CSE 431::Cryptography and Network Security

MD. ARSHAD WASIF

MSc. (appeared), BSc. In CSE from IUT

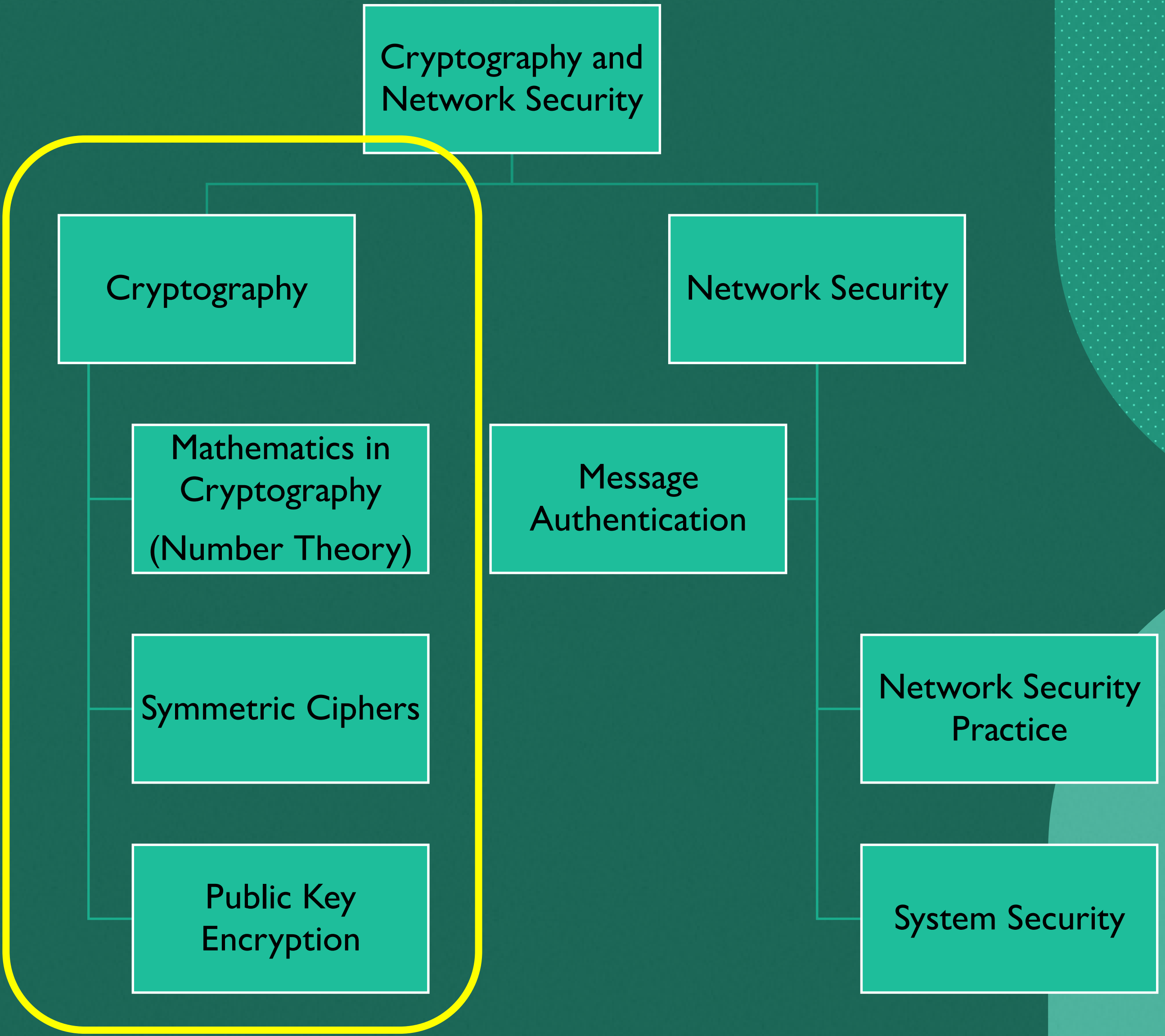
Varendra University, Rajshahi.

