INF 638
Cryptography & Cryptosystems

Section: 2 Elements of Number Theory

Dr. Bertrand Cambou
Professor of Practice NAU, Cybersecurity
School of Informatics, Computing, and Cyber-Systems
Bertrand.cambou@nau.edu

NORTHERN ARIZONA UNIVERSITY

INF 638: Cryptography & Cryptosystems

- 1- Motivation & Definitions
- 2- Elements of Number theory
- 3- Early Cryptographic methods
- 4- Symmetrical Cryptography: DES
- 5- Symmetrical Cryptography: AES
- 6- Quantum Cryptography: Key distribution
- 7- Elements of Asymmetrical Cryptography
- 8- Asymmetrical Cryptography: RSA
- 9- ECC Key Distribution
- 10- PKI & Digital Signatures
- 11- Hash Functions
- 12- Smartcards

NORTHERN ARIZONA UNIVERSITY

2- Elements of Number Theory

- 2-1 Modulo arithmetic
- 2-2 Prime numbers – co-primes
- 2-3 Composite numbers
- 2-4 Pascal triangle
- 2-5 Fermat Theorem
- 2-6 Euler Theorem
- 2-7 Chinese remainder theorem

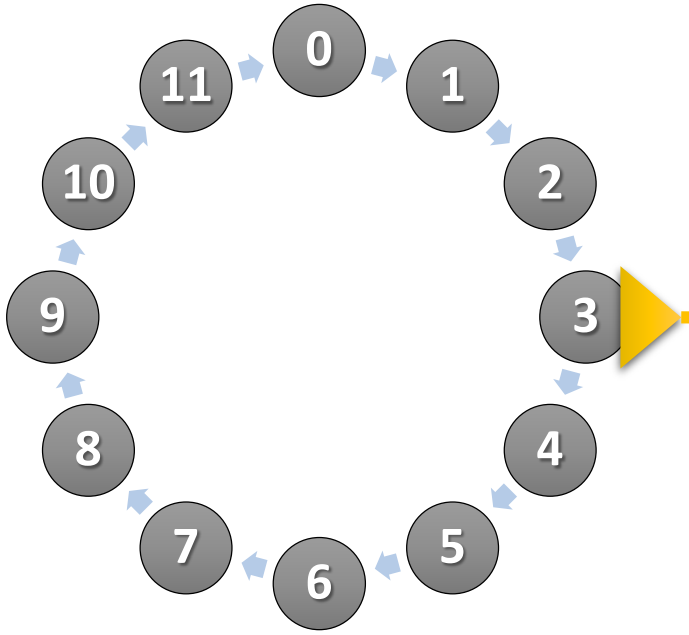
Definition 1

Let $m \neq 0$ be an integer; ***a*** is congruent to ***b*** modulo ***m***

$$a \bmod m = b \quad \text{or} \quad a \equiv b \bmod m$$

if $m \mid (a-b)$, or $\exists$ integer ***k*** such as: $a - b = km$

Class of solutions: $\ldots, b-2m, b-m, y, b+m, b+2m, \ldots$



Example #1: 3 Mod 12 = ?

{ …, -45, -33, -21, -9, 3, 15, 27, 39, 51, ….}

k = -4 -3 -2 -1 0 1 2 3 4

$-45 \equiv 3 \bmod 12$

$-9 \equiv 3 \bmod 12$

$15 \equiv 3 \bmod 12$

$51 \equiv 3 \bmod 12$

Basic Arithmetic

Let a, b, c, d, m, n be integers; $m \neq 0$;

$a \equiv b \bmod(m)$ & $c \equiv d \bmod(m)$ then:

(1) $(a + c) \equiv (b + d) \bmod(m)$

(2) $(a - c) \equiv (b - d) \bmod(m)$

(3) $(a \times c) \equiv (b \times d) \bmod(m)$

(4) $a^n \equiv b^n \bmod(m)$

Example #2: Modulo 5

$$(13 \times 16) - 8 \equiv b \bmod 5$$

Hard way:

$$(13 \times 16) - 8 = 208 - 8 = 200 \equiv 0 \bmod 5$$

$$b = 0$$

Smart way:

$$(3 \times 1) - 3 = 3 - 3 \equiv 0 \bmod 5$$

Example #3: Modulo 7

Hard way:

