Name: Luong Thi Uy Thieu
Class: DMA-B05

HOMEWORK
DISCRETE MATHEMATICS
PROBLEM SET 05

Problem 1:

gcd(2n+1, 3n+2) = gcd(3n+2, (2n+1) mod (3n+2))

Take any n is a positive integer, n = 2 for instance

=> gcd(5,8) = gcd(8,5 mod 8)

= gcd(8, 5) = gcd(5,8 mod 5) =

gcd(5,3) = gcd (3,5mod3) =

gcd(3,2) = gcd (2,3mod2) =

gcd(2,1) = gcd(1,2mod1) =

gcd (1,1) = gcd (1,1mod1) = gcd(1,0)

=> Greatest common divisor or these two number with n is a positive integer is 1.

Problem 2:

+) Take any m is a positive integer: m = 2

And a,b,c are integers: a = 2, b = 4, c = 5, with c satisfied: gcd(c,m) = 1

We have: ac ≡ bc (mod m), then:

2.5 ≡ 4.5 mod 2 = 10 ≡ 20 mod 2 (always true)

Remove c from both sides of congruence :

2 ≡ 4 mod 2 (always true)

=> proved

+) example: a = 2, b = 8, c = 6, and m = 9

Then, gcd(c,m) = 3 ≠ 1

$ac \equiv bc \pmod{m} \Rightarrow 12 \equiv 48 \bmod 9$ (always true)

Take c from both sides:

=> $2 \not\equiv 8 \bmod 9$

=> proved

Problem 3:

a) $13x \equiv 1 \pmod{29}$

d = gcd(13,29) = 1, d|b => the congruence has one root.

d = n*s + a*r => find 1 = 29*s + 13*r

Euclidean algorithm

Dividend	Divisor	Quotient	Remainder
29	13	2	3
13	3	4	1
3	1	3	0

=> 1 = 13 - 3.4 = 13 + (-4).3 = 13 - 4.(29-13.2) = 9.13 - 4.29 = 29(-4)+ 13.9

// d = n.s + a.r

Xo = r*b/d (mod n/d) = 9*1/1 (mod 29/1) = 9

=> x = x0 + k.$\frac{n}{d}$ = 9 + k.$\frac{29}{1}$, k = 0 since the congruence only has one root

=> x = 9.

b) $384x \equiv 1038 \pmod{2418}$

d = gcd(a,n) = gcd (384, 2418)

Euclidean algorithm

Dividend	Divisor	Quotient	Remainder
2418	384	6	114
384	114	3	42
114	42	2	30
42	30	1	12
30	12	2	6
12	6	2	0

=> d = gcd(384,2418) = 6, d|b => 6 roots

d = n.s + a.r => find 6 = 2418.s + 384.r

=> 6 = 30 – 12.2 = (114 - 84) – 2.(42-30) = 2418 – 6.384 – 84 – 2.(384 - 342 – 114 + 84)

= 2418 – 6.384 - 2.384 + 2.342 + 2.114 - 2.84 - 84 = 2418 – 8.384 + 6.114 + 2.114 – 6.42

// 342.2 / 114 = 6

//-3.84 /42 = -6.

= 2418 – 8.384 + 8.114 – 6(384 – 3.114) = 2418 – 8.384 + 8.114 – 6.384 + 18.114

= 2418 – 14.384 + 26.114 = 2418 – 14.384 + 26(2418 – 6.384) = 2418.27 – 384.170

Xo = r*b/d (mod n/d) = (-170) * 1038/6 (mod 2418/6) = -29410 mod 403 = 9

x = x0 + k.$\frac{n}{d}$ = 9 + k.$\frac{2418}{6}$ with n ∈ (0,1,2,3,4,5)

=> x = {9,412,815,1218,1621,2024}

c) $372x \equiv 183 \pmod{579}$

d = gcd(372,579)