Course Contents

- Cryptography and Network Security
  - Cryptography
    - Mathematics in Cryptography (Number Theory)
    - Symmetric Ciphers
    - Public Key Encryption
  - Network Security
    - Message Authentication
    - Network Security Practice
    - System Security

Course Contents

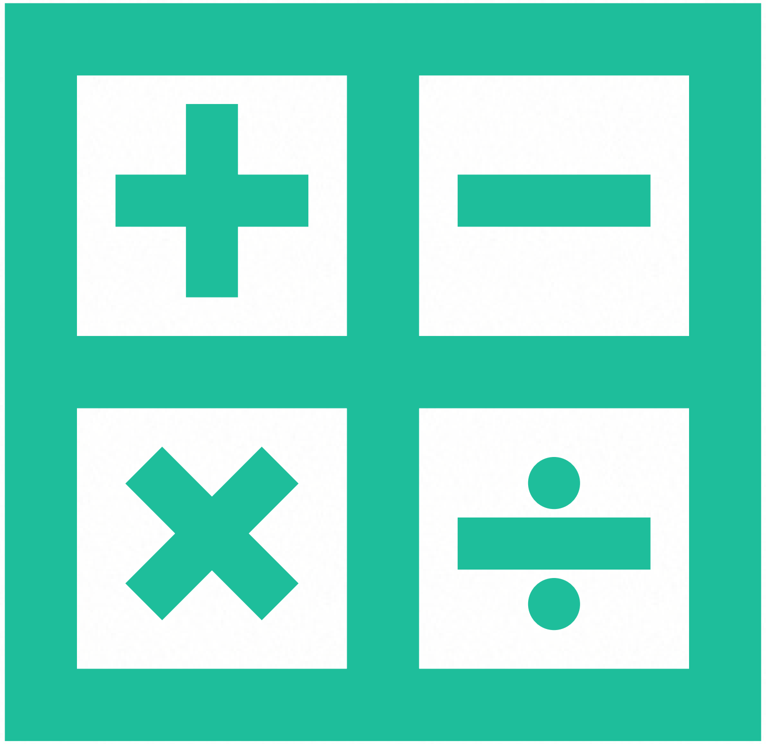
MID EXAM
SYLLABUS
MAR 18 – 31



Number Theory (Mathematics in Cryptography)

- Fields
- Algebraic Closures
- Integers
- Divisibility
- Primes
- Testing Primes
- Factorization
- Euclidean Algorithm

Page 45
Forouzan book



Symmetric Ciphers

- Symmetric Cipher Model,
- Substitution Techniques,
- Transposition Techniques,
- Steganography,
- Simplified DES,
- Block Cipher Principles,
- The Data Encryption Standard,
- The Strength of DES,
- Block Cipher Design Principles,
- Evaluation Criteria for AES,
- The AES Cipher, Triple DES, Blowfish, RC5
- Characteristics of Advanced Symmetric Block Ciphers,
- RC4 Stream Cipher, Placement of Encryption Function,
- Traffic Confidentiality,
- Key Distribution

