Introduction to Cryptology

Lecture-02

Mathematical Background for Cryptography:

Modular Arithmetic and gcd

07.03.2023, v4

Mathematical Background

Number Theory, Groups, Rings and Fields

Outlines

Deepest thanks

To James Massey (ETH Zürich).
for allowing me to use his lecture slides in 1987.

Many slides, especially those on mathematical fundamentals were inspired or used in modified forms in whole or in part from Jim Massey's lecture slides.

I had the pleasure and luck to be first introduced to this topic by Jim Massey at the ETH Zurich in 1985

1934-2013

James Massey is a well known coding theorist and cryptographer Having outstanding and major fundamental contributions in the last 60 years in the theory and technology of coding and cryptography.

Mathematical Background: in Number Theory

In many modern cryptographic systems, data blocks are represented as integers. Therefore integer algebra need to be introduced in the form of number theory:

Number sets of interest in cryptography*:*

- Natural numbers **N** = 0 1 2 3 .....
- Integers set **Z** = ... -3 -2 -1 0 1 2 3 ......
- For any integer $n \in$ **N** and n **>1 :**

$$n = \prod_{i=1}^{r} p_i \quad \text{where all } p_i \text{'s are prime factors of n}$$

r is the number of prime factors of n.

Modern cryptosystems deploy intensively the above two number sets **N** and **Z** in representing data blocks.

Integer Algebra: Euclidean Division Theorem for Integers

For any Integers n and d with $d \neq 0$ there is q and r, such that:

$$n / d = q + r / d$$
$$n = q d + r \quad \text{where} \quad \mathbf{0 \leq r < |d|}$$

We say: $R_d(n) = r$, ***r** is **Remainder** of **n** modulo **d***

Example: 13/5 = 2 + 3/5
or 13 = 2 . 5 + 3

In the remainder algebra $R_5(13) = 3$

Integer Algebra: Some Rules in the Remainder Arithmetic

Superposition Property (in linear systems):

$R_d\ (a + b) = R_d\ [R_d(a) + R_d(b)]$

$R_d\ (a \,.\, b) = R_d\ [R_d(a)\,.\, R_d(b)]$

Examples:

$R_5\ (7 + 14) = R_5\ [R_5(7) + R_5(14)]$
$= R_5\ [2 + 4] = R_5(6) = 1$

$R_5\ (9 \,.\, 22) = R_5\ [R_5(9)\,.\, R_5(22)]$
$= R_5\ [4 \,.\, 2] = R_5(8) = 3$

Equivalence Theorem: In the integer remainder system modulo d

$R_d(n) = R_d\ (n + i\,d\,)$ where n, i are any integers

Example: Remainders modulo 5 *(adding and substracting multiples of 5)*:

$R_5\ (7) = R_5\ [7 + 3 \times 5\,] = R_5\ [22\,] = 2$
$R_5\ (7) = R_5\ [7 + -2 \times 5\,] = R_5\ [-3\,] = 2$
→ **In this remainder algebra: 22 = -3 = 2** *(all are equivalent)*

The Standard Array of remainders in Z:

Integers having the same remainder can be tabulated in the so called "Standard Array" or "Slepian Array". For ***d=5***, the elements of Z can be ordered in a table having ***5 cosets***:

r									
0	···	-10	-5	0	5	10	15	....	← Remainder Class (coset)
1	···	-9	-4	1	6	11	16	....	
2	···	-8	-3	2	7	12	17	....	
3	···	-7	-2	3	8	13	18	....	
4	···	-6	-1	4	9	14	19	....	

Coset leader
mallest positive integer (Remainder)

Example this coset is equivalent to **3**
We have a total of 5 such cosets modulo 5

gcd: the greatest common divisor of Integers

gcd (m_1 , m_2 .... m_t) is the greatest positive integer which divides m_1 , m_2 .... m_t without remainder.

Example: gcd (15,5) = 5
gcd (15,9,27,12) = 3

If gcd (n_1 , n_2) = 1, then n_1 , n_2 are called ***relatively prime integers (coprimes)***

Example: gcd (15,28) = 1 => 15, 28 are relatively prime or coprimes

Properties of gcd:

gcd (n, 0) = n (for $n \neq 0$)
gcd (n, 0) = ? , undefined (if n = 0)
gcd (n_1 , n_2) = gcd (n_2 , n_1)
gcd (n_1 , n_2) = gcd ($\pm n_1$, $\pm n_2$)

The fundamental property of gcd:

