# Cryptography : The Survival Kit



**Few words about the exam :**

- **Calculator are allowed**
- **First test will be on 17 November**
- **Notes aren't allowed**

- **2 hours, 10 questions**

## Theorems

List of all theorems seen during lessons. During exercises, we will see which theorems are the most important. Please, color them as follows :

- Unknown yet
- Not important
- Quite important
- Very important

[If you find theorem names, please put them...]

- Theorem of uniqueness of division (#1)

$IF\ \ a, b \in Z\ and\ |b| \neq 0$

$THEN\ there\ is\ a\ unique\ g \in Z\ and\ unique\ 0 \leq r\ \ \leq |b|;\ r \in Z\ that\ \ :$

$$a = gb + r$$

- Theorem (#2)

$IF\ \ a, b, c, d\ \ \in Z\ and\ n \in N,\ \ n \geq 2\ AND\ a \equiv b\ (mod\ n),\ \ c \equiv d\ (mod\ n)$

$THEN\ \ a + c \equiv b + d\ (mod\ n)\ AND\ a.c\ \ \equiv b.d\ (mod\ n)$

- Theorem "of the definition of inverse" (#3)

$IF\ \ a \in Zn\ has\ an\ inverse\ and\ there\ is\ b \in Zn\ that\ \ :$

$$a \otimes_n b\ \ =\ \ b \otimes_n a\ \ =\ \ 1$$
$THEN\ \ we\ say\ that\ b\ is\ an\ inverse\ of\ a\ and\ we\ write\ b = a^{-1}$

- Theorem (#4)

$IF\ \ (Zn, \oplus\ n,\ \ \otimes\ n)\ n \in N,\ \ n \geq 2$

$THEN\ \ a \in Zn\ has\ an\ inverse$

$IFF\ \ GCD(a, n)\ \ =\ \ 1$

- Euler's Function

$\varphi(n)\ \ =\ \ number\ of\ element\ that\ verify\ GCD(k, n) = 1\ (where\ k \in\ \ < 0, n - 1 >)$

Properties :

  - $\varphi(p)\ \ =\ \ p - 1\ (where\ p\ is\ a\ prime)$
  - $\varphi(p^k)\ \ =\ \ (p - 1) * p^{k-1}\ (where\ p\ is\ a\ prime)$

- Theorem (#5)

$IF\ \ a, b \in N\ and\ GCD(a, b) = 1\ (aka\ number\ are\ relatively\ prime)$

$THEN\ \ \varphi(a * b) = \varphi(a) * \varphi(b)$

- Theorem (#6)

$IF\ n \in N,\ n \geq 2,\ then\ there\ are\ unique\ primes\ p1 \leq p2\ \leq ...\ \leq\ pr\ and\ unique\ k1, k2, ..., kr \in N\ U\ \{0\}$

$THAT\ n = p1^{k1} * p2^{k2} * ... * pr^{kr}\ (It's\ called\ the\ factorisation\ of\ n)$

$For\ n\ we\ have\ :\ \varphi(n) = (p1 - 1) * p1^{k-1} * (p2 - 1) * p2^{k2-1} ... (pr - 1) * pr^{kr-1}$

- The Euler's theorem (#7)

$IF\ a \in Z;\ n \in N,\ n \geq 2\ , GCD(a, n) = 1$

$THEN\ a^{\varphi(n)} \equiv 1(mod\ n)\ (aka\ :\ a^{\varphi(n)}(mod\ n) = 1)$

- Fermat's theorem (#8)

$IF\ a \in N;\ p\ is\ a\ prime\ (so\ GCD(a, p) = 1)$

$THEN\ a^{p-1} \equiv 1(mod\ p)$

$(OR\ a^{p-1} - 1 \equiv 0(mod\ p))$

- Fact (#1)

$IF\ a \in Z;\ n, k \in Z; n\ \geq 2;\ GCD(a, n) = 1$

$$THEN\ a^k \equiv a^{k(mod\ \varphi(n))}\ (mod\ n)$$

- Chinese Remainder Theorem (CRT) (#9)

