Week 8 HW – Cryptography
Theo Shin

Part A: Finding Modular Inverses

1. $x \cdot 3 \bmod 10 = 1$

$\gcd(3,10) = \frac{3^1}{2^1 \cdot 5^1} = 1$

$\boxed{x^3 \equiv 1} \bmod 10$

$-17, -7, \boxed{7}, 17, 27$

2. Modular inverses are not unique, Looking at the first problem, the 7 representative can be written so that $\boxed{x \cdot 3 \equiv 1}$ mod 10 such that a progression of numbers would work by adding or subtracting 10 from 7. Since we are progressing by 10, they all x's end with 7.

3. $x \cdot 5 \bmod 10 = 1$

$\gcd(5,10) = \frac{5^1}{2^1 5^1} = 5 \Rightarrow$ Since they are not relatively prime, a modular inverse does not exist

$x \cdot 2 \bmod 10 = 1$

$\gcd(2,10) = \frac{2^1 \cdot 5^1}{2} = 2 \Rightarrow$ Again, not relatively prime so a modular inverse does not exist.

Week 8 HW – Cryptography
Theo Shin

Find the inverse if you can.

x * 7 mod 10 = 1

x * 26 mod 13 = 1

x * 7 mod 5 = 1

x * 5 mod 21 = 1

x * 6 mod 35 = 1

x * 7 mod 13 = 1

① $x * 7 \bmod 10 = 1$

$\gcd(7, 10) = \frac{7^1}{2^1 \cdot 5^1} = 1$

$\boxed{x * 7 \equiv 1} \bmod 10$

$x = 3$

$\{-23, -13, 3, 13, 23\}$

③ $x * 7 \bmod 5 = 1$

$\gcd(5, 7) = \frac{5^1}{7^1} = 1$

$\boxed{x * 7 \equiv 1} \bmod 5$

$x = 3$

$\{-7, -2, 3, 8, 13\}$

② $x * 26 \bmod 13 = 1$

$\gcd(13, 26) = \frac{13^1}{13^1 \cdot 2} = 13$

Not relatively prime ⇒ Cannot compute inverse

④ $x * 5 \bmod 21 = 1$

$\gcd(5, 21) = \frac{5^1}{3^1 \cdot 7^1} = 1$

$\boxed{x * 5 \equiv 1} \bmod 21$

$x = 17$

$\{-25, -4, 17, 38, 59\}$

⑤ $x * 6 \bmod 35 = 1$

$\gcd(6, 35) = \frac{2^1 \cdot 3^1}{5^1 \cdot 7^1} = 1$

$\boxed{x * 6 \equiv 1} \bmod 35$

$x = 6$

$\{-64, -29, 6, 41, 76\}$

⑥ $x * 7 \bmod 13 = 1$

$\gcd(7, 13) = \frac{7^1}{13^1} = 1$

$x = 2$

$\{-24, -11, 2, 15, 28\}$

What is the rule for when Modular inverses exist?

A modular inverse exists only if the two integers are relatively prime (GCD is 1).

Week 8 HW – Cryptography
Theo Shin

4. Do #1-4 page 284 SHOW YOUR WORK

p. 284

1. $\boxed{x \cdot 7 \equiv 1}$ (mod 26)

$\gcd(7, 26) = \frac{7^1}{2^1 \cdot 13^1} = 1$

$x = 15$

$\{-37, -11, \boxed{15}, 41, 67\}$

2. $\boxed{x \cdot 13 \equiv 1}$ (mod 2436)

$\gcd(13, 2436) = \frac{13^1}{1218 \cdot 2}$
$= 609 \cdot 2^2$
$= 203 \cdot 3 \cdot 2^2$
$= 29 \cdot 7 \cdot 3 \cdot 2^2$

relatively prime

$x = 937 \Rightarrow 937 \cdot 13 = \boxed{12{,}181 \equiv 1 \pmod{2436}}$

3. $\gcd(a, m) = 1$
$sa + tm = 1$
$sa + tm \equiv 1 \pmod{m}$
$sa \equiv 1 \pmod{m}$

4 mod 9

$(j) \cdot 4 \equiv 1 \pmod{9}$

$\gcd(4, 9) = \frac{2^2}{3^2} = 1$

$j = 7$

$\{-11, -2, \boxed{7}, 16, 25\}$

4. 2 mod 17

$\boxed{(j) \cdot 2 \equiv 1}$ (mod 17)

$\gcd(2, 17) = \frac{2^1}{17^1} = 1$

$j = 9$

$\{-25, -8, \boxed{9}, 26, 43\}$

Week 8 HW – Cryptography
Theo Shin

Part B:

If an inverse of a mod n exists, what is the gcd(a,n)? Why?

