Lecture 25   12/3/2025

Primality Testing

Given an integer N, check if N is a prime number.

Note that the representation size is $\log N$ bits. So an efficient algorithm $\Rightarrow$ runs in $\text{poly}(\log N)$ time.

$$\text{PRIMES} = \{ x \in \{0,1\}^* \mid x \text{ interpreted as a binary integer is prime} \}.$$

$$\text{COMPOSITE} = \{0,1\}^* - \text{PRIMES}$$

It is easy to see that COMPOSITE is in NP since one can prove that N is COMPOSITE by exhibiting x, y such that

$$N = x y.$$

Not obvious that PRIMES is in NP. Vaughn Pratt in 1975 showed that PRIMES is in NP.

Is there a poly-time algorithm to check if N is a prime?

It had to wait till 2002 for a deterministic poly-time algorithm due to Agarwal, Kayal and Saxena. However a randomized poly-time algorithm was known since 1977 due to Solovay and Strassen and Miller and Rabin.

We need some number theoretic and group theoretic background.

<u>Claim:</u> Given non-negative integers a, k, n can compute $a^k \bmod n$ efficiently.

<u>Proof:</u> Exercise.

Background

Given integers $a, b > 0$, Euclid's algorithm can be used to obtain the following.

Theorem: Given integers $a, b > 0$ $\exists$ integers x, y such that $\gcd(a,b) = xa + yb$. Moreover, x, y can be computed in poly-time.

Let $n > 0$ be a positive integer.

$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ defines an additive abelian group under the operation $+$ mod n.

Let $\mathbb{Z}_n^* = \{ a \mid 0 < a < m, \gcd(a,n) = 1 \}$

be the set of numbers that are relatively prime to n and in $\mathbb{Z}_n$.

Claim: $\mathbb{Z}_n^*$ is a group under multiplication mod n.

Proof: Recall Euclid's gcd algorithm.
Given a, b it returns $\gcd(a,b)$.
Can be implemented to run in poly-time.
As a by product it also returns
x, y such that

$$xa + yb = \gcd(a,b).$$

Now consider $a \in \mathbb{Z}_n^*$ and $b = n$

$\Rightarrow \exists\ x, y$ such that

$xa + yn = 1$.

$\Rightarrow \quad xa = 1 \mod n$.

$\Rightarrow$ $x \mod n$ is a candidate for the inverse of a in $\mathbb{Z}_n^*$

Cannot have $x_1 \neq x_2$ such that

$x_1 a = 1$ and $x_2 a = 1 \mod n$

because $(x_1 - x_2) a = 0 \mod n$

but $\gcd(a, n) = 1 \Rightarrow x_1 = x_2$. 17.

Corollary: $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ is a group. $\Rightarrow$ $\mathbb{Z}_p$ is a field.

Remark: Proof also shows that given $a \in \mathbb{Z}_n^*$ one can find a^{-1} efficiently.

Defn: Euler totient function

$\phi(m)$ for integer $m > 0$ is

$= |\mathbb{Z}_m^*|$.

Properties of ϕ.

- $\phi(1) = 1$
- For prime p $\phi(p) = p-1$
- For prime p and $k > 0$ $\phi(p^k) = p^{k-1}(p-1)$
- For relatively prime #s n, m

  $\phi(nm) = \phi(n)\phi(m)$.

Via above properties

Theorem: If n has prime factorization $p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ then

$$\phi(n) = \prod_{i=1}^{t} p_i^{k_i - 1}(p_i - 1)$$

Theorem: [Lagrange]
Let G be a finite group and let $H \subseteq G$ be a subgroup. Then $|H|$ divides $|G|$.

Defn: A group G is cyclic if $\exists$ an element $g \in G$ such that $\forall\, a \in G$ $\exists$ integer k such that $g^k = a$. g is called a generator for the group.

Defn: Given group G and $a \in G$ order(a) is smallest integer k such that $g^k = 1$.
identity

For any $a \in G$ $H_a = \{1, a, a^2, \ldots, a^{ord(a)}\}$

forms a cyclic subgroup of G.

Therefore we have $ord(a)$ divides $|G|$ $\forall a \in G$.

This implies

<u>Theorem</u> [Euler] For any $a \in \mathbb{Z}_m^*$

$$a^{\varphi(m)} \equiv 1 \mod m.$$

<u>Corollary</u>: [Fermat] For any prime p,

$$a^{p-1} \equiv 1 \mod p \text{ (or } a^p \equiv a \mod p).$$

Another useful lemma.

<u>Lemma</u>: For any $n > 0$ $\sum_{d|n} \varphi(d) = n$.

Proof: Consider integer $d \in \{1, 2, \ldots, n\}$.

Let $A_d = \{1 \le x \le n \mid \gcd(x, n) = d\}$.

$A_d = \{\}$ if d is <u>not</u> a divisor of n.

A_d, $d = \{1, 2, \ldots, n\}$ partition $\{1, 2, \ldots, n\}$

Hence $\sum\limits_{d} |A_d| = n$.

Not difficult to see $|A_d| = \varphi\left(\frac{n}{d}\right)$.

Hence $\sum\limits_{d|n} \varphi(d) = \sum\limits_{d|n} \varphi\left(\frac{n}{d}\right) = \sum\limits_{d|n} |A_d|$

$= n$.

$\square$.

It is easy to see that $\mathbb{Z}_n$ for any n is cyclic. However $\mathbb{Z}_n^*$ need not be cyclic in general.

However

<u>Theorem</u>: Let p be prime. Then $\mathbb{Z}_p^*$ is cyclic.

<u>Proof</u>: Recall $|\mathbb{Z}_p^*| = p-1$.
For $k \mid p-1$ let $O_k = \{ j \in \mathbb{Z}_p^* \mid \text{ord}(j) = k \}$ be the set of elements with order k.
From previous lemma $\sum_{k \mid p-1} \varphi(k) = p-1$.
We will show later that $|O_k| = 0$ or $\varphi(k)$.

$$\Rightarrow \sum_{k} |O_k| = \sum_{k \mid p-1} \varphi(k) = p-1$$

and $|O_k| = \varphi(k) \ \forall\, k \mid p-1$.

$$\Rightarrow |O_{p-1}| = \varphi(p-1) \geq 1 \text{ for } p > 2.$$

<u>Claim</u>: $|O_k| = 0$ or $\varphi(k)$.

All elements in O_k are roots of the polynomial $X^k \equiv 1 \mod p$ over the <u>field</u> $\mathbb{Z}_p$. Suppose $O_k \neq \{\}$. Then $\exists$ a root r for the above polynomial and further all the roots are $\{r^0, r^1, \ldots, r^{k-1}\}$ since these are distinct (order$(r) = k$). Note that $r^l \in O_k$ iff $\gcd(l, k) = 1$.

Thus $|O_k| = \varphi(k)$ if $O_k \neq \{\}$. $\square$

A number theoretic theorem.

<u>Theorem:</u> $\mathbb{Z}_n^*$ is cyclic iff $n = 1, 2, 4,$ p^k or $2p^k$ for integer k and odd prime p.

Chinese Remainder Theorem

Theorem: Let $n = n_1 n_2 \cdots n_k$ where $n_1, n_2, \ldots, n_k$