$IF\ m1, m2, ..., mr \in N\ \geq 2\ AND\ for\ every\ i\ \neq j\ < 1, r >,\ GCD(mi, mj) = 1\ (aka\ they\ are\ all\ relatively\ prin$

$THEN\ for\ every\ a1, a2, ...,\ ar \in Z\ a\ set\ of\ congruencies\ :$

$X \equiv a1\ (mod\ m1)$

$X \equiv a2\ (mod\ m2)$

…

$X \equiv ar\ (mod\ mr)$

$has\ exactly\ one\ solution\ X0\ in\ a\ set\ < 0, M - 1 >\ (where\ M\ =\ m1, m2, ..., mr)$

$and\ there\ are\ constants\ c1, c2, ..., cr \in Z\ and\ X0\ = (c1a1 + c2a2 + ... + crar)\ (mod\ n)$

$and\ all\ solutions\ of\ the\ set\ of\ congruencies\ are\ given\ by\ the\ formula\ :$

$Xk\ =\ X0 + k * M;\ k \in Z$

See handy links section to see how to apply it.

- Theorem (#10)

$IF\ m1, m2, ..., mr \in N,\ mi\ \geq 2,\ AND\ m1, m2, ..., mr\ are\ relatively\ prime$

$THEN$

$a \equiv b\ (mod\ m1)$

$a \equiv b\ (mod\ m2)$

...

$a \equiv b\ (mod\ mr)$

$IFF\ a \equiv b\ (mod\ m1, m2, ..., mr)$

- Theorem (#11)

$IF\ a \in Z\ then\ a^{-1}(inverse)\ exists\ IFF\ GCD(a, n) = 1$

- Definition of an inverse

$a^{\varphi(n)-1}(mod\ n)\ =\ a^{-1}$

$a^{\varphi(n)-1}\ \equiv\ a^{-1}(mod\ n)$

$a^{\varphi(n)} \equiv 1(mod\ n)$

- Theorem (#12)

$IF\ a, b \in Z\ then\ there\ are\ x, y \in Z\ such\ as\ :$

$xa + yb\ =\ GCD(a, b)$

$(Below\ we\ take\ b = n)$

$xa + yn\ =\ GCD(a, n) = 1$

$xa + yn\ = 1$

$xa\ (mod\ n) = 1$

$xa\ (mod\ n) \otimes_n a\ = 1$

$xa\ (mod\ n)\ = a^{-1}$

$a\ \varepsilon\ G\ ;\ a^{\#G} = 1; a^{\#G-1} = a^{-1}$

- Lagrange's theorem (group theory) (#13)

$IF\ G\ is\ a\ finite\ group\ and\ H\ is\ a\ subgroup\ of\ G$

$THEN\ \#H\ /\ \#G$

This means that the number of element of H divide the number of element of G.

- Theorem (#14)

$For\ every\ element\ a\ of\ a\ finite\ group\ (Gi)\ that\ have\ :\ a^{\#G} = 1$

$THEN\ :\ a^{\#G} * a^{-1} = a^{-1}\ AND\ a^{\#G-1} = a^{-1}$

- Also need to know…
    - Group theory
    - Galois Group
    - Cyclic Group
    - Discrete logarithm
    - RSA cipher
    - ...

- [Complete me]

# Handy links

- Handbook of Applied Cryptography (Course's book reference)

http://cacr.uwaterloo.ca/hac/

- The Chinese Remainder Theorem (CRT) explained (EZ mode) :

https://www.youtube.com/watch?v=ru7mWZJlRQg&feature=youtu.be

- Finite fields explained

https://www.youtube.com/watch?v=z9bTzjy4SCg

- First 1000 prime numbers

https://primes.utm.edu/lists/small/1000.txt

- Euler function online (good to verify results)

http://www.javascripter.net/math/calculators/eulertotientfunction.htm

- Calcul inverse of a number online

https://planetcalc.com/3311/

- Wolfram Alpha

https://www.wolframalpha.com

- [Complete me]

# Problems for midterm

Here we gather all solutions for exercise in pdf : “ECRYP PROBLEMS FOR MIDTERM TEST #1.pdf” which you can find in courses materials.

