod 12235 = (9917 \cdot 8458) \bmod 12235$

$= 83877986 \bmod 12235 = 7061 \bmod 12235$