The inverse of a mod n exists only when gcd(a,n) is 1 by Bezout's theorem.

LEMMA 2 If a, b, and c are positive integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Proof: Because $\gcd(a, b) = 1$, by Bézout's theorem there are integers s and t such that

$$sa + tb = 1.$$

Multiplying both sides of this equation by c, we obtain

$$sac + tbc = c.$$

We can now use Theorem 1 of Section 4.1 to show that $a \mid c$. By part (ii) of that theorem, $a \mid tbc$
Because $a \mid sac$ and $a \mid tbc$, by part (i) of that theorem, we conclude that a divides $sac + tbc$
Because $sac + tbc = c$, we conclude that $a \mid c$, completing the proof.

This can also be expressed as ax ≡ 1 (mod b) and if a and b have a common factor, then it can be proved by contradiction, the common factor would divide the 1.

Week 8 HW – Cryptography
Theo Shin

1. Now do #5 and #6 page 284

#5

5. (a) $a=4, m=9$

$\gcd(4,9)$

$9 = 4(2) + \boxed{(1)}$

$4 = 1(4) + 0$

$\gcd(9,4) = 1$

$9 - 4(2) = (1)$

$9s + 4t = \gcd(9,4)$

$9s + 4t = 1$

$9 - 4(2) = 1$

$9s + 4(-2) = 1$

$s = 1$

$t = -2$

inverse

coefficient of a

(b) $a=19, m=141$

$\gcd(141,19)$

$141 = 19(7) + (8)$

$19 = 8(2) + (3)$

$8 = 3(2) + (2)$

$3 = 2(1) + \boxed{(1)}$

$2 = 1(2) + (0)$

$141 - 19(7) = (8)$

$19 - 8(2) = (3)$

$8 - 3(2) = (2)$

$3 - 2(1) = (1)$

$141s + 19t = \gcd(141,19)$

$141s + 19t = 1$

$3 - 2(1) = 1$

$3 - (8 - 3(2)) = 1$

$3 - 8 + (2)3 = 1$

$3(3) - 8 = 1$

$3(19 - 8(2)) - 8 = 1$

$3 \cdot 19 - 6 \cdot 8 - 8 = 1$

$3 \cdot 19 - 7 \cdot 8 = 1$

$3 \cdot 19 - 7 \cdot (141 - 19(7)) = 1$

$3 \cdot 19 - 7 \cdot 141 + 49 \cdot 19$

$= 52 \cdot 19 - 7 \cdot 141 = 1$

$= 141(-7) + 19(52) = 1$

$s = -7$

$t = 52$

Week 8 HW – Cryptography
Theo Shin

5. (c) $a = 55, m = 89$

$\gcd(89, 55)$

$89 = 55(1) + (34)$
$55 = 34(1) + (21)$
$34 = 21(1) + (13)$
$21 = 13(1) + (8)$
$13 = 8(1) + (5)$
$8 = 5(1) + (3)$
$5 = 3(1) + (2)$
$3 = 2(1) + \boxed{(1)}$

$89 - 55(1) = (34)$
$55 - 34(1) = (21)$
$34 - 21(1) = (13)$
$21 - 13(1) = (8)$
$13 - 8(1) = (5)$
$8 - 5(1) = (3)$
$5 - 3(1) = (2)$
$3 - 2(1) = (1)$

$89s + 55t = \gcd(89, 55)$
$89s + 55t = 1$

$3 - 2 = (1)$
$3 - (5 - 3) = 1$
$3 - 5 + 3 = 1$
$2 \cdot 3 - 5 = 1$
$2 \cdot (8 - 5) - 5 = 1$
$2 \cdot 8 - 2 \cdot 5 - 5 = 1$
$2 \cdot 8 - 3 \cdot 5 = 1$
$2 \cdot 8 - 3 \cdot (13 - 8) = 1$
$2 \cdot 8 - 3 \cdot 13 + 3 \cdot 8 = 1$
$5 \cdot 8 - 3 \cdot 13 = 1$
$5 \cdot (21 - 13) - 3 \cdot 13 = 1$
$5 \cdot 21 - 5 \cdot 13 - 3 \cdot 13 = 1$
$5 \cdot 21 - 8 \cdot 13 = 1$
$5 \cdot 21 - 8 \cdot (34 - 21) = 1$
$5 \cdot 21 - 8 \cdot 34 + 8 \cdot 21 = 1$
$13 \cdot 21 - 8 \cdot 34 = 1$
$13 \cdot (55 - 34) - 8 \cdot 34 = 1$
$13 \cdot 55 - 13 \cdot 34 - 8 \cdot 34 = 1$
$13 \cdot 55 - 21 \cdot 34 = 1$
$13 \cdot 55 - 21 \cdot (89 - 55) = 1$
$13 \cdot 55 - 21 \cdot 89 + 21 \cdot 55 = 1$
$34 \cdot 55 - 21 \cdot 89 = 1$