$3^8 \bmod 7 = 6561 \bmod 7 = 2$

Smart way:

$3^2 \times 3^2 \times 3^2 \times 3^2 \equiv 2 \times 2 \times 2 \times 2 \bmod 7$

$\equiv (\quad 1 \quad) \times 2 \bmod 7 = 2$

Example #4: $31^{7} \bmod (33) = ?$

Brute force way to resolve 31^7 mod (33)

$31^7 = 27{,}512{,}614{,}111$

$= 27{,}512{,}614{,}107 + 4 \equiv 4 \bmod 33$

$33 \times 833{,}715{,}579$

$31^7 = 27{,}512{,}614{,}111$

33x**8**00,000,000 = 26,400,000,000

rest 1,112,614,111

33x **3**0,000,000 = 990,000,000

rest 122,614,111

33x **3**,000,000 = 99,000,000

rest 23,614,111

33x **7**00,000 = 23,100,000

rest 514,111

33x **1**0,000 = 330,000

rest 184,111

33x **5**,000 = 165,000

rest 19,111

33x **5**00 = 16,500

rest 2,611

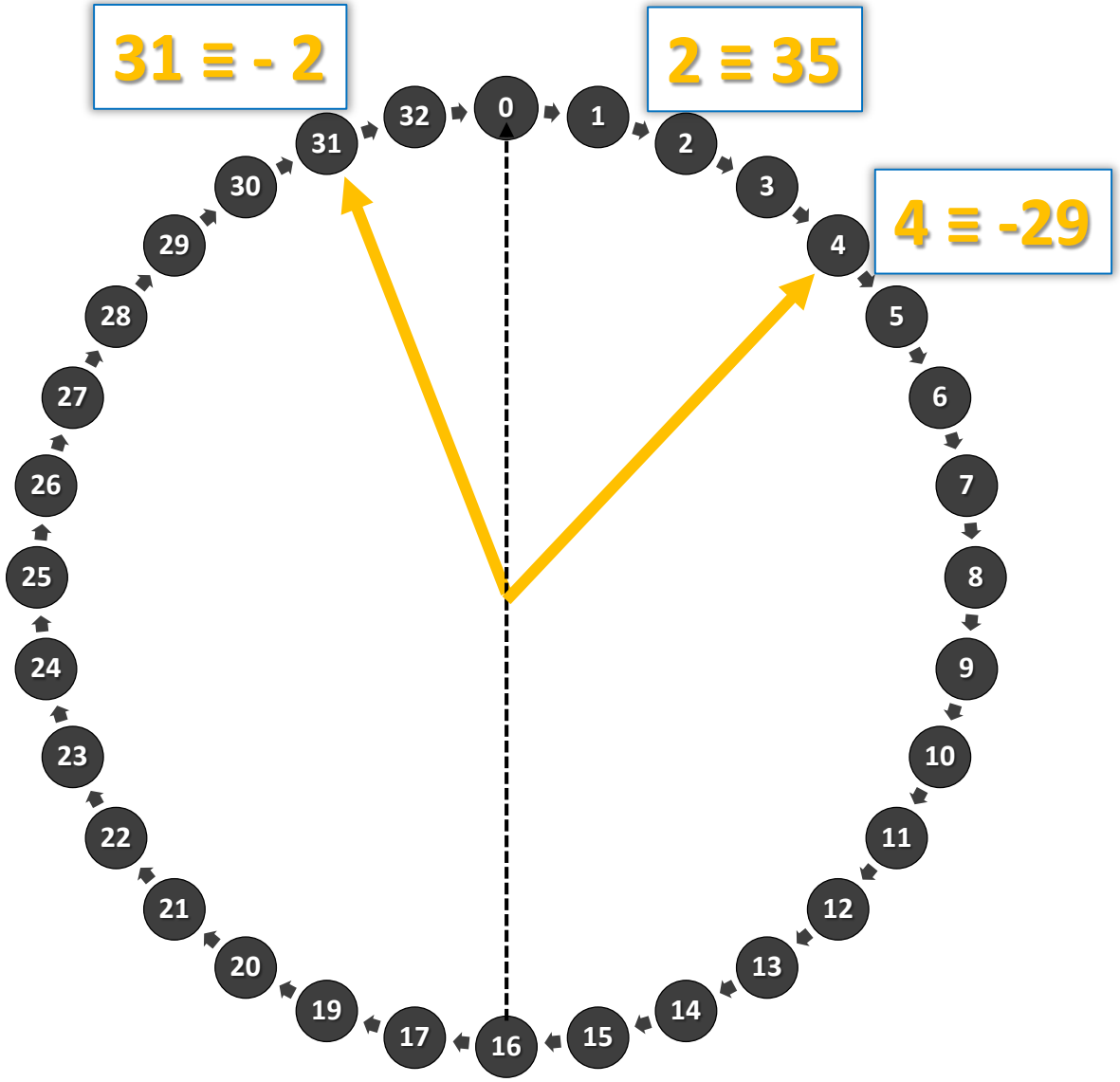
33x **7**0 = 2,310

rest 301

33x **9** = 297

rest **4**

Fast way to resolve 31^7 mod (33)



$$
\begin{aligned}
31^7 &\equiv (-2)^7 && \mod 33 \\
&\equiv (-128) && \mod 33 \\
&\equiv -(29 + \cancel{99}) && \mod 33 \\
&\equiv 4 && \mod 33
\end{aligned}
$$

$$
\begin{aligned}
35^7 &\equiv (2)^7 && \mod 33 \\
&\equiv (128) && \mod 33 \\
&\equiv (29 + \cancel{99}) && \mod 33 \\
&\equiv -4 && \mod 33
\end{aligned}
$$

Example #5: $31^9 \bmod (33)$?

$$
\begin{aligned}
