COMP8760 Lecture - 4

Lagrange's Theorem, Fermat's Theorem, Primality Testing, Contrapositivity

Sanjay Bhattacharjee

University of Kent

gmkgcm

Study Material

Book 1	*Cryptography Made Simple*
Author	Nigel P. Smart.
	Link to eBook

Section 1.1.1 Groups
Section 1.1.3 Euler's Functions
Section 1.1.5 The Set $\mathbb{Z}_N^\star$
Section 2.1.1 The Prime Number Theorem
Section 2.1.2 Trial Division
Section 2.1.3 Fermat's Test

$\mathbb{Z}_{12} = \{0, 1, 2, 3, \ldots, 11\}$

For $a, b \in \mathbb{Z}_{12}$, the following table shows all possible $a \times b = a \cdot b$ (except 0's)

(We use the notations $\times$ and $\cdot$ interchangeably to denote multiplication.)

a	1	2	3	4	5	6	7	8	9	10	11
b											
1	1	2	3	4	5	6	7	8	9	10	11
2	2	4	6	8	10	0	2	4	6	8	10
3	3	6	9	0	3	6	9	0	3	6	9
4	4	8	0	4	8	0	4	8	0	4	8
5	5	10	3	8	1	6	11	4	9	2	7
6	6	0	6	0	6	0	6	0	6	0	6
7	7	2	9	4	11	6	1	8	3	10	5
8	8	4	0	8	4	0	8	4	0	8	4
9	9	6	3	0	9	6	3	0	9	6	3
10	10	8	6	4	2	0	10	8	6	4	2
11	11	10	9	8	7	6	5	4	3	2	1

Note that the rows of $\mathbb{Z}_{12}^{\star} = \{1, 5, 7, 11\}$ have the element 1 but no 0, while the other rows have 0 but not 1.

- Row b has 0 when $\gcd(b, 12) > 1$
- Row b has 1 when $\gcd(b, 12) = 1$

$\mathbb{Z}_{12}^{\star} = \{1, 5, 7, 11\}$

So,

a / b	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11
2	2	4	6	8	10	0	2	4	6	8	10
3	3	6	9	0	3	6	9	0	3	6	9
4	4	8	0	4	8	0	4	8	0	4	8
5	5	10	3	8	1	6	11	4	9	2	7
6	6	0	6	0	6	0	6	0	6	0	6
7	7	2	9	4	11	6	1	8	3	10	5
8	8	4	0	8	4	0	8	4	0	8	4
9	9	6	3	0	9	6	3	0	9	6	3
10	10	8	6	4	2	0	10	8	6	4	2
11	11	10	9	8	7	6	5	4	3	2	1

- $\mathbb{Z}_{12}^{\star}$ is the set of elements in $\mathbb{Z}_{12}$ that are mutually prime with 12. In other words, for all $a \in \mathbb{Z}_{12}^{\star}$,

$$\gcd(a, 12) = 1.$$

- Note that only if $a \in \mathbb{Z}_{12}^{\star}$, then there is a solution to the equation

$$a \cdot x = 1.$$

In other words, only elements in $\{1, 5, 7, 11\}$ have multiplicative inverses!

$\mathbb{Z}_{13}^{\star} = \{1, 2, 3, \ldots, 12\}$

Here,

a \ b	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	4	6	8	10	12	1	3	5	7	9	11
3	3	6	9	12	2	5	8	11	1	4	7	10
4	4	8	12	3	7	11	2	6	10	1	5	9
5	5	10	2	7	12	4	9	1	6	11	3	8
6	6	12	5	11	4	10	3	9	2	8	1	7
7	7	1	8	2	9	3	10	4	11	5	12	6
8	8	3	11	6	1	9	4	12	7	2	10	5
9	9	5	1	10	6	2	11	7	3	12	8	4
10	10	7	4	1	11	8	5	2	12	9	6	3
11	11	9	7	5	3	1	12	10	8	6	4	2
12	12	11	10	9	8	7	6	5	4	3	2	1

- All positive integers between 1 and 12 are mutually prime with 13. In other words, for all $a \in \mathbb{Z}_{13}^{\star}$,
$$\gcd(a, 13) = 1.$$
- All elements in $\{1, 2, \ldots, 12\}$ have multiplicative inverses!