$s = 21$
$t = 34$

(d) $a = 89, m = 232$

$\gcd(232, 89)$

$232 = 89(2) + (54)$
$89 = 54(1) + (35)$
$54 = 35(1) + (19)$
$35 = 19(1) + (16)$
$19 = 16(1) + (3)$
$16 = 3(5) + \boxed{(1)}$

$232 - 89(2) = (54)$
$89 - 54(1) = (35)$
$54 - 35(1) = (19)$
$35 - 19(1) = (16)$
$19 - 16(1) = (3)$
$16 - 3(5) = (1)$

$232s + 89t = 1$

$16 - 3(5) = 1$
$16 - 5(19 - 16) = 1$
$16 - 5 \cdot 19 + 5 \cdot 16 = 1$
$6 \cdot 16 - 5 \cdot 19 = 1$
$6 \cdot (35 - 19) - 5 \cdot 19 = 1$
$6 \cdot 35 - 6 \cdot 19 - 5 \cdot 19 = 1$
$6 \cdot 35 - 11 \cdot 19 = 1$
$6 \cdot 35 - 11 \cdot (54 - 35) = 1$
$6 \cdot 35 - 11 \cdot 54 + 11 \cdot 35 = 1$
$17 \cdot 35 - 11 \cdot 54 = 1$
$17 \cdot (89 - 54) - 11 \cdot 54 = 1$
$17 \cdot 89 - 17 \cdot 54 - 11 \cdot 54 = 1$
$17 \cdot 89 - 28 \cdot 54 = 1$
$17 \cdot 89 - 28 \cdot (232 - 89 \cdot 2) = 1$
$17 \cdot 89 - 28 \cdot 232 + 56 \cdot 89 = 1$
$73 \cdot 89 - 28 \cdot 232 = 1$

$s = 28$ $t = 73$

Week 8 HW – Cryptography
Theo Shin

#6

#6 p.284

(a) $a=2, m=17$

$\gcd(17,2)$

$17 = 2(8) + \boxed{1}$

$2 = 1(2) + 0$

$17 - 2(8) = 1$

$17s + 2t = 1$

$17 - 2(8) = 1$

$17 + 2(-8) = 1$

$s = 1$

$t = -8$ inverse => coefficient of a

(b) $a=34, m=89$

$\gcd(89,34)$

$89 = 34(2) + (21)$

$34 = 21(1) + (13)$

$21 = 13(1) + (8)$

$13 = 8(1) + (5)$

$8 = 5(1) + (3)$

$5 = 3(1) + (2)$

$3 = 2(1) + \boxed{(1)}$

$89 - 34(2) = (21)$

✓ $34 - 21(1) = (13)$

✓ $21 - 13(1) = (8)$

✓ $13 - 8(1) = (5)$

✓ $8 - 5(1) = (3)$

✓ $5 - 3(1) = (2)$

✓ $3 - 2(1) = (1)$

$89s + 34t = 1$

$3 - 2(1) = 1$

$3 - (5 - 3) = 1$

$3 - 5 + 3 = 1$

$2 \cdot 3 - 5 = 1$

$2 \cdot (8 - 5) - 5 = 1$

$2 \cdot 8 - 3 \cdot 5 = 1$

$2 \cdot 8 - 3 \cdot (13 - 8) = 1$

$5 \cdot 8 - 3 \cdot 13 = 1$

$5 \cdot (21 - 13) - 3 \cdot 13 = 1$

$5 \cdot 21 - 8 \cdot 13 = 1$

$5 \cdot 21 - 8 \cdot (34 - 21) = 1$

$13 \cdot 21 - 8 \cdot 34 = 1$

$13 \cdot (89 - 34(2)) - 8 \cdot 34$

$13 \cdot 89 - 26 \cdot 34 - 8 \cdot 34 = 1$

$13 \cdot 89 - 34 \cdot 34 = 1$

$13 \cdot 89 + (-34)34$

$s = 13$

$t = -34$

Week 8 HW – Cryptography
Theo Shin

(c) $a=144,\ m=233$

$\gcd(233,144)$

$233 = 144(1) + 89$
$144 = 89(1) + 55$
$89 = 55(1) + 34$
$55 = 34(1) + 21$
$34 = 21(1) + 13$
$21 = 13(1) + 8$
$13 = 8(1) + 5$
$8 = 5(1) + 3$
$5 = 3(1) + 2$
$3 = 2(1) + \boxed{1}$

