SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107
An Autonomous Institution
Accredited by NAAC-UGC with 'A' Grade
Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Course Code and Name : 19CS503 – CRYPTOGRAPHY AND NETWORK SECURITY

III YEAR / V SEMESTER

Unit 2: Symmetric Cryptography

Topic 2: Modular arithmetic-Euclid"s algorithm

Modular Arithmetic

- Obey the relationship
- a= qn + r ; 0<= r<= n ; q = [a/n]
- a = a/n * n + (a mod n)
- Congruent Modulo n
- if (a mod n) = (b mod n).
- $a \equiv b \pmod{n}$.

$$a = q_0 b + r_0$$
$$b = q_1 r_0 + r_1$$
$$r_0 = q_2 r_1 + r_2$$
$$r_1 = q_3 r_2 + r_3$$
$$\vdots$$

Positive integer n

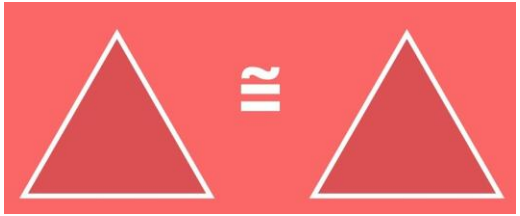
Non negative integer a

Divide a by n

Get integer Quotient q & integer remainder r

Properties of Congruence

- $a \equiv b \pmod{n}$ if $n \mid (a - b)$.
- $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$.
- $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply $a \equiv c \pmod{n}$.



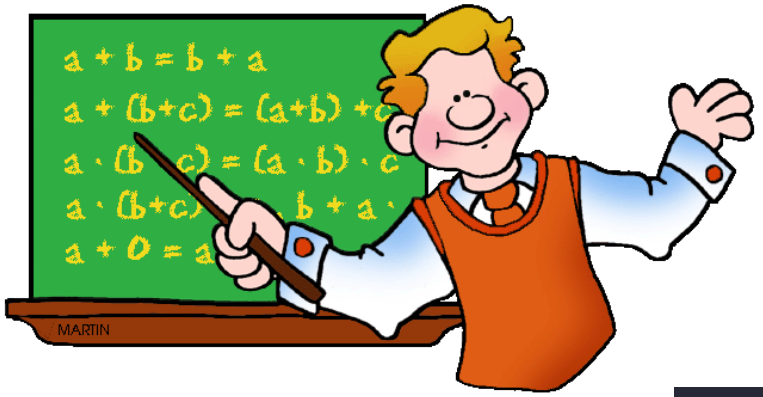
$23 \equiv 8 \pmod{5}$	because	$23 - 8 = 15 = 5 \times 3$
$-11 \equiv 5 \pmod{8}$	because	$-11 - 5 = -16 = 8 \times (-2)$
$81 \equiv 0 \pmod{27}$	because	$81 - 0 = 81 = 27 \times 3$

- $a = b + kn$, for some k

Properties of Modular Arithmetic

- $(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$
- $(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$
- $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$
- Define $(a \bmod n) = r_a$; $a = jn + r_a$ for some j
  $(b \bmod n) = r_b$; $b = kn + r_b$ for some k

$$
\begin{aligned}
(a + b) \bmod n &= (jn + r_a + kn + r_b) \bmod n \\
&= (r_a + r_b + (k + j)n) \bmod n \\
&= (r_a + r_b) \bmod n \\
&= [(a \bmod n) + (b \bmod n)] \bmod n
\end{aligned}
$$



Example

- Solve this for the properties
- 11 mod 8 = 3; 15 mod 8 = 7

$[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 =$
$10 \bmod 8 = 2$
$(11 + 15) \bmod 8 = 26 \bmod 8 = 2$

$[(11 \bmod 8) - (15 \bmod 8)] \bmod 8 =$
$-4 \bmod 8 = 4$
$(11 - 15) \bmod 8 = -4 \bmod 8 = 4$