$\mathbb{Z}_N^\star$ is a Multiplicative Abelian Group

It satisfies the following properties with respect to modular multiplication.

- **Closure**:
  For any two elements $x, y \in \mathbb{Z}_N^\star$,
  $$x \cdot y \in \mathbb{Z}_N^\star$$
- **Associativity**:
  For any three elements $x, y, z \in \mathbb{Z}_N^\star$,
  $$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$
- **Identity**:
  The element $1 \in \mathbb{Z}_N^\star$ is the identity such that, for all $x \in \mathbb{Z}_N^\star$,
  $$x \cdot 1 = x$$
- **Inverse**:
  For any element $x \in \mathbb{Z}_N^\star$, there is a unique $\bar{x} \in \mathbb{Z}_N^\star$ such that,
  $$x \cdot \bar{x} = 1$$
- **Commutativity**:
  For any two elements $x, y \in \mathbb{Z}_N^\star$,
  $$x \cdot y = y \cdot x$$

Group: $(\underbrace{\mathbb{Z}_{11}^{\star}}_{\text{The set}}, \underbrace{\times \pmod{11}}_{\text{The operation}})$

where the set $\mathbb{Z}_{11}^{\star} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

- Closure:
  For any two elements $x, y \in \mathbb{Z}_{11}^{\star}$, $x \times y \pmod{11} \in \mathbb{Z}_{11}^{\star}$.
  Examples:
  $$3 \times 2 = 6 \pmod{11} \in \mathbb{Z}_{11}^{\star}.$$
  $$3 \times 4 = 1 \pmod{11} \in \mathbb{Z}_{11}^{\star}.$$
  $$9 \times 3 = 5 \pmod{11} \in \mathbb{Z}_{11}^{\star}.$$
  $$9 \times 1 = 9 \pmod{11} \in \mathbb{Z}_{11}^{\star}.$$
- Associativity:
  For any three elements $x, y, z \in \mathbb{Z}_{11}^{\star}$, $x \times (y \times z) \pmod{11} = (x \times y) \times z \pmod{11}$.
  Examples:
  $$1 \times (2 \times 3) \pmod{11} = (1 \times 2) \times 3 \pmod{11}.$$
  $$9 \times (8 \times 7) \pmod{11} = (9 \times 8) \times 7 \pmod{11}.$$
  $$1 \times (7 \times 8) \pmod{11} = (1 \times 7) \times 8 \pmod{11}.$$
  $$0 \times (7 \times 8) \pmod{11} = (0 \times 7) \times 8 \pmod{11}.$$

Group: $(\underbrace{\mathbb{Z}_{11}^{\star}}_{\text{The set}}, \underbrace{\times \pmod{11}}_{\text{The operation}})$

$(\underbrace{\mathbb{Z}_{11}^{\star}}_{\text{The set}}, \underbrace{\times \pmod{11}}_{\text{The operation}})$ satisfies all four properties and hence is a group.

- Identity:
  The element $1 \in \mathbb{Z}_{11}^{\star}$ is unique. For all $x \in \mathbb{Z}_{11}^{\star}$, $x \times 1 \pmod{11} = x$.

$$0 \times 1 \pmod{11} = 0.$$

$$1 \times 1 \pmod{11} = 1.$$

$$\vdots$$

$$9 \times 1 \pmod{11} = 9.$$

- Inverse:
  For any element $x \in \mathbb{Z}_{11}^{\star}$, there is a unique $\bar{x} \in \mathbb{Z}_{11}^{\star}$ such that, $x \times \bar{x} \pmod{11} = 1$. Examples:

$$3 \times 7 \pmod{11} = 1.$$

$$4 \times 6 \pmod{11} = 1.$$

$$5 \times 5 \pmod{11} = 1.$$

gmkgcm

University of Kent

$\phi(N)$ elements in $\mathbb{Z}_N^\star$

We note here that,

The group $\mathbb{Z}_N^\star$ has all elements of $\mathbb{Z}_N$
that are mutually prime to N.