31^9 &\equiv 31^7 \text{x } 31^2 \pmod{33} \\
&\equiv 4 \text{ x } (-2)^2 \pmod{33} \\
&\equiv 16 \pmod{33}
\end{aligned}
$$

Example #6: 31^{14} mod (33) ?

$31^{14} = 31^{7} \times 31^{7} \equiv \mathbf{4 \times 4} \bmod 33 = 16$

Example #7: 31^{20} & 35^{20} mod (33) ?

$$31^{20} = (31^7)^3 / 31$$
$$\equiv (4x4x4)/(-2) \bmod 33$$
$$\equiv -32 \bmod 33$$
$$\equiv 1 \bmod 33$$

$$35^{20} = (35^7)^3 / 35$$
$$\equiv -(4x4x4)/2 \bmod 33$$
$$\equiv -32 \bmod 33$$
$$\equiv 1 \bmod 33$$

Other properties for congruence

Let a, b, c, m be integers; $m \neq 0$;

1- $ac \equiv bc \bmod(m)$ ➔ $a \equiv b \bmod(m)$??? Not always!!!

Ex: $3 \times 4 \equiv 3 \times 8 \bmod 12$ however $4 \neq 8 \bmod 12$

2- If $\gcd(c, m)=1$

$ac \equiv bc \bmod(m)$ ➔ $a \equiv b \bmod(m)$

Proof: $m \mid (ac-bc)$ m does not divide c so: $m \mid (a-b)$

3- If $\gcd(c, m)=d$

$ac \equiv bc \bmod(m)$ ➔ $a \equiv b \bmod(m/d)$

Proof: $m \mid (ac-bc)$ ➔ $(m/d) \mid (ac-bc)/d = (a-b)(c/d)$

m/d does not divide c/d ➔ $m/d \mid (a-b)$

NORTHERN ARIZONA UNIVERSITY

2- Elements of Number Theory

- 2-1 Modulo arithmetic
- 2-2 Prime numbers – co-primes
- 2-3 Composite numbers
- 2-4 Pascal triangle
- 2-5 Fermat Theorem
- 2-6 Euler Theorem
- 2-7 Chinese remainder theorem