## Problem template

Just copy paste it so we get the same format every time...

### Problem #n

[The problem text]

**Things used to solve it**

- Theorem #n
- …

**Approach**

Lorem ipsum dolor sit amet, consectetur adipiscing elit.

**Results**

To avoid spoil, please put background in black for the result as follows : This is an answer. (Just select the text to see it). If you can, put some intermediate calculation in your answer...

- [Your name], [Another name which found the same result] : The answer is 42
- [Name from a guy who find an other response] : No, it’s 41

**Questions**

- Here we can question ourselves about the answer of life and stuff...
  - Here is the response (which is obviously 42)

# Test 1

## Shit just got real

### Problem #1

Alice and Bob use a binary Vernam's cryptosystem with a secret key k = k1,k2...kr where k € {0,1} . Assume we know a plain text message M = m1,m2...mr, where m € {0,1} and a corresponding cryptogram C = c1,c2...cr c € {0,1} . Compute the secret key k1,k2...kr from M and C.

**Things used to solve it**

- Wikipedia
- Good to know that, A xor A = 0 and A xor 0 = A

**Approach**

Definition of Vernam cipher is as follows :
Plaintext ⊕ Key = Ciphertext
Ciphertext ⊕ Key = Plaintext
Where ⊕ is a XOR.
(Thanks Wikipedia)

**Results**

- Anthony : Solve C ⊕ K? = M, you can alway guess ki with ci and mi (ex : if ci=1 and mi=0,then ki=1 etc…) (Andreas's answer is better explained…)
- Andreas : C ⊕ K? = M,
  - C ⊕ C ⊕ K = C ⊕ M
  - 0 ⊕ K = C ⊕ M
  - K = C ⊕ M

**Questions**

- -

Problem #2

Compute inverses of 7, 8, 9
a) in the multiplicative group Z*11
b) in the multiplicative group Z*13.

**Things used to solve it**

- Definition of an inverse
- Theorem (#11)

**Approach**

You can use the theorem 11 to prove that an inverse exists for your number.
Then just compute it with the definition of an inverse.

**Results**

- a) Anthony, Andreas:
    - 11 is prime so $\varphi(11) = 10$
    - $Inv(7) = 7^{\varphi(11)-1}(mod\ 11) = 7^9\ (mod\ 11) = 8$
    - $Inv(8) = 8^{\varphi(11)-1}(mod\ 11) = 8^9\ (mod\ 11) = 7$
    - $Inv(9) = 9^{\varphi(11)-1}(mod\ 11) = 9^9\ (mod\ 11) = 5$
- b) Anthony, Andreas :
    - $Inv(7) = 2$
    - $Inv(8) = 5$
    - $Inv(9) = 3$

**Questions**

- -

## Problem #3

Compute inverses of 4, 5, 6
a) in the multiplicative group Z*13
b) in the multiplicative group Z*15
c) List all elements of Z*13 and Z*15

**Things used to solve it**

- Definition of an inverse
- Theorem (#11)

**Approach**

You can use the theorem 11 to prove that an inverse exists for your number.
Then just compute it with the definition of an inverse.