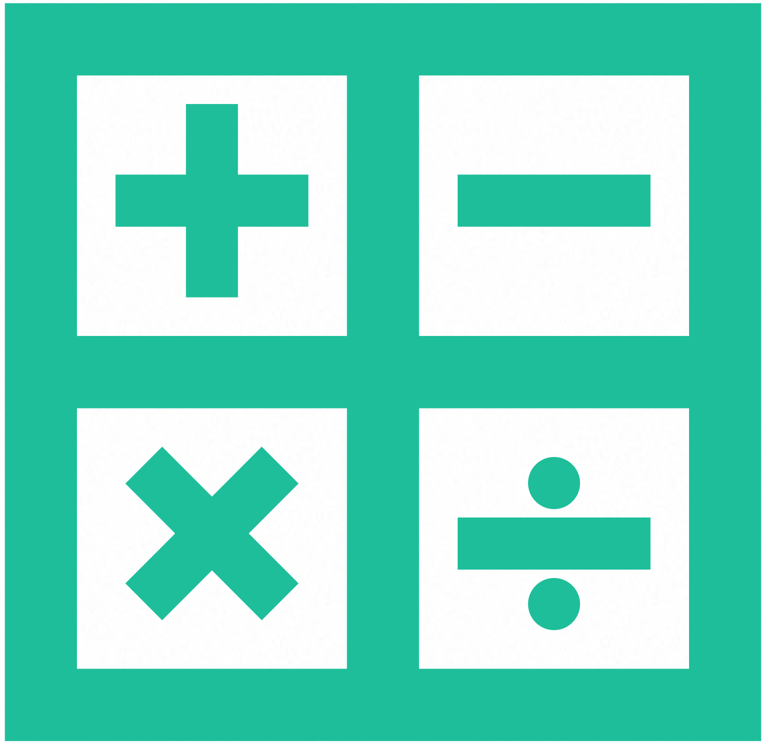
Public Key Encryption

- Principles of Public-Key Cryptosystems,
- The RSA Algorithm,
- Key Management

Number Theory (Mathematics in Cryptography) overview

- Fields
- Algebraic Closures
- Integers
- Divisibility
- Primes
- Testing Primes
- Factorization
- Euclidean Algorithm

Page 45
Forouzan book



FIELDS

- Arithmetic Operations: +, -, ×, ÷
- IF YOU CAN + and – it is a "GROUP" (a+b), (a-b)
- IF YOU CAN + – and × it is a "RING" (a+b), (a-b), a×b , b×a
- IF YOU CAN + – × and ÷ it is a "FIELD" (a+b), (a-b), a×b , b×a, a/b, b/a

❖ Terminology:
  - ❖ Subtract = Additive inverse
  - ❖ Divide = Multiplicative inverse

FIELDS

Sets	Elements	Commutative Groups under +	Multiplication × (rings)	Commutative rings (a.b = b.a)	Multiplicative Inverses (except 0)
Z	{…,-3,-2,-1,0,1,2,3,…}	✓	✓	✓	✗ Not integer
R(2×3)	$\begin{matrix} 1 & 2 & 3 \\ 5 & 9 & 0 \end{matrix}$	✓	✗	✗	✗
R(2×2)	$\begin{matrix} 1 & 2 \\ 5 & 0 \end{matrix}$	✓	✓	✗	✗
Q	$\{\frac{p}{q}\} :: \{\frac{2}{3}, \frac{6}{10}, \ldots\}$	✓	✓	✓	✓

FIELDS – formal Mathematical Definition

- A field(F) is a set of elements with two operations addition and multiplication. Under addition the elements are commutative group and under multiplication the non-zero elements are commutative group. Also, addition and multiplication are linked with distributive property.