Example of prime number - Multiply modulo 19

19	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	2	4	6	8	10	12	14	16	18	1	3	5	7	9	11	13	15	17
3	3	6	9	12	15	18	2	5	8	11	14	17	1	4	7	10	13	16
4	4	8	12	16	1	5	9	13	17	2	6	10	14	18	3	7	11	15
5	5	10	15	1	6	11	16	2	7	12	17	3	8	13	18	4	9	14
6	6	12	18	5	11	17	4	10	16	3	9	15	2	8	14	1	7	13
7	7	14	2	9	16	4	11	17	6	13	1	8	15	3	10	17	5	12
8	8	16	5	13	2	10	17	6	15	4	12	1	9	17	6	14	3	11
9	9	18	8	17	7	16	6	15	5	14	4	13	3	12	2	11	1	10
10	10	1	11	2	12	3	13	4	14	5	15	6	16	7	17	8	18	9
11	11	3	14	6	17	9	1	12	4	15	7	18	10	2	13	5	16	8
12	12	5	17	10	3	15	8	1	13	6	18	11	4	16	9	2	14	7
13	13	7	1	14	8	2	15	9	3	16	10	4	17	11	5	18	12	6
14	14	9	4	18	13	8	3	17	12	7	2	16	11	6	1	15	10	5
15	15	11	7	3	18	14	10	6	2	17	13	9	5	1	16	12	8	4
16	16	13	10	7	4	1	17	14	11	8	5	2	18	15	12	9	6	3
17	17	15	13	11	9	7	5	3	1	18	16	14	12	10	8	6	4	2
18	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

N	Inv.
1	1
2	10
3	13
4	5
5	4
6	16
7	11
8	12
9	17
10	2
11	7
12	8
13	3
14	15
15	14
16	6
17	9
18	19

Properties prime numbers

1- If m is prime all $\mathbb{Z}_m$:{*1, 2, …m-1*} have an inverse.

Proof: See Extended Euclidian Algorithm (EEA) Section-8

2- If m is prime: only *m-1* and *1* *are the inverse of each others*

Proof: $a_i a_i^{-1} \equiv 1 \, mod \, m$

If $a_i = a_i^{-1}$ ➔ $a_i^2 \equiv 1 \, mod \, m$

$$a_i^2 - 1 = (a_i - 1)(a_i + 1) \equiv 0 \bmod m$$

➔ Two solutions $\boldsymbol{a_i}$ = 1 and $\boldsymbol{a_i}$ = -1 = m-1

Wilson Theorem

If m prime

$(m-1)! \equiv -1 \bmod m$

Proof:

$$(m-1)! \equiv (m-1)(m-2) \ldots (2)(1) \equiv (m-1)(1) \equiv -1 \bmod m$$

Only **m-1** and **1** are the inverse of each others

All others disappear with their inverse

$$(m-1)! \equiv -1 \bmod m$$

NORTHERN ARIZONA UNIVERSITY

2- Elements of Number Theory

- 2-1 Modulo arithmetic
- 2-2 Prime numbers – co-primes
- 2-3 Composite numbers
- 2-4 Pascal triangle
- 2-5 Fermat Theorem
- 2-6 Euler Theorem
- 2-7 Chinese remainder theorem

Definition of composite number

$$m = a_1^{e_1}\ a_2^{e_2}\ \ldots a_f^{e_f}$$

with $a_1, a_2, \ldots, a_f$ prime integer numbers

Properties co-prime numbers

- Group $\mathbb{Z}'_m$ of ϕ_m **co-primes** of m : $\{a_1, a_2, \ldots, a_{\phi_m}\}$; gcd(a_i,m)=1

  ϕ_m is the Euler parameter

- If a_i and a_j are **co-primes** [a_i;a_j ϵ $\mathbb{Z}'_m$: $\{a_1, a_2, \ldots, a_{\phi_m}\}$],

  then their multiplication modulo m is also part of $\mathbb{Z}'_m$

  $(a_i \,.\, a_j) mod m$ ϵ $\mathbb{Z}'_m$: $\{a_1, a_2, \ldots, a_{\phi_m}\}$

- Co-primes of m are a closed group $\mathbb{Z}'_m$ with multiplication mod m

Euler parameter ϕ_{15} of 15:

$\phi_{15} = 8$

The co-primes of 15 are: {1, 2, 4, 7, 8 11 13 14}

Properties co-prime numbers

- If *m* is **not prime**, only **co-primes** of *m* have an inverse;
  Proof: See Extended Euclidian Algorithm (EEA) Section-8