$[(11 \bmod 8) * (15 \bmod 8)] \bmod 8 =$
$21 \bmod 8 = 5$
$(11 * 15) \bmod 8 = 165 \bmod 8 = 5$

Modulo 8 Addition and Multiplication

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

*	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Inverse:

$(x + y) \bmod 8 = 0.$

$(x \times y) \bmod 8 = 1$

Modulo 8 Addition and Multiplication

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

*	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

w	-w	w^{-1}
0	0	-
1	7	1
2	6	-
3	5	3
4	4	-
5	3	5
6	2	-
7	1	7

Inverse: $(x+y) \bmod 8 = 0.$ $(x \times y) \bmod 8 = 1$

Properties of Modular Arithmetic

Property	Expression
Commutative Laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative Laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive Law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive Inverse (-w)	For each $w \in Z_n$, there exists a z such that $w + z \equiv 0 \bmod n$

Modular Arithmetic Recap

Compute the table for Modulo 7 Arithmetic – Addition, Multiplication and their inverse

$$a = q_0 b + r_0$$
$$b = q_1 r_0 + r_1$$
$$r_0 = q_2 r_1 + r_2$$
$$r_1 = q_3 r_2 + r_3$$
$$\vdots$$

Euclid's Algorithm

- Greatest Common Divisor (gcd)
- gcd : A common problem in number theory.
- gcd(a, b) : (greatest common divisor of a and b) is the largest number that divides evenly into both a and b
  - gcd(a, b) = max{ k ; such that k|a and k|b }
  - gcd(60, 24) = 12
- If gcd(a, b) = 1, i.e. if a and b have no common factors
  - (except 1) and hence a and b are relatively prime
- gcd(8,15) = 1 implies 8 and 15 are relatively prime

Algorithm and Example gcd(1970, 1066)

1970 = 1 x 1066 + 904	gcd(1066, 904)
1066 = 1 x 904 + 162	gcd(904, 162)
904 = 5 x 162 + 94	gcd(162, 94)
162 = 1 x 94 + 68	gcd(94, 68)
94 = 1 x 68 + 26	gcd(68, 26)
68 = 2 x 26 + 16	gcd(26, 16)
26 = 1 x 16 + 10	gcd(16, 10)
16 = 1 x 10 + 6	gcd(10, 6)
10 = 1 x 6 + 4	gcd(6, 4)
6 = 1 x 4 + 2	gcd(4, 2)
4 = 2 x 2 + 0	gcd(2, 0)

Euclid(A,B)
If B=0 then return A
else return Euclid(B, A mod B)

Therefore, gcd(1970, 1066) = 2

Step *k*	Equation	Quotient and remainder
0	$1071 = q_0\,462 + r_0$	$q_0 = 2$ and $r_0 = 147$
1	$462 = q_1\,147 + r_1$	$q_1 = 3$ and $r_1 = 21$
2	$147 = q_2\,21 + r_2$	$q_2 = 7$ and $r_2 = 0$; algorithm ends

Extended Euclidean Algorithm

- For given integers a and b, the extended Euclidean algorithm not only calculate the greatest common divisor d but also two additional integers x and y that satisfy the following equation.
  - $ax + by = d = gcd(a, b)$

Extended Euclidean Algorithm Example gcd(1759,550)

c	d	q	r	Conclusion
1759	550	3	109	109=1759-3(550) 109=a-3b
550	109	5	5	5=550-5(109) 5=b-5(a-3b) 5=b-5a+15b 5=-5a+16b
109	5	21	4	4=109-21(5) 4=a-3b-21(-5a+16b) 4=a-3b+105a-336b 4=106a-339b
5	4	1	1	1=5-1(4) 1=-5a+16b-106a+339b 1=-111a+355b
4	1	4	0	

a= 1759 b=550 Answer: -111a+355b =1=gcd(a,b)

Assessment

Find the GCD of the (24140,16762)

Thanks!

References

- William Stallings, Cryptography and Network Security: Principles and Practice, PHI 3rd Edition, 2006.