Euclidean Algorithm

Dividend	Divisor	Quotient	Remainder
579	372	1	207
372	207	1	165
207	165	1	42
165	42	3	39
42	39	1	3
39	3	13	0

=> d = gcd(372,579) = 3, d|b => 3 roots
d = n.s + a.r => find 3 = 579.s + 372.r

3 = 42 – 39 = 207 – 165 -165 + 42.3 = 207 – 2.165 + 42.3 = 207 – 2.(372 – 207) + 3.(207 – 165)
= -2.372 + 6.207 -3.165 = -2.372 + 6(579 – 372) – 3.(372 – 207) = 6.579 – 11.372 + 3.207
= 6.579 – 11.372 + 3. (579-372) = 579.9 – 372.14

Xo = r*b/d (mod n/d) = (-14). (183/3) (mod 579/3) = 111

x = x0 + k.$\frac{n}{d}$ = 111 + k.$\frac{579}{3}$ with k ∈ {0,1,2}
=> x ∈ {111,304,497}

Problem 4:

a) $134x \equiv 1 \pmod{467}$
d = gcd (134,467)

Euclidean Algorithm

Dividend	Devisor	Quotient	Remainder
467	134	3 (q1)	65
134	65	2 (q2)	4
65	4	16 (q3)	1

4	1	4	0

=> d = gcd(134,467) = 1, d|b then congruence has one root
d = n.s + a.r => find 1 = 467.s + 134.r

i	
0	R0 = 0
1	R1 = 1
2	R2 = r0 – q1 * r1 = 0 – 3 * 1 = -3 mod 467 = 464
3	R3 = r1 – q2 * r2 = 1 – 2 * 464 = - 927 mod 467 = 7
4	R4 = r2 – q3 * r3 = 464 – 16 * 7 = 352 mod 467

// r0 = 0, r1 = 1, R i = R i -2 – Q i – 1 * R i – 1
*small "I" because I don't know how to type that!
// r = last value of R i

Xo = r*b/d (mod n/d) = 352 *(1/1) (mod 467/1) = 352

x = x0 + k.$\frac{n}{d}$ = 352 + k.$\frac{467}{1}$ with k = 0 since the congruence only has 1 root

=> x = 352

b) 384x ≡ 1029 (mod 341)

We have, 384x ≡ 1029 (mod 341)
341x + 43x ≡ 6 (mod 341)
43x ≡ 6 (mod 341)
We have d = gcd(43,341)
Euclidean Algorithm

Dividend	Devisor	Quotient	Remainder
341	43	7 (q1)	40
43	40	1 (q2)	3

40	3	13 (q3)	1
3	1	3	0

=> d = gcd(43,341) = 1, d|b then congruence has 1 root

i	
0	R0 = 0
1	R1 = 1
2	R2 = r0 – q1 * r1 = 0 – 7 * 1 = -7 mod 341 = 334
3	R3 = r1 – q 2 * r2 = 1 – 1 * 334 = -333 mod 341 = 8
4	R4 = r 2 – q3 * r3 = 334 – 13 * 8 = 230 mod 341

// r0 = 0, r1 = 1, R i = R i -2 – Q i – 1 * R i – 1
*small "I" because I don't know how to type that!
// r = last value of R i

Xo = r*b/d (mod n/d) = 230 * (6/1) = 1380
X = x1 + k.$\frac{n}{d}$ = 1380 + k.$\frac{341}{1}$ with k = 0 since the congruence only has 1 root
=> x = 1380.

Problem 5:

a) CEBBOXNOB XYG

Converted into numbers:

2 - 4 - 1 – 1 - 14 – 23 – 13 - 14 – 1 23 – 24 – 6

Apply decryption: $f^{-1}(p)$= (p - 10) mod 26.