**Results**

- a) Anthony, Andreas:
  - 13 is prime so $\varphi(13) = 12$
  - $Inv(4) = 4^{\varphi(13)-1}(mod\ 13) = 4^{11}\ (mod\ 13) = 10$
  - $Inv(5) = 5^{\varphi(13)-1}(mod\ 13) = 5^{11}\ (mod\ 13) = 8$
  - $Inv(6) = 6^{\varphi(13)-1}(mod\ 13) = 6^{11}\ (mod\ 13) = 11$
- b) Anthony, Andreas:
  - !! 15 is not a prime !!
  - $Inv(4) = 4$
  - $GCD(15, 5)! = 1,\ can't\ compute$
  - $GCD(15, 6)! = 1,\ can't\ compute$
- c) Anthony :
  - Z*13={1,2,..,12}
  - Z*15={1,2,..,14}

**Questions**

- - Doesn't Z*15 only contains the invertible elements of Z15? So the answer on c should be : Z*13={1,2,..,12} and Z*15={1,2,4,7,8,11,13}?
  - Don't know man, for me it's just : Z*15 = Z15\{0}
  - Kutay: http://mathworld.wolfram.com/ModuloMultiplicationGroup.html -SOLVED-

Problem #4

Compute all generators

1) of the multiplicative group Z*17

2) of the multiplicative group Z*13.

**Things used to solve it**

- Definition of generator
- Example of lesson

**Approach**

https://docs.google.com/spreadsheets/d/1Dkf5PV9tiAxwasQYSA-Ad-zTp66ksoUGzsZHR5FgOEE/edit#gid=0

Detail example for Z*17

**Results**

- 1) Anthony,Andreas : 3,10,5,11,14,7,12,6
- 2) Anthony : 2,6,7,11

**Questions**

- -

## Problem #5

Compute log5(8) in the multiplicative group Z*13 and in the the multiplicative group Z*19 .

**Things used to solve it**

- Logarithmic definition in lesson

**Approach**

$log_5(8) = ? == 5^? mod\ n = 8$ (With n, number of Z*n)

Brute force seems to be the only way...

**Results**

- Z*13 Anthony,Andreas : 3
- Hannah : Z*13: 3,7,11? There is a loop,from 5^1(mod 13) to 5^4(mod 13).
  The same with 5^x(mod 19),x from 1 to 9,so there isn't x,making
  5^x (mod 19) = 8
- Z*19 Anthony : No solution ?
- Kutay & Miguel : As Hannah said there is one loop for each group,so final answer would be:
  For Group Z13 ⇒ X=3+4n , n=0,1,2,3,4……………
  For Group Z19 ⇒ X doesn't exist. Because there is no 8 in the loop.(5,6,11,17,9,7,16,4,1,5,6…..)

**Questions**

- -

## Problem #6

Give an example proving that the assumption in RSA definition: „n is a square-free number” is important

**Things used to solve it**

- RSA cipher system

**Approach**

lulz

**Results**

- Anthony if “n” is NOT a square free number, then
- $\sqrt{n} = p = q$ So we can calculate $\varphi(n) = (p - 1)(q - 1)$ and get “d” (the private key) by calculate the inverse of “e” (the public key) modulo $\varphi(n)$.

**Questions**

- -

## Problem #7

Assume we have a RSA cryptosystem with n=p*q (where p and q are secret different primes) and e is a public key. Prove that factorization of n breaks the RSA cryptosystem.

**Things used to solve it**

- RSA cipher system
- Theorem #6

**Approach**

lulz

**Results**

- Anthony : If "n" can be factorize, we can easly get $\varphi(n)$ (see theorem #6) and then get "d" (the private key) by calculate the inverse of "e" (the public key) modulo $\varphi(n)$.

**Questions**

- -

Problem #8

Assume we deal with the RSA cipher with n=p*q and RSA has two different public keys e1 and e2 which are relatively prime (GCD(e1,e2)=1). Prove that if we have two cryptogrammes c1 and c2 of the unknown plain text message m (in Zn).

c1 (cryptogramme obtained with e1 ) and

c2 (cryptogramme obtained with e2 )

then we can easily compute the plain text message m (in Zn) from c1 and c2.

**Things used to solve it**

- RSA cipher system
- Theorem #2
- Theorem #12

**Approach**

lulz

**Results**

- Anthony (copied from Andreas) :
  - We know that : GCD(e1,e2)=1 so based on theorem #12 : $e1 * a + e2 * b = 1$
  - By definition of the RSA system : $c1 \equiv m^{e1} (mod\ n)$ ; $c2 \equiv m^{e2} (mod\ n)$
  - So : $c1^a \equiv (m^{e1})^a (mod\ n)$ ; $c2^b \equiv (m^{e2})^b (mod\ n)$
  - With theorem #2 we can write :
  - $c1^a * c2^b \equiv (m^{e1})^a * (m^{e2})^b (mod\ n)$
  - $c1^a * c2^b \equiv (m^{e1*a+e2*b})\ (mod\ n)$
  - With the first point we can write :
  - $c1^a * c2^b \equiv m\ (mod\ n)$
  - We then need to calculate a and b, we can do that using the Euler Ext. Algorithm.
  - (Thanks Andreas !)

**Questions**

- -

## Problem #9

Add the following polynomials (bytes) in the quotient ring : Z2[x]/(x^8+x^4+x^3+x+1)=GF(2^8)
a) ‘57’+’02’
b) ‘03’+’03’
c) ‘FF’+’0F’

**Things used to solve it**

- Xor

**Approach**

Take those number as binary number and xor them (Addition in Z2 is equal to xoring).

**Results**

- a) Anthony : 0x55 (with hex notation), 59 (with decimal notation)
- b) Anthony : 0x00
- c) Anthony : 0xF0

**Questions**

- - Miguel&Kutay: We are not sure if the decimal notation is okay on question A. Shouldn`t it be ‘55’ = 85?

## Problem #10

Multiply the following polynomials (bytes) in the quotient ring : Z2[x]/(x^8+x^4+x^3+x+1)=GF(2^8)
a)‘57’*’02’
b) ‘57’*’04’
c) ‘57’*’10’

**Things used to solve it**

- Binary modulo or polynomial division

**Approach**

Take those numbers as binary number and convert them in polynomial (e.g : 0x57 = 0b01010111 = x^6+x^4+x^2+x+1) then multiply them. If the result is more (or equal) than the polynomial x^8+x^4+x^3+x+1 (so : 0b100011011) then do a modulo (in binary) or calcul the rest by doing a polynomial division. (by this polynomial)

**Questions**

**Results**

- a) Anthony : 0xAE
- b) Anthony : 0x47
- c) Anthony : 0x7
- -

## Problem #11

Solve the following set of 4 congruencies :

x ≡ 3 (mod 7)
x ≡ 3 (mod 5)
x ≡ 3 (mod 11)
x ≡ 3 (mod 13)

**Things used to solve it**

- Theorem #9 (CRT)
- or just some basic logic...

**Approach**

CRT : 5,7,11,13 are all prime (aka gcd between them is 1), we can apply CRT.
Logic : Mhhh, theses numbers looks similar...

**Results**

- hannah : 5008 is the smallest one.lcg=5*7*11*13=5005 then 5005 +3 = 5008
- Anthony : 10013(mod 5005)=3 with CRT (Which is obvious with some logic…)

**Questions**

- -

## Problem #12

Solve the following set of 4 congruencies :

$x \equiv 4 \pmod{5}$
$x \equiv 6 \pmod{7}$
$x \equiv 10 \pmod{11}$
$x \equiv 12 \pmod{13}$

**Things used to solve it**

- Theorem #9 (CRT)

**Approach**

CRT : 5,7,11,13 are all prime (aka gcd between them is 1), we can apply CRT.

**Results**

- Anthony : 15014(mod 5005) = 5004

**Questions**

- -

### Problem #13

Solve the following set of 5 congruencies :

x ≡ 5 (mod 7)
x ≡ 3 (mod 5)
x ≡ 9 (mod 11)
x ≡ 11 (mod 13)
x ≡ 15 (mod 17)

**Things used to solve it**

- Theorem #9 (CRT)

**Approach**

CRT : 5,7,11,13,17 are all prime (aka gcd between them is 1), we can apply CRT.

**Results**

- hannah : 85083
- Anthony : 12155*4+17017*4+7735*10+6545*4+5005*4=240238

**Questions**

- -

## Problem #14

Solve the following set of 3 congruencies :

x ≡ 1 (mod 7)
x ≡ 2 (mod 5)
x ≡ 3 (mod 11)

**Things used to solve it**

- Theorem #9 (CRT)

**Approach**

CRT : 5,7,11,13
,17 are all prime (aka gcd between them is 1), we can apply CRT.

**Results**

- hannah : 267
- Anthony : 55*6+77+35*18=1037

**Questions**

- -

## Problem #15

Solve the following set of congruencies :

$x \equiv 3 \pmod 7$
$x \equiv 9 \pmod{13}$
$x \equiv 1 \pmod 5$
$x \equiv 7 \pmod{11}$

**Things used to solve it**

- Theorem #9 (CRT)

**Approach**

CRT : 5,7,11,13,17 are all prime (aka gcd between them is 1), we can apply CRT.

**Results**

- hannah : 5001+5005k (k=0,1,2,......)
- Anthony : 715*3+385*6+1001+455*10=10006

**Questions**

- -

### Problem #16

Solve the following set of congruencies :

x ≡ 3 (mod 7)
x ≡ 3 (mod 5)
x ≡ 7 (mod 11)
x ≡ 7 (mod 13)

**Things used to solve it**

- Theorem #9 (CRT)

**Approach**

CRT : 5,7,11,13,17 are all prime (aka gcd between them is 1), we can apply CRT.

**Results**

- Anthony : 715*3+1001*3+455*3*7+385*5*7=28178

**Questions**

- -

## Problem #17

Compute values of the Euler phi function :

a) $\varphi(3458)$
b) $\varphi(3459)$
c) $\varphi(5357)$
d) $\varphi(5358)$
e) $\varphi(2^{1000})$
f) $\varphi(10^{1000})$

**Things used to solve it**

- Theorem #5
- Theorem #6
- Euler function properties

**Approach**

Make your number and primes numbers play together and hope something happen...

**Results**

- Anthony
  - a)
    - $3458 = 19^1 * 13^1 * 7^1 * 2^1$
    - $\varphi(3458) = 1 * 2^0 * 6 * 7^0 * 12 * 13^0 * 18 * 19^0 = 1296$
  - b)
    - $\varphi(3459) = \varphi(1153 * 3) = \varphi(1153) * \varphi(3) = 1152 * 2 = 2304$
    - 1153 (and 3) is prime
  - c)
    - $\varphi(5357) = \varphi(487 * 11)$ – $487$ *and* $11$ *are prime*
    - $= \varphi(487) * \varphi(11)$
    - $= 486 * 10$
    - $= 4860$
  - d)
    - $\varphi(5358) = \varphi(2 * 3 * 19 * 47) = 1 * 2 * 18 * 46 = 1656$
    - 2,3,19 and 47 are primes
  - e)
    - $\varphi(2^{1000}) = 1 * 2^{999}$ – $2$ *is prime*
  - f)
    - $\varphi(10^{10}) = \varphi(2^{10} * 5^{10}) = \varphi(2^{10}) * \varphi(5^{10})$ – $2$ *and* $5$ *are prime*
    - $= 2^9 * 4 * 5^9 = 2^{11} * 5^9$

**Questions**

- -

## Problem #18

Compute values of the Euler phi function :

a) $\varphi(\varphi(5358))$
b) $\varphi(\varphi(3458))$
c) $\varphi(\varphi(2^{1000}))$

**Things used to solve it**

- Theorem #5
- Theorem #6
- Euler function properties
- Problem #17

**Approach**

Make your number and primes numbers play together and hope something happen...

**Results**

- Anthony
  - a)
    - $\varphi(\varphi(5358)) = \varphi(1656)\ -\ See\ Problem\ 17$
    - $\varphi(1656) = \varphi(2^3 * 3^2 * 23) = (1 * 2^2 * 2 * 3^1 * 22) = 528$
  - b)
    - $\varphi(3458) = 1296\ -\ see\ problem\ 17$
    - $\varphi(1296) = \varphi(3^4 * 2^4) = \varphi(2 * 3^3 * 1 * 2^3) = 432$
  - c)
    - $\varphi(2^{1000})\ = 1 * 2^{999} - 2\ is\ prime$
    - $\varphi(2^{999}) = 2^{998}$

**Questions**

- -

Problem #19

Assume a,n e N and n>=2. Prove that if GCD(a,n)= 1 then

$a^{m\ (mod\ \varphi(n))} \equiv a^{m}\ (mod\ n)$

where $\varphi$ is the Euler function.

**Things used to solve it**

- Euler's Theorem

**Approach**

.

**Results**

- Anthony (copied from Andreas…) :
    - $a^{m} = a^{r*\varphi(n)+m\ (mod\ \varphi(n))} = a^{\varphi(n)^{r}} * a^{m\ (mod\ \varphi(n))}$
    - So $a^{m}\ (mod\ n) = (a^{\varphi(n)}\ \ (mod\ n))^{r} * a^{m\ (mod\ \varphi(n))}$
    - Euler theorem say that $(a^{\varphi(n)}\ \ (mod\ n)) \equiv 1$ so we got :
    - $a^{m}\ (mod\ n) = a^{m(mod\ \varphi(n))} mod\ (n)$

**Questions**

- -

Problem #20

Prove that the polynomial x^2+1 is irreducible in the ring Z3[x] and describe the field GF(9) (aka $F_9$)

**Things used to solve it**

- Look at example of in the lesson

**Approach**

A polynomial is irreducible if we can’t factorize it.
Still have no idea how to prove that...

**Results**

- Hannah : suppose x^2 +1 is reducible,then x^2 + 1 =(ax + b)(cx + d),where a,b,c,d take the values 0,1 or 2.So x^2 +1 = acx^2 + (bc + ad)x + bd,and ac = 1, bc+ad =0,bd=1,so bcad=-a^2c^2=1,from with 1 = -a^2*c^2,which is impossible.So it is irreducible.
- Anthony : GF(9)=GF( $3^2$ ) So elements are :
    - 0+0x;1+0x; 2+0x;0+1x;1+1x; 2+1x;0+2x;1+2x;2+2x = 9 elements

**Questions**

- If someone found out who to prove the irreducibility of a polynomial...

Problem #21

Assume GF(2^k)[x] where ( k is a fixed natural number ) is a ring of polynomials with coefficients in the field GF(2^k)[x] . Prove that for every polynomial x^n (where n e N ) from GF(2^k)[x] we have :
$x^n(mod(x^4+1)) = x^{n(mod\ 4)}$

**Things used to solve it**

- ?

**Approach**

Apparently this guy solve it… still didn't understand tho :
https://math.stackexchange.com/questions/738655/prove-xi-mod-x4-1-xi-mod-4-in-gf2x

**Results**

-

**Questions**

-

Problem #22 / 30 / 31

Design an ELGamal cryptosystem for the field F(19) .
(Problem 30 is very similar : Describe the ElGamal public key cipher and design an example of the cipher “for small numbers” with an example of ciphering.)
(Problem 31 is the same…)

**Things used to solve it**

- Knowing how ElGamal cipher works

**Approach**

Find the elements of F(19) and one of the generator.
Make an example (take ElGamal cipher’s formulas and replace them with arbitrary inputs) to show that it works.

**Results**

- Anthony :
  - 19 is prime so elements of F(19) are : Z*(19).
  - 2 is a generator ( $\forall i \in F(19),\ 2^i mod\ 19 = F(19)$ )
  - Now we take input :
  - g = 3 ; a = 8 so b= $3^8 = 6$ ; k=7 ; inv(k) = 11 ; m=10
  - $c = m * b^k = 10 * 9 = 14$
  - $m = c * g^{-ka} = 14 * 17 = 10$
  - It works !

**Questions**

-

## Problem #23

Compute three last decimal digits of the number 2^1000   (in common decimal notation).

**Things used to solve it**

- Theorem #9 (CRT)
- The Euler's theorem

**Approach**

CRT (long process) : To get the last few digits of a number, you need to find x mod( $10^{number\ of\ last\ digits\ you\ wants}$ ) (where x is your number so here 2^(1000) ). Use Euler's theorem to get a set of simplified congruencies. Then use CRT to resolve it.

Faster approach : Doing this recursively : 2^1000 (mod n) = (2^10 (mod n))^100 (mod n) = (24^10 (mod n))^10 (mod n) etc... Your calculator will manage to get (2^10 mod n) and so on...

**Results**

- Anthony (CRT) :
  - $2^{1000} mod(1000) = ?$
  - $1000 = 8 * 125$ ($8$ *and* $125$ *are relatively prime*)
  - *So we need to find* $2^{1000} mod(8) = ?$ *and* $2^{1000} mod(125) = ?$
  - $2^{1000} mod(8) = 0$ – *because* $2^n$ *can be divide by* $2^{n-1}$
  - $2^{1000} mod(125) = ?$
  - $GCD(2, 125) = 1$ (*we can apply euler theorem*)
  - $\varphi(125) = \varphi(5^3) = 4 * 5^2 = 100$
  - *So* $2^{100} \equiv 1(mod\ 125)$
  - *So* $2^{1000}(mod\ 125) = (2^{100})^{10}(mod\ 125) = 1^{10}(mod\ 125) = 1(mod\ 125)$
  - Now we need to find x (last 3 digits) of the following set of congruencies, (we'll do that using the CRT) :
  - $x \equiv 0(mod\ 8)$
  - $x \equiv 1(mod\ 125)$
  - With CRT we got : $x = 8 * 125 + 47 * 8 = 1376$
  - $x\ (mod\ 1000) = 376$
  - Last 3 digits of 2^1000 is 376.
- Anthony (Fast approach) :
  - $2^{1000}(mod\ 1000) = (2^{10}(mod\ 1000))^{100}(mod\ 1000) = (24^{10} mod\ 1000)^{10}$
  - $= (376^2(mod\ 1000))^5(mod\ 1000) = 376^5(mod\ 1000) = 376$

**Questions**

- -

## Problem #24

Compute two last decimal digits of the number 2^1000 (in radix 7 notation).

**Things used to solve it**

- The Euler's theorem

**Approach**

As you will do 2^1000 modulo (10^2) to find it in base 10, you just have to do 2^1000 modulo (7^2), then convert the number you have in base 10 to base 7.

**Results**

- Anthony :
  - 2^10%49=44
  - 44^10%49=23
  - 23^10%49=9
  - 9 base 10 = 12 base 7
  - Last 2 digits are 12

**Questions**

- -

## Problem #26

Find the last 4 decimal digits of the number 2^(10^6) using Chinese Remaider Theorem.

**Things used to solve it**

- Problem 23 CRT approach

**Approach**

It’s the same as problem 23 but to the power of 2 and mod 10000...

**Results**

- HANNAH : 6876

**Questions**

- .

[Complete me...]

# Test 2

Problem #1

Describe the ElGamal signature algorithm  and prove that verification formula is true when the signature parameters are correct.

**Things used to solve it**

- Lecture

**Approach**

See the lecture

**Results**

- 

**Questions**

- .

Problem #2

Describe the Nyberg-Rueppel signature algorithm  and prove that verification formula is true when the signature parameters are correct.

**Things used to solve it**

- Lecture (I guess)

**Approach**

See the lecture

**Results**

- 

**Questions**

- .

♥ *Work Well...* ♥