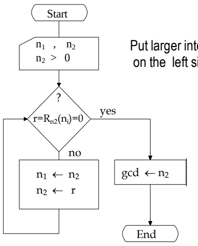
$\gcd(n_1 , n_2) = \gcd(\ n_1 + i\,n_2\ ,\ n_2\ )$

or $\gcd(n_1 , n_2) = \gcd(\ R_{n_2}(\,n_1)\ ,\ n_2\ )$

Examples:
gcd (15, 10) = gcd (15+10 , 10) = gcd (15-10 , 10)
= gcd (15 – 2x10 , 10) = gcd (-5,10)

Or gcd (15, 10) = gcd (R_{10}(15) , 10) = gcd (5 , 10) = gcd (5 , R_5 (10)) = gcd (5 , 0) = 5

Euclidean gcd Algorithm



Example:

Put larger integer on the left side

Remainder of dividing 132 by 108

n1	n2	r
132	108	24
108	24	12
24	12	0

gcd when r = 0

Time Complexity: < $\log_2 n + 1$ operations
n = Max [n_1, n_2]
Example: for 1000 bit integers, at most 1000 steps (divisions) are required to compute the gcd

Stein`s improvement for the Euclidean gcd Algorithm

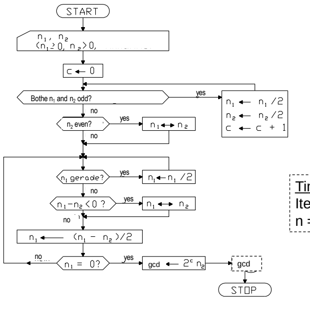
karl Stein *Prof. Univ LMU München (1913-2000). Mathematician, Cryptographer)*

There are 4 cases for n_1 and n_2 being even or odd integers:

1. n_1 and n_2 are even: → **gcd (n_1 , n_2) = 2 . gcd (n_1 /2 , n_2 /2)**
2. n_1 even, n_2 odd : → **gcd (n_1 , n_2) = gcd (n_1 /2 , n_2)**
3. n_1 odd, n_2 even : → **gcd (n_1 , n_2) = gcd (n_1 , n_2 /2)**
4. n_1 and n_2 are odd: → **gcd (n_1 , n_2) = gcd [(n_1-n_2) /2 , n_2]**

This simplifies the Euclidian algorithm to avoid real division operations as dividing an even integer by 2 is just a single bit right-shift (skip LSB).
Example: 6/2=3 in binary form 110/2 = 011

Stein's Improvement for the Euclidean gcd Algorithm



Time Complexity: < $\log_2 n + 1$
Iterations (substraction+shift)
n = Max [n_1, n_2]

Special gcd Properties

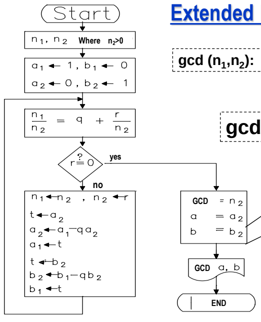
gcd (t^n-1, t^m-1) = $t^{\text{gcd (n, m)}}$ - 1

Examples:
gcd(2^{15}-1, 2^{20}-1) = $2^{\text{gcd}(15,20)}$ - 1 = 2^5-1 = 31
gcd[$(x + y)^{15}$-1, $(x + y)^{20}$-1] = $(x + y)^5$-1

more general:

$$\gcd\left(x^{q^n} - x ,\ x^{q^d} - x \right) = x^{q^{\gcd(n,d)}} - x$$

Extended Euclidean gcd Algorithm



gcd (n_1,n_2): is a linear combination of n_1 and n_2

gcd (n_1 , n_2) = a . n_1 + b . n_2

Example 1 : Extended Euclidean gcd Algorithm

gcd (n_1 , n_2) = a . n_1 + b . n_2
gcd (156, 117) = a 156 + b 117 find a and b

n_1	n_2	a_1	b_1	a_2	b_2	q	r	computation
156	117	1	0	0	1	1	39	156/117=1+ 39/117
117	(39)	0	1	1	-1	3	0	

gcd
a_1-qa_2= 1 –1 x 0 =1
b_1-qb_2 = 0 – 1 x 1 = -1

gcd (156, 117) = a . 156 + b . 117
= 1 . 156 + (-1) . 117 = 39
=> a = 1 , b = -1

Example 2 : Extended Euclidean gcd Algorithm

gcd (n_1 , n_2) = a . n_1 + b . n_2

Compute gcd (38, 7) = a x 38 + b x 7 find a and b

a_1-qa_2= 1 –5 x 0 =1
b_1-qb_2 = 0 – 5 x 1 = -5

n_1	n_2	a_1	b_1	a_2	b_2	q	r	computation
38	7	1	0	0	1	5	3	38/7=5+ 3/38
7	3	0	1	1	-5	2	1	7/3=2+ 1/7
3	(1)	1	-5	0-2x1 -2	1-2x-5 11	3	0	3/1=3+ 0/3