=> new numbers: 18 – 20 – 17 – 17 – 4 – 13 – 3 – 4 – 17 13 – 14 – 22

Message: Surrender now

b) LO WI PBSOXN

numbers: 11-14   22 – 8   15 – 1 – 18 – 14 – 23 – 13

Apply decryption: $f^{-1}(p) = (p - 10)\ mod\ 26$

=> numbers: 1-4 12-24 5-17-8-4-13-3

Message: Be My Friend

c) DSWO PYB PEX

numbers: 3-18-22-14   15-24-1   15-4-23

Apply decryption: $f^{-1}(p) = (p - 10)\ mod\ 26$

=> numbers: 19-8-12-4   5-4-17   5-20-13

=> message: time for fun

Problem 6:

Read chapter 4.2, Textbook, summarize the method (section 4.2.4 page 267) and show your own example.

To be able to find $b^n\ mod\ m$ efficiently, where b, n and m are large integers, we can use an algorithm that employs the binary expansion of the exponent n:

- We explain how to use the binary expansion of n, say n = $(a_{k-1} \dots a_1 a_0)_2$, to compute b^n

  Note that:

  $$b^n = b^{a_{k-1}\cdot 2^{k-1}+\cdots+a_1\cdot 2+a_0} = b^{a_{k-1}\cdot 2^{k-1}} \cdots b^{a_1\cdot 2} \cdot b^{a_0}.$$

  => + To compute b^n, we need only compute the values of b, $b^2,\ (b^2)^2 = b^4$, $(b^4)^2 = b^8, \dots, b^{2^k}$

  + When we have these values, multiply the term b^{2^j} in the list, where $a_j = 1$.
  + This gives us b^n

  => The algorithm successively finds b mod m, b^2 mod m, b^4 mod m, … , $b^{2^{k-1}}$ mod m and multiplies together those terms b^{2^j} mod m where $a_j = 1$, finding the remainder of the product when divided by m after each multiplication.

Ex: 5^{117}mod 19

Step 1: Divide B into powers of 2 by writing it in binary: 117 = 1110101

Start at the rightmost digit, let k=0 and for each digit:

- If the digit is 1, we need a part for 2^k, otherwise we do not
- Add 1 to k, and move left to the next digit

  117 = $(2^0 + 2^2 + 2^4 + 2^5 + 2^6)$

  117 = 1 + 4 + 16 + 32 + 64

  $5^{117} mod\ 19 = 5^{1+4+16+32+64}$mod 19

$$5^{117} mod\ 19 = (5^1 * 5^4 * 5^{16} * 5^{32} * 5^{64}) mod\ 19$$

Step 2: Calculate mod C of the powers of two ≤ B

5^**1** mod 19 = **5**

5^**2** mod 19 = (**5^1 * 5^1**) mod 19 = (**5^1 mod 19** * **5^1 mod 19**) mod 19
5^**2 mod 19** = (**5 * 5**) mod 19 = **25** mod 19
5^2 mod 19 = 6

5^**4** mod 19 = (**5^2 * 5^2**) mod 19 = (**5^2 mod 19 * 5^2 mod 19**) mod 19
5^**4** mod 19 = (**6 * 6**) mod 19 = **36** mod 19
5^4 mod 19 = 17

5^**8** mod 19 = (**5^4 * 5^4**) mod 19 = (**5^4 mod 19 * 5^4 mod 19**) mod 19
5^**8** mod 19 = (**17 * 17**) mod 19 = **289** mod 19
5^8 mod 19 = 4

5^**16** mod 19 = (**5^8 * 5^8**) mod 19 = (**5^8 mod 19 * 5^8 mod 19**) mod 19
5^**16** mod 19 = (**4 * 4**) mod 19 = **16** mod 19
5^16 mod 19 = 16

5^**32** mod 19 = (**5^16 * 5^16**) mod 19 = (**5^16 mod 19 * 5^16 mod 19**) mod 19
5^**32** mod 19 = (**16 * 16**) mod 19 = **256** mod 19
5^32 mod 19 = 9

5^**64** mod 19 = (**5^32 * 5^32**) mod 19 = (**5^32 mod 19 * 5^32 mod 19**) mod 19
5^**64** mod 19 = (**9 * 9**) mod 19 = **81** mod 19
5^64 mod 19 = 5