Example: 15

N	Inv.
1	*1*
2	*8*
4	*4*
7	*13*
8	*2*
11	*11*
13	*7*
14	*14*

Example of composite number: Multiply modulo 15

X 15	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	2	4	6	8	10	12	14	1	3	5	7	9	11	13
3	3	6	9	12	0	3	6	9	12	0	3	6	9	12
4	4	8	12	1	5	9	13	2	6	10	14	3	7	11
5	5	10	0	5	10	0	5	10	0	5	10	0	5	10
6	6	12	3	9	0	6	12	3	9	0	6	12	3	9
7	7	14	6	13	5	12	14	11	3	10	2	9	1	8
8	8	1	9	2	10	3	11	4	12	5	13	6	14	7
9	9	3	12	6	0	9	3	12	6	0	9	3	12	6
10	10	5	0	10	5	0	10	5	0	10	5	0	10	5
11	11	7	3	14	10	6	2	13	9	5	1	12	8	4
12	12	9	6	3	0	12	9	6	3	0	12	9	6	3
13	13	11	9	7	5	3	1	14	12	10	8	6	4	2
14	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Composite numbers

If m is a composite of prime numbers, and m >5: $(m\text{-}1)! \equiv 0 \bmod m$

Proof: $(m\text{-}1)! = (m\text{-}1) \times (m\text{-}2) \times \ldots 2 \times 1$

case 1: $m = a_1^{e_1} a_2^{e_2} \ldots a_f^{e_f}$

$$(m\text{-}1)! = (m\text{-}1) \ldots a_1^{e_1} \ldots a_2^{e_2} \ldots a_f^{e_f} \ldots (1) \equiv k \times m \bmod m$$

All factors $a_i^{e_i}$ are smaller than m, therefore part of the factorial term

$$(m\text{-}1)! \equiv k\, m \bmod m \equiv 0 \bmod m$$

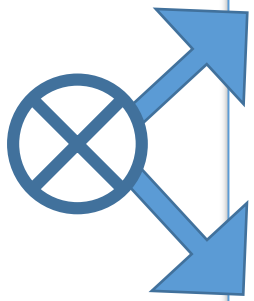
case 2: $m = a_1^{e_1}$

$$(m\text{-}1)! = (m\text{-}1) \ldots a_1^{e_1-1} \ldots a_1 \ldots (1) \equiv k\, m \bmod m$$

$$(m\text{-}1)! \equiv k\, m \bmod m \equiv 0 \bmod m$$

Compare Prime numbers versus Composite numbers

(m-1)! mod m



m is prime ➔ $(m-1)! \equiv -1 \bmod m$

m is composite ➔ $(m-1)! \equiv 0 \bmod m$

NORTHERN ARIZONA UNIVERSITY

2- Elements of Number Theory

- 2-1 Modulo arithmetic
- 2-2 Prime numbers – co-primes
- 2-3 Composite numbers
- 2-4 Pascal triangle
- 2-5 Fermat Theorem
- 2-6 Euler Theorem
- 2-7 Chinese remainder theorem