<F,+> is a commutative group

<F,> is a commutative group

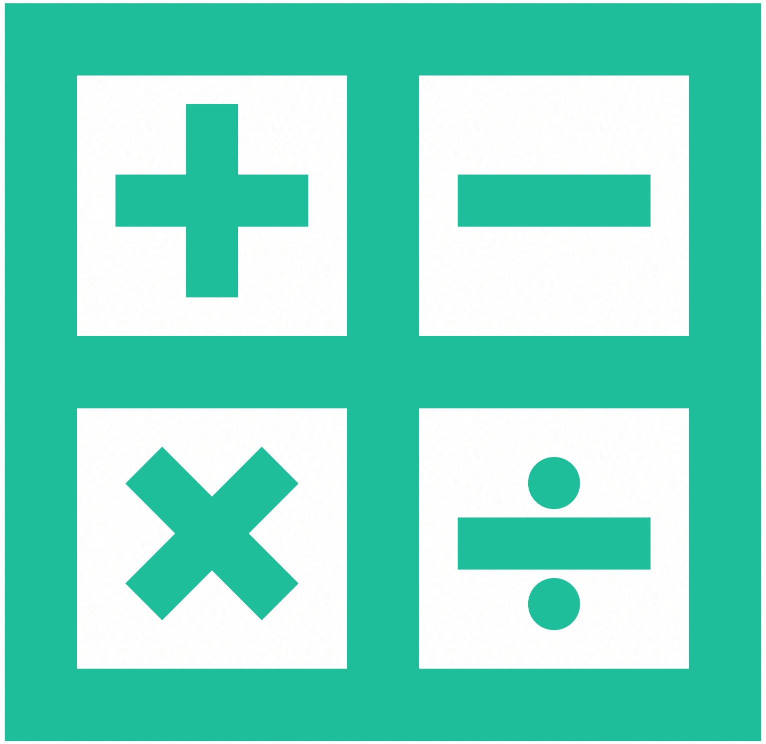
a.(b+c) = a.b + a.c

(b+c).a = b.a + c.a

Number Theory (Mathematics in Cryptography) overview

Page 45
Forouzan book

- Fields
- Algebraic Closures
- Integers
- Divisibility
- Primes
- Testing Primes
- Factorization
- Euclidean Algorithm



Divisibility

- A | B if and only if A%B = 0
- A ∤ B if A%B != 0

Property 1: if $a|1$, then $a = \pm 1$.
Property 2: if $a|b$ and $b|a$, then $a = \pm b$.
Property 3: if $a|b$ and $b|c$, then $a|c$.
Property 4: if $a|b$ and $a|c$, then $a|(m \times b + n \times c)$, where m and n are arbitrary integers.

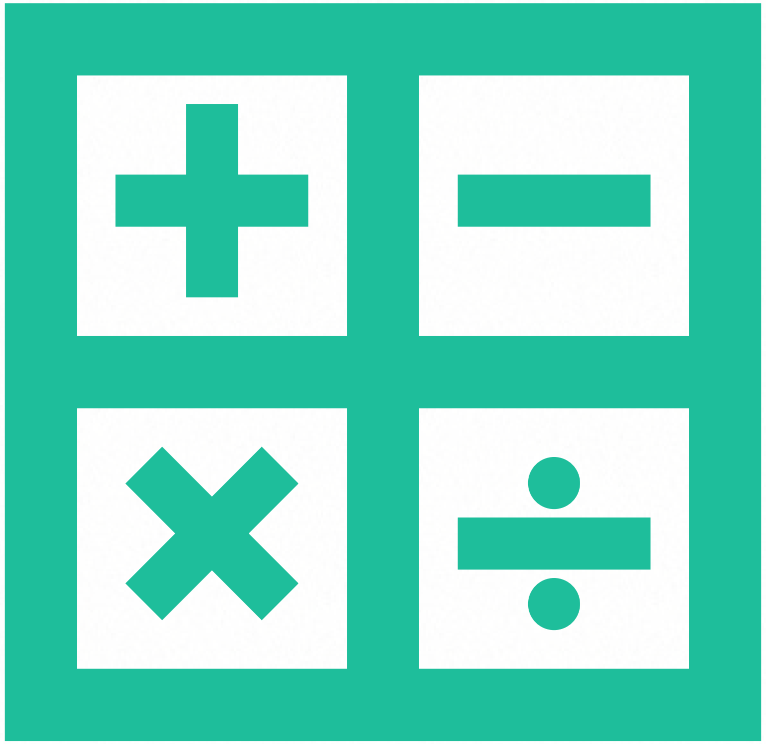
General rules of divisibility:

Number	Rules
2	Even number (x%2==0)
3	Sum(all digits)%3 == 0
4	Number(with last 2 digits)%4 ==0
5	Unit's digit 0, 5
6	X%2 && X%3
7	Only divisible to 7*n itself
9	X%3 && sum of digits%9
10	Unit's digit 0