We recollect here that,

$\phi(N)$ is the number of integers between 1 and N
that are mutually prime to N.

In other words,

$$|\mathbb{Z}_N^\star| = \phi(N).$$

gmkgcm

University of Kent

Lagrange's Theorem

Theorem

For any $a \in G$,

$$a^{|G|} = 1.$$

Corollary

We apply this Theorem to the group $\mathbb{Z}_N^\star$.

For any $a \in \mathbb{Z}_N^\star$,

$$a^{\phi(N)} = 1.$$

Fermat's Little Theorem

Theorem

Let p be a prime number and a be an integer. Then,

$$a^p = a \mod p.$$

Proof Idea.

In Lagrange's Theorem, consider the group $(Z_p^\star = \{1, 2, \ldots, p-1\}$.
For any $a \in \mathbb{Z}_p^\star$,

$$a^{p-1} = 1 \mod p.$$

And hence,

$$a^p = a \mod p.$$

Prime Numbers

Definition:

A positive integer p is prime if it is only divisible by 1 and p.

Some prime numbers:

- $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$

The Prime Number Theorem

Conjectured by Gauss (in early 1800s):

Let $\pi(X)$ be the function that counts the number of primes less than X.
We have the approximation

$$\pi(X) \approx \frac{X}{\log_e X}.$$

Primes are quite common

Example: Number of primes less than 2^{16} is

$$\underbrace{\approx}_{\text{approximately}} \frac{2^{16}}{\log_e(2^{16})} = \frac{2^{16}}{\log_2(2^{16}) / \log_2 e} \approx \frac{2^{16}}{16} = \frac{2^{16}}{2^4} = 2^{12}.$$

Example: Number of primes less than 2^{1024} is

$$\approx \frac{2^{1024}}{\log_e(2^{1024})} = \frac{2^{1024}}{\log_2(2^{1024}) / \log_2 e} \approx \frac{2^{1024}}{1024} = \frac{2^{1024}}{2^{10}} = 2^{1014}.$$

Choose a Random Number: Is it Prime?

Probability

If a number is chosen at random from $\{1, \ldots X\}$,
the probability that it will be a prime is approximately:

$$\approx \frac{\pi(X)}{X}.$$

Probability for $X = 2^{1024}$

If a 1024-bit number (between $0, \ldots, 2^{1024} - 1$) is chosen at random,
the probability that it will be a prime is approximately:

$$\approx \frac{\pi(2^{1024})}{2^{1024}} = \frac{\left(\frac{2^{1024}}{\log_e 2^{1024}}\right)}{2^{1024}}$$

$$= \frac{1}{\log_e(2^{1024})} = \frac{1}{(\log_2 2^{1024} / \log_2 e)} = \frac{1}{709}$$

Generate 1024-bit random numbers.

How many have to be generated to get a prime?
One out of 709 will be a prime!

Primality Testing

But how do we test if a randomly generated number n is prime or not?

Trial Division

Exhaustive Search

- For each $2 \leq d \leq \sqrt{n}$
  - if $n \mod d = 0$, then n is not a prime;
    hence, break the loop
- if the above loop was not broken, then n is a prime

When p is not a prime, the value of d (the least factor) will be
the certificate of compositeness!

If n is prime, there is no certificate of primality!
To verify, one has to run the test once again!

Partial Trial Division

Search till a bound Y

- For each $2 \leq d \leq Y$
  - if $n \mod d = 0$, then n is not a prime;
    hence, break the loop
- if the above loop was not broken, then n is a prime

Eliminating Composites

Let $\{2, 3, \dots, p_k\}$ be the set of all prime numbers less than Y.
Partial Trial Division will eliminate all but

$$\prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

fraction of composites.

For all $p_i < 100$, we have $\prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) \approx 0.12$

Recall: Lagrange's Theorem

Theorem

For any $a \in G$,

$$a^{|G|} = 1.$$

Corollary

We apply this Theorem to the group $\mathbb{Z}_N^\star$.