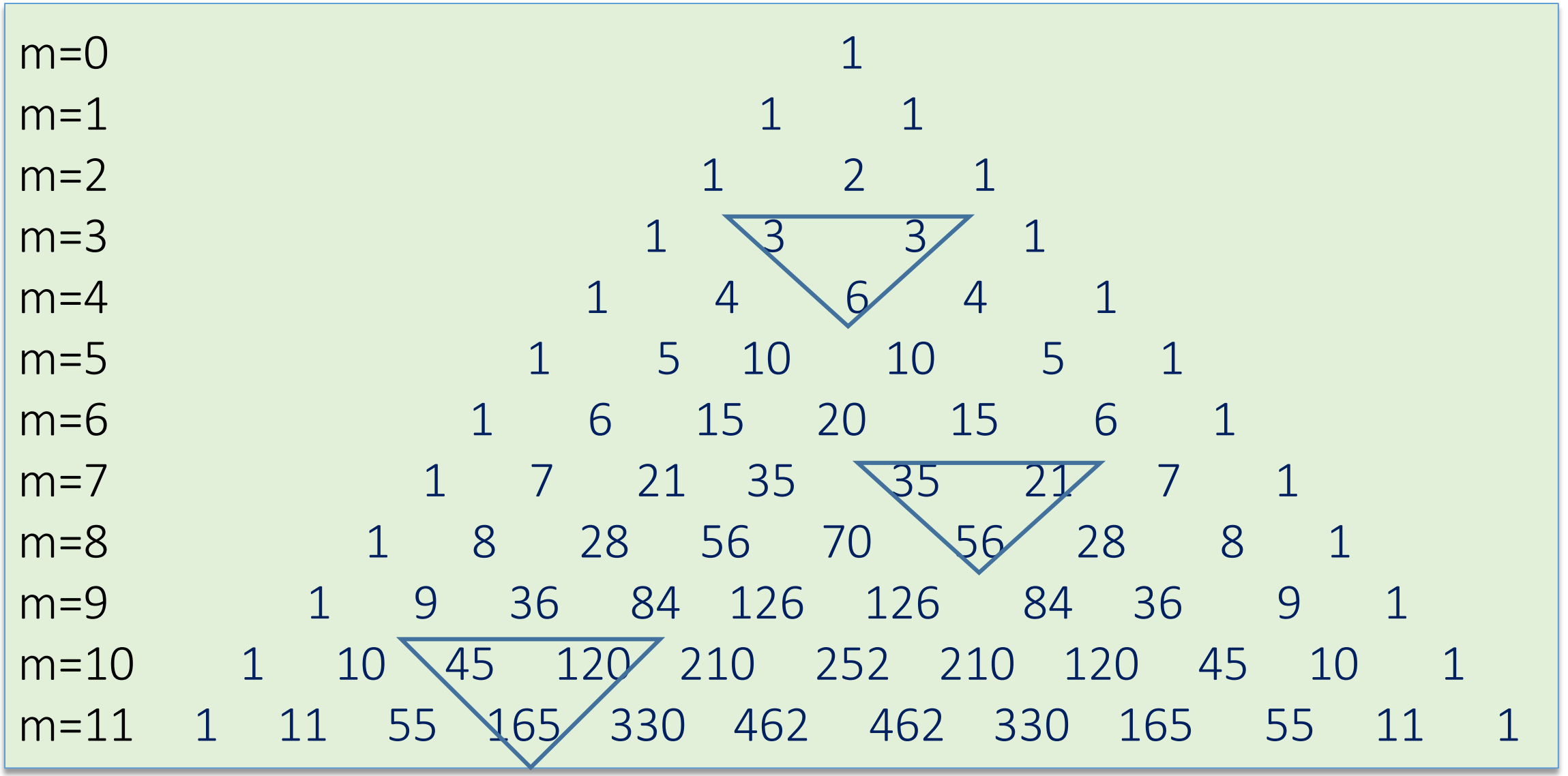
Pascal triangle

$(1+X)^m = \sum_{k=0}^{k=m} \binom{m}{k} X^k$ with: $\binom{m}{k} = \frac{m!}{(m-k)!k!} \in \mathbf{N}$ and 0!=1

m=0						1						
m=1					1		1					
m=2				1		2		1				
m=3			1		3		3		1			
m=4		1		4		6		4		1		
m=5	1		5		10		10		5		1	
m=6		1		6		15		20		15		6		1	
m=7	1		7		21		35		35		21		7		1
m=8		1		8		28		56		70		56		28		8		1
m=9	1		9		36		84		126		126		84		36		9		1
m=10		1		10		45		120		210		252		210		120		45		10		1
m=11	1		11		55		165		330		462		462		330		165		55		11		1

Pascal triangle:

In a triangle: add the two terms above to find the bottom one



Pascal triangle:

when m prime, all terms are multiples of m ➔ ≡ 0 mod m

m=0						1						
m=1					1		1					
m=2				1		2		1				
m=3			1		3		3		1			
m=4		1		4		6		4		1		
m=5	1		5		10		10		5		1	
m=6		1		6		15		20		15		6		1
m=7	1		7		21		35		35		21		7		1
m=8		1		8		28		56		70		56		28		8		1
m=9	1		9		36		84		126		126		84		36		9		1
m=10		1		10		45		120		210		252		210		120		45		10		1
m=11	1		11		55		165		330		462		462		330		165		55		11		1

Pascal triangle and prime numbers

If m is prime, $k \in \mathbb{Z}_m$ $\{1, 2, \ldots m-1\}$;

$$\binom{m}{k} \equiv \frac{m!}{(m-k)!k!} \bmod m \equiv m \frac{(m-1)(m-2)\ldots(m-k+1)}{k(k-1)(k-2)\ldots 1} \bmod m$$