Number Theory (Mathematics in Cryptography) overview

Page 45
Forouzan book

Fields	Algebraic Closures	Integers
Divisibility	Primes	Testing Primes
Factorization	Euclidean Algorithm	



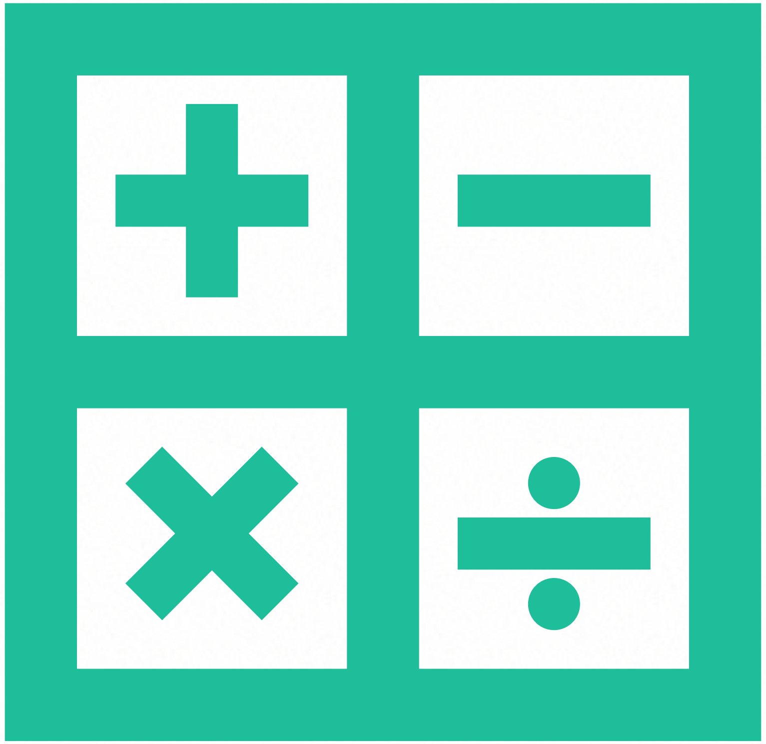
Prime Numbers and Finding them (Sieve of Eratosthenis)

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Number Theory (Mathematics in Cryptography) overview

Page 45
Forouzan book

- Fields
- Algebraic Closures
- Integers
- Divisibility
- Primes
- Testing Primes
- Factorization
- Euclidean Algorithm