For any $a \in \mathbb{Z}_N^\star$,

$$a^{\phi(N)} = 1.$$

Recall: Fermat's Little Theorem

Theorem

Let p be a prime number and a be an integer. Then,

$$a^p = a \mod p.$$

Proof Idea.

In Lagrange's Theorem, consider the group $\mathbb{Z}_p^\star = \{1, 2, \ldots, p-1\}$.
For any $a \in \mathbb{Z}_p^\star$,

$$a^{p-1} = 1 \mod p.$$

And hence,

$$a^p = a \mod p.$$

Fermat's Test

$$a^{n-1} \mod n.$$

If the n is prime, then value is 1.

This implies (by contrapositivity):

if the value is not 1, then n is composite.

If the value is 1, then n is prime (with high probability).

The Test for n:

for i=0 to k-1 do

    Pick $a \in [2, \ldots, n-1]$

    $b \leftarrow a^{n-1} \mod n$

    if $b \neq 1$, return (Composite, a)

return "Probably Prime"

gmkgcm

University of Kent

Fermat's Test

The Test for n:

```
for i=0 to k-1 do
    Pick a ∈ [2, ..., n − 1]
    b ← a^(n−1) mod n
    if b ≠ 1, return (Composite, a)
return "Probably Prime"
```

Properties:

- a is the "witness of compositeness"
- Very efficient (fast)
- No proof of primality
  As the value of k is increased, there is increased probability that n is indeed a prime.

Carmichael Numbers: Failure of Fermat's Test

Carmichael Numbers

Composite numbers for which the Fermat Test will always output
"Probably Prime"
for every a coprime to n.

Properties:

- Always odd
- At least three prime factors
- Square free
- If p divides n, then $p - 1$ divides $n - 1$
- The first three are 561, 1105 and 1729.
- Rare but infinitely many!

Contrapositive Argument

Consider the function B() below with A() as a subroutine:

```
B(){
    ··· (little computation)
    A();
    ··· (little computation)
    A();
    ··· (little computation)
}
```

Statement $\mathcal{A}$: algorithm A runs in polynomial time (is efficient)
Statement $\mathcal{B}$: algorithm B runs in polynomial time (is efficient)

If algorithm A runs in polynomial time, then algorithm B runs in polynomial time.
If $\mathcal{A}$, then $\mathcal{B}$.

$\iff$ (is equivalent to)

If algorithm B is not polynomial time, then algorithm A is not polynomial time.
If $\neg\mathcal{B}$, then $\neg A$

Contrapositivity

$\mathcal{A}$	$\mathcal{B}$	If $\mathcal{A}$, then $\mathcal{B}$
T	T	T
T	F	F
F	T	T
F	F	T

$\mathcal{A}$	$\mathcal{B}$	If $\mathcal{A}$, then $\mathcal{B}$	$\neg A$	$\neg B$	If $\neg\mathcal{B}$, then $\neg A$
T	T	T	F	F	T
T	F	F	F	T	F
F	T	T	T	F	T
F	F	T	T	T	T

Truth values of equivalent statements are the same for all value assignments. Hence, they are equivalent:

$$\text{If } \mathcal{A}, \text{ then } \mathcal{B} \iff \text{If } \neg\mathcal{B}, \text{ then } \neg A.$$

Example:

$\mathcal{A}$: there is a smoke
$\mathcal{B}$: there is fire

If there is smoke, then there must be a fire.

If there is no fire, then there can be no smoke.

Example:

$\mathcal{A}$: there is a shadow
$\mathcal{B}$: there is light

If there is a shadow, then there must be a light.

If there is no light, then there can not be a shadow.

Example:

$\mathcal{A}$: rain in the past 5 minutes
$\mathcal{B}$: wet streets

If it has rained in the past 5 minutes, then the streets must be wet.

If the streets are not wet, then it has not rained in the past 5 minutes.

Thank you for your kind attention!

gmkgcm

University of Kent