The terms $k, (k-1), (k-2), \ldots, 1$ cannot divide m (m is prime)

They have to divide $(m-1)(m-2)\ldots(m-k+1)$

$$\binom{m}{k} \equiv m \, x \, f \bmod m$$

with $f = \frac{(m-1)(m-2)\ldots(m-k+1)}{k(k-1)(k-2)\ldots 1} \in \mathbb{N}$

$$\binom{m}{k} \equiv 0 \bmod m$$

→ $(1+X)^m \equiv 1 + X^m \bmod m$

→ $(1-X)^m \equiv 1 + (-X)^m \bmod m$

NORTHERN ARIZONA UNIVERSITY

2- Elements of Number Theory

- 2-1 Modulo arithmetic
- 2-2 Prime numbers – co-primes
- 2-3 Composite numbers
- 2-4 Pascal triangle
- 2-5 Fermat Theorem
- 2-6 Euler Theorem
- 2-7 Chinese remainder theorem

Proof#1

Fermat Little Theorem:

If m prime $a^{m-1} \equiv 1 \bmod m$

- *a=1* is obvious
- *a=2* ; *k* ϵ {*0, 1, 2, …m*} :

$$2^m = (1+1)^m = \sum_{k=0}^{k=m} 1^k \binom{m}{k} \equiv 1 + \sum_{k=1}^{k=m-1} 1^k \frac{m!}{(m-k)!\,k!} + 1 \bmod m$$

$\frac{m!}{(m-k)!\,k!} \equiv 0 \bmod m$

$$\equiv 2 \bmod m$$

$$\rightarrow 2^{m-1} \equiv 1 \bmod m$$

- If true for *a-1* can we conclude that it is true for *a*?

$$a^m = ((a-1)+1)^m \equiv (a-1)^m + \sum_{k=1}^{k=m-1} (a-1)^k \frac{m!}{(m-k)!\,k!} + 1 \bmod m$$

$(a-1)^m \equiv (a-1) \bmod m$

$$\equiv ((a-1)+1) \bmod m$$

$\frac{m!}{(m-k)!\,k!} \equiv 0 \bmod m$

$$\rightarrow a^{m-1} \equiv 1 \bmod m$$

Proof#2

Fermat Little Theorem:

If m prime $a^{m-1} \equiv 1 \, mod \, m$

The non zero congruent classes of m is: {1, 2, ….., m-1} [A]

By multiplying by a we obtain: {1.a, 2.a, ….., (m-1).a} [B]

The classes [A] and [B] (modulo n) contain the same elements in a different order.

The multiplication of all elements of [A] and [B] are the same:

$[1.2. \ldots .(m-1)]=[(1.a).(2.a) . \ldots .((m-1).a)]=[1.2. \ldots .(m-1)].\mathbf{a^{m-1}}$

➔ $a^{m-1} \equiv 1 \, mod \, m$

Example: 31^{32} mod (33) ?

$$31^{32} \equiv 31^7 \text{x } 31^7 \text{x } 31^{20} / 31^2 \mod 33$$

$$\equiv 4 \text{ x } 4 \text{ x } 1 / (-2)^2 \mod 33$$

$$\equiv 4 \mod 33$$

33 is not prime, so “Fermat” is not working

Example: 33^{30} & 34^{30} mod (31) ?

$$33^{30} \equiv 2^{30} \bmod 31$$
$$\equiv 2^5 \times 2^5 \times 2^5 \times 2^5 \times 2^5 \times 2^5 \bmod 31$$
$$\equiv 1 \times 1 \times 1 \times 1 \times 1 \times 1 \bmod 31$$
$$34^{30} \equiv 3^{30} \bmod 31$$
$$\equiv 3^5 \times 3^5 \times 3^5 \times 3^5 \times 3^5 \times 3^5 \bmod 31$$
$$\equiv (-5)\times(-5)\times(-5) \times (-5)\times(-5)\times(-5) \bmod 31$$
$$\equiv (-125) \times (-125) \bmod 31$$
$$\equiv (-1) \times (-1) \bmod 31$$

NORTHERN ARIZONA UNIVERSITY

2- Elements of Number Theory

- 2-1 Modulo arithmetic
- 2-2 Prime numbers – co-primes
- 2-3 Composite numbers
- 2-4 Pascal triangle
- 2-5 Fermat Theorem
- 2-6 Euler Theorem
- 2-7 Chinese remainder theorem