Algebraic Closures

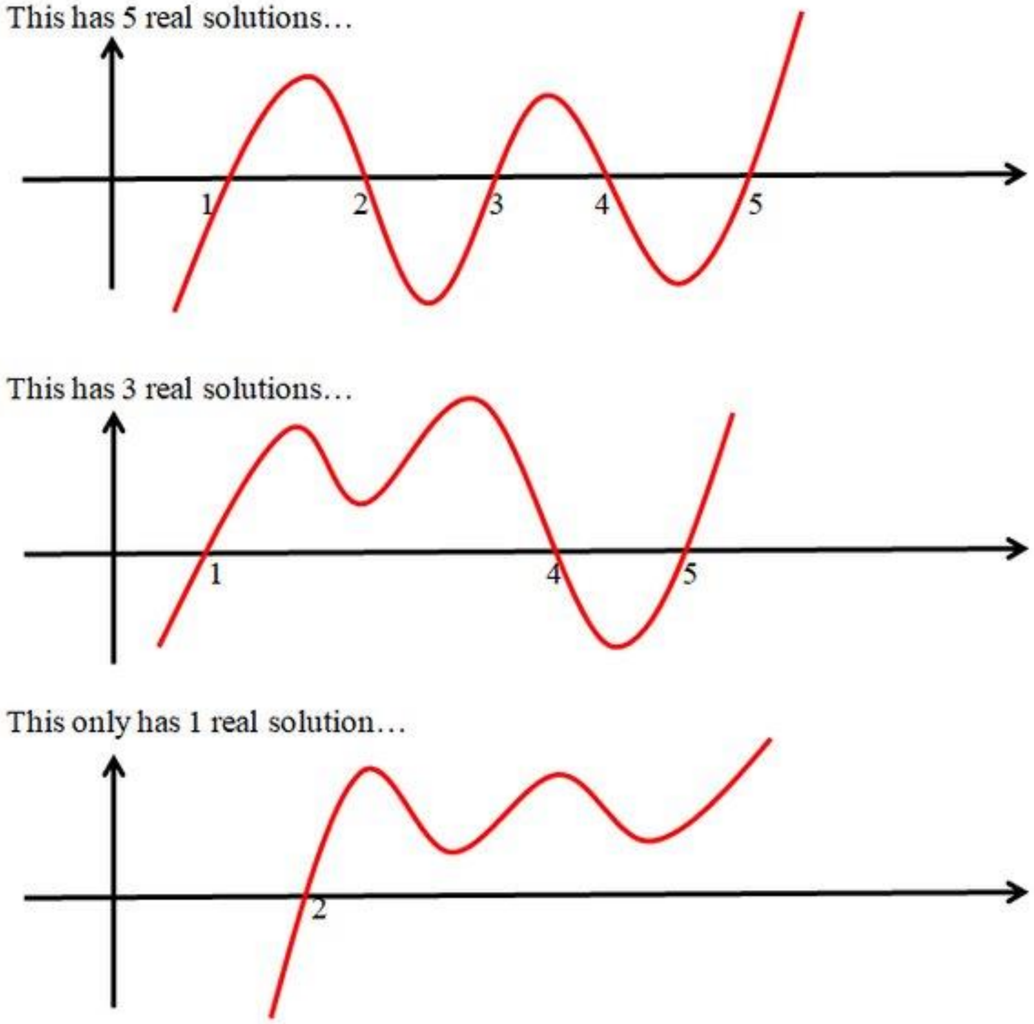
- A field K is called algebraically closed if every nonconstant polynomial f(x) ∈ K[x] has a root in K.

f(x) = a x^n + b $x^{n-1}. 1^1$ + c $x^{n-2}. 1^2$ + c $x^{n-2}. 1^2$ + … + 1^n

Has a root in K[x] then we call K as a closure $\overline{K}$.

Similarly, $\overline{K}$ has a closure in K.

Theorem: Every field F has an algebraic closure $\overline{F}$.