$233 - 144(1) = 89$
$144 - 89(1) = 55$
$89 - 55 = 34$
$55 - 34 = 21$
$34 - 21 = 13$
$21 - 13 = 8$
$13 - 8 = 5$
$8 - 5 = 3$
$5 - 3 = 2$
$3 - 2 = 1$

$233s + 144t = 1$

$3 - 2 = 1$
$3 - (5 - 3) = 1$
$2\cdot 3 - 5 = 1$
$2\cdot(8 - 5) - 5 = 1$
$2\cdot 8 - 3\cdot 5 = 1$
$2\cdot 8 - 3\cdot(13 - 8) = 1$
$5\cdot 8 - 3\cdot 13 = 1$
$5\cdot(21 - 13) - 3\cdot 13 = 1$
$5\cdot 21 - 8\cdot 13 = 1$
$5\cdot 21 - 8\cdot(34 - 21) = 1$
$13\cdot 21 - 8\cdot 34 = 1$
$13\cdot(55 - 34) - 8\cdot 34 = 1$
$13\cdot 55 - 21\cdot 34 = 1$
$13\cdot 55 - 21\cdot(89 - 55) = 1$
$34\cdot 55 - 21\cdot 89 = 1$
$34\cdot(144 - 89) - 21\cdot 89 = 1$
$34\cdot 144 - 55\cdot 89 = 1$
$34\cdot 144 - 55(233 - 144) = 1$
$89\cdot 144 - 55\ 233 = 1$
$233(-5) + 144(89) = 1$

$s = -5$
$t = 89$

(d) $a=200,\ m=1001$

$\gcd(1001,200)$

$1001 = 200(5) + \boxed{1}$
$\cancel{200 = 1(200) + 0}$

$1001 - 200(5) = (1)$

$1001s + 200t = 1$
$1001s + 200(-5) = 1$
$s = 1$
$t = -5$

Week 8 HW – Cryptography
Theo Shin

2. Do #33 and #34 page 285

33. $7^{121} \bmod 13$

$$\boxed{a^{p-1} \equiv 1 \pmod{p}}$$

$$7^{12} \equiv 1 \pmod{13}$$

$$7^{121} \equiv 7^{(12\times10)+1}$$
$$\equiv (7^{12})^{10} \times 7^{1}$$
$$\equiv (1)^{10} \times 7$$

$$7 \equiv 7 \pmod{13}$$
$$= 7$$

34. $23^{1002} \bmod 41$

$$23^{40} \equiv 1 \pmod{41}$$

$$23^{40} \equiv 23^{(40\times25)+2}$$
$$\equiv (23^{40})^{25} \times 23^{2}$$
$$\equiv (1)^{25} \times 23^{2}$$
$$529 \equiv 37 \pmod{41}$$
$$\equiv 37$$

$$529 \equiv (41\cdot12)+37$$

3. Using the book's solution for extended Euclidean algorithm, I understood the pseudocode as initializing values and dividing 2 numbers together to compute the quotient and remainder through a loop sequence. By continuing this sequence, the remainders should successfully decrease until the lowest nonzero remainder will result, which is the gross common denominator. The pseudocode incorporates Bezout's theorem (r = ax + by) so that at every iteration not only is the remainder returned, but the coefficients for x and y (the pseudocode example uses varying variables). Essentially the pseudocode will compute the GCD and Bezout coefficients done by hand in our homework.

Week 8 HW – Cryptography
Theo Shin

Part C

1. Choose 2 very large primes $[p \times q = n]$
2. Calculate constant φ (Euler totient function) $\Rightarrow x^{\varphi} \bmod n = 1$

$\varphi = (p-1)(q-1)$ → must not share factor with e

3. Choose exponents e and d → small number, greater than 2

Encrypt $m^e \bmod n = c$
Decrypt $c^d \bmod n = m$
$(m^e \bmod n)^d \bmod n = m$

Example 8: STOP ⇒ key $(2537, 13)$

$2537 = 43 \cdot 59$ (p) (q)

$p = 43, q = 59, e = 13$
$n = 2537, d =$

$\varphi = (42)(58) = 2{,}436$

$e \cdot d \bmod \varphi = 1$

$13 \cdot d \bmod 2436 = 1$

4. Using Extended Euclidean algorithm

$d = 937$

$(13 \cdot 937) \bmod 2436 = 1$

private				public	
p	q	φ	d	n	e
43	59	2436	937	2537	13

Decryption $m = c^d \bmod n$

0981 0461

$0 = 0^{937} \bmod 2537$
$9 = 9^{937} \bmod 2537$
$8 = 8^{937} \bmod 2537$
$1 = 1^{937} \bmod 2537$

$0 = 0^{937} \bmod 2537$
$4 = 4^{937} \bmod 2537$
$6 = 6^{937} \bmod 2537$
$1 = 1^{937} \bmod 2537$