Euler Theorem

If m, and a co-primes: $a^{\Phi m} \equiv 1 \, mod \, m$

The non congruent classes of ϕm is: $\{X_1, X_2, ..., X_{Им}\}$ [A]

By multiplying by a we obtain: $\{a.X_1, a.X_2, ..., a.X_{Им}\}$ [B]

[A] and [B]contain the same elements in a different order:

The multiplication of all elements of [A] and [B] are the same:

$$[X_1.X_2. \dots .X_{\phi m}]=[(X_1.a).(X_2.a). \dots .(X_{\phi m}.a)]=[X_1.X_2. \dots .X_{\phi m}].a^{\Phi m}$$

$$\rightarrow \quad a^{\Phi m} \equiv 1 \bmod m$$

Euler Theorem

(Extension of Fermat little theorem)

If m, and a co-primes: $a^{\Phi m} \equiv 1 \, mod \, m$

Φ_m is Euler coefficient: Number of co-primes of m

If m=p x q with p and q primes: $\Phi_m = (p-1)(q-1)$

Example #7: Fast way to resolve 31^{20} mod (33) ?

$31^{20} = (31^7)^3 \, / \, 31$

$= - (4x4x4)/2 = -32$

$\equiv 1 \text{ mod } 33$

$\Phi_{33} = (11-1)(3-1) = 20$

$31^{20} = 31^{\Phi_{33}} \equiv 1 \text{ mod } 33$

NORTHERN ARIZONA UNIVERSITY

2- Elements of Number Theory

- 2-1 Modulo arithmetic
- 2-2 Prime numbers – co-primes
- 2-3 Composite numbers
- 2-4 Pascal triangle
- 2-5 Fermat Theorem
- 2-6 Euler Theorem
- 2-7 Chinese remainder theorem

Chinese remainder theorem

1-Problem: find x in the following system of congruence:

$\boldsymbol{m_i}$ and $\boldsymbol{m_j}$ are co-primes, *i and j* ∈ {*1,2, …,k*}, *i≠j* ➔ *cgd*($\boldsymbol{m_i}$, $\boldsymbol{m_j}$)=1

$$x \equiv a_1 \, mod \, \boldsymbol{m_1}$$
$$\dots$$
$$x \equiv a_i \, mod \, \boldsymbol{m_i}$$
$$\dots$$
$$x \equiv a_k \, mod \, \boldsymbol{m_k}$$

2- Solution: $x \equiv (a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_k M_k y_k) \, mod \, M$

$M = \boldsymbol{m_1} \dots \boldsymbol{m_i} \dots \boldsymbol{m_k}$

$M_i = M / \boldsymbol{m_i}$

$M_i y_i \equiv 1 \, mod \, \boldsymbol{m_i}$ (y_i is the inverse of M_i)

Chinese remainder theorem: Example

1-Define the system of congruence:

$$x \equiv 2 \; mod \; 3$$
$$x \equiv 3 \; mod \; 5$$
$$x \equiv 2 \; mod \; 7$$

$M = m_1 m_2 m_3 = 105 \quad M_1 = 35 \quad M_2 = 21 \quad M_3 = 15$

2- Solution: $x \equiv (a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3) \; mod \; M$

$M_1 y_1 \equiv 1 mod m_1$ → $35y_1 \equiv 1 \text{mod } 3$ → $2y_1 \equiv 1 \text{mod } 3$ → $y_1 = 2$

$M_2 y_2 \equiv 1 mod \; m_2$ → $21y_2 \equiv 1 \text{mod } 5$ → $y_2 \equiv 1 \text{mod } 5$ → $y_2 = 1$

$M_3 y_3 \equiv 1 mod \; m_3$ → $15y_3 \equiv 1 \text{mod } 7$ → $y_3 \equiv 1 \text{mod } 7$ → $y_3 = 1$

$x \equiv (2x35x2+3x21x1+2x15x1) mod 105 \equiv 233 mod 105 \equiv 23 mod 105$

QUESTIONS ?

Dr. Bertrand Cambou
Professor of Practice NAU, Cybersecurity
School of Informatics, Computing, and Cyber-Systems
Bertrand.cambou@nau.edu