Number Theory (Mathematics in Cryptography) overview

Fields

Algebraic Closures

Integers

Divisibility

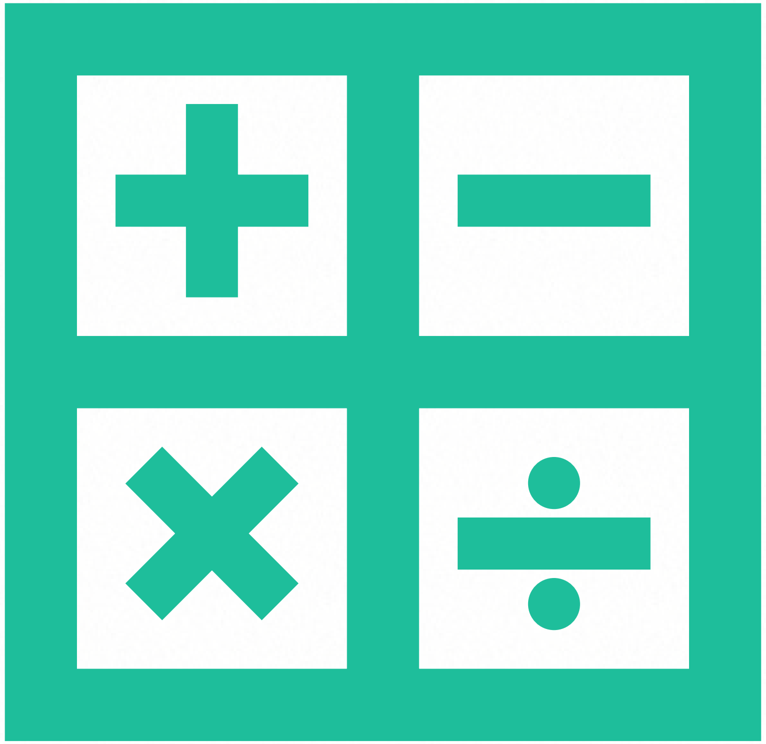
Primes

Testing Primes

Factorization

Euclidean Algorithm

Page 45
Forouzan book



Prime Power Factorization (PPF)

- If N is any positive integer, you can always write it down using factors of single/multiple prime(s).

$388 = 4 \times 97 = 2^2 \times 97^1$

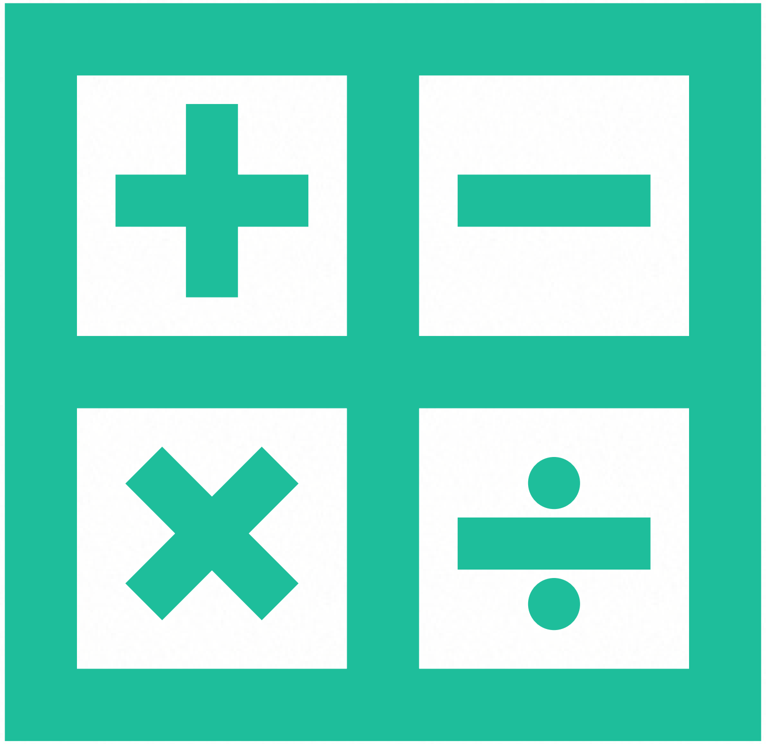
$$
\begin{aligned}
3880000 &= 4 \times 97 \times 10000 \\
&= 2^2 \times 97^1 \times 10^4 \\
&= 2^2 \times 97^1 \times (2\times5)^4 \\
&= 2^6 \times 5^4 \times 97^1
\end{aligned}
$$

How many distinct prime factors are there in number 5120?

Number Theory (Mathematics in Cryptography) overview

Page 45
Forouzan book

- Fields
- Algebraic Closures
- Integers
- Divisibility
- Primes
- Testing Primes
- Factorization
- Euclidean Algorithm



Euclidian Algorithm (A way of finding GCD)

- GCD = Greatest Common Divisor

gcd (36, 10) = gcd (10, 6) = gcd (6, 4) = gcd (4, 2) = gcd (2, 0) = 2

$$10 \,)\, 36 \,(\, 3$$
$$30$$
$$6 \,)\, 10 \,(\, 1$$
$$6$$
$$4 \,)\, 6 \,(\, 1$$
$$4$$
$$2 \,)\, 4 \,(\, 2$$
$$4$$
$$0$$