Step 3: Use modular multiplication properties to combine the calculated mod C values

5^117 mod 19 = (**5^1 * 5^4 * 5^16 * 5^32 * 5^64**) mod 19
5^117 mod 19 = (**5^1 mod 19 * 5^4 mod 19 * 5^16 mod 19 * 5^32 mod 19 * 5^64 mod 19**) mod 19
5^117 mod 19 = (**5 * 17 * 16 * 9 * 5**) mod 19
5^117 mod 19 = **61200** mod 19 = **1**
5^117 mod 19 = 1

Problem 7:

Encrypt the message UPLOAD using the RSA system with n = 53 · 61 and e = 17.

We have: n = 53 .61 => **p= 53, q= 61**

Compute z = (p-1).(q-1) = (53-1).(61-1)= 3120; 1 < **e = 17** < **z = 3120**, gcd(e,z) = gcd(17,3120) = 1 => satisfy

+ Public key: (n,e) = (53.61, 17)

Compute d as multiplicative inverse of e modulo z: e (mod z) = 17 (mod 3120)

// y is called the multiplicative inverse of x mod m if xy ≡ 1 (mod m)

=> 17.d ≡ 1 (mod 3120)

gcd (17,3120)

Dividend	Devisor	Quotient	Remainder
3120	17	183	9
17	9	1	8
9	8	1	1
8	1	8	0

=> d = gcd(17,3120) = 1 => d|b => congruence has 1 root
d = n*s + a*r = > find 1 = 3120*s + 17*r

1 = 9 – 8 = 3120 – 17.183 – 17 + 9 = 3120 – 17.183 – 17 + 3120 – 17.183 = 2.3120 – 367.17

d =Xo = r*b/d (mod n/d) = (-367).(1/1) mod (3120) = -367 mod 3120 = 2753

=> **d = 2753**

+ Private key (n,d) = (53.61,2753)

*** encrypt:**

UPLOAD => Mu=20 Mp=15 Ml=12 Mo=14 Ma=0 Md=3 e = 17, n = 53.61

*M is the position of (i)letter in alphabet

Apply the formula: c = $m^e mod\ n$

=> c = (20^{17} 15^{17} 12^{17} 14^{17} 0^{17} 3^{17}) (mod 53.61)

Problem 8: What is the original message encrypted using the RSA system with n = 43 · 59 and e = 13 if the encrypted message is 0667 1947 0671?

n = 43.59 = 2537

e = 13

z = (p-1).(q-1) = 2436

// y is called the multiplicative inverse of x mod m if xy ≡ 1 (mod m)

d is a multiplicative inverse of e modulo z: 13.d ≡ 1 mod 2436

Dividend	Divisor	Quotient	Remainder
2436	13	187	5
13	5	2	3
5	3	1	2
3	2	1	1
2	1	2	0

=> gcd(13,2436) = 1, d|b so the congruence has 1 root

d = n.s + a.r => 2436.s + 13.r => find 1 = 2436.s + 13.r

1 = 3 – 2 = 13 – 10 – 5 + 3 = 13 – 15 + 13 – 10 = 2.13 – 25 = 2.13 – 5.5 = 2.13 – 5.(2436 – 13.187)

= 2.13 – 5.2436 + 935.13 = -5.2436 + 937.13

d = Xo = r*b/d (mod n/d) = 937*(1/1) mod (2436/1) = 937

public key (n,e) = (2537,13)

private key (n,d) = (2537,937)

***Decrypt**

m = $c^d \ mod \ n$

Decrypt each block: m1 = $0667^{937} \ mod \ 2537 = 1808$

m2 = $1947^{937} \ mod \ 2537 = 1121$

m3 = $0671^{937} \ mod \ 2537 = 0417$

=> the decrypted numbers: 1808 1121 0417

=> SILVER