gcd

gcd (38, 7) = a . 38 + b . 7
= -2 . 38 + 11 . 7 = 1

Check! -76 + 77 =1

Extended "gcd" and the Modular Multiplicative Inversion

***Definition:* If an integer is invertible under multiplication modulo m, then it is called a unit**

***Example*: 2 x 3 = 6 = 1 (mod 5)**
says that : 3 is the multiplicative inverse of 2 modulo 5 (2^{-1}=3)
or 2 is the multiplicative inverse of 3 modulo 5 (3^{-1}=2)

Fundamental Theorem of units:
An integer **u** is a unit modulo m (or **u** has a ***multiplicative inverse* modulo m)** iff (if and only if):

gcd (m, u) = 1

Computing the multiplicative inverse: If gcd (m, u) = 1 then **a.m + b.u = 1**
Taking the remainder modulo m of both sides: R_m (a m + b u) = R_m (1)
R_m (b . u) = 1
or R_m b • R_mu =1 => **u^{-1} = R_m (b)**
or **u^{-1} =b (mod m)**

That is the multiplicative inverse of *u mod m* is the parameter *b mod m* in the extended Euclidian gcd Algorithm.

Example: gcd (7, 3) = 1 = **1 . 7 - 2 . 3** *(Extended Euclidian Algorithm)*
R_7(1 . 7 – 2 . 3) = 1
R_7(-2 . 3) = 1 => R_7 (3^{-1}) = -2 or -2 = -2+7 = 5 (mod 7)
That is **3^{-1} = -2= 5** Check: 3 . -2 = -6 = 1 (mod 7) or 3 . 5 = 15 = 1 (mod 7)

Example 3 : Extended gcd Algorithem and Multiplicative Inverse

gcd (n_1 , n_2) = a . n_1 + b . n_2

Question: Compute the multiplicative inverse of **9** modulo **11**

Solution: Compute gcd (11, 9) = a x 11 + b x 9 $\stackrel{?}{=}$ 1
if gcd=1, then the inverse is **b**

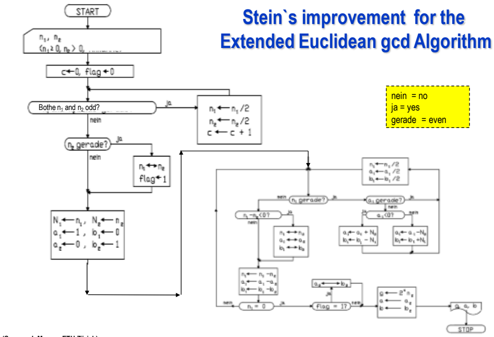
a_1-qa_2 b_1-qb_2

n_1	n_2	a_1	b_1	a_2	b_2	q	r	computation
11	9	1	0	0	1	1	2	11/9 = 1 + 2/11
9	2	0	1	1	0-1x1 -1	4	1	9/2 = 4 + 1/2
2	(1)	1	-1	0-4x1 -4	1-4x-1 5	2	0	2/1=2+ 0/1

gcd

gcd (11,9) = a . 11 + b . 9
= -4 . 11 + 5 . 9 = 1 ← **mod 11 => 0 + 5 x 9 = 1 (mod 11)**
=> 5 x 9 mod 11 =1
Check! -44 + 45 =1
That is 9^{-1} mod 11 = 5

Stein`s improvement for the Extended Euclidean gcd Algorithm



(Source: J. Massey ETH Zürich)

Extended gcd Solution as Excel Sheet:

Solution: Compute gcd (156, 17) = a x 156 + b x 17 = 1
if gcd=1, then the inverse is **b**

m	u	a1	a2	b1	b2	q	r	INVERSE VALUE = B2		GCD	
156	17	1	0	0	1	9	3				
17	3	0	1	1	-9	5	2				
3	2	1	-5	-9	46	1	1				
2	1	-5	6	46	-55	2	0	NVERSE=	-55	GCD=	1

Check: 17 x - 55 = -155 = -155+156 = 1 mod 156
Or 17^{-1}= -55 = -55 +156 = 101

Check: 17 x 101 = 1717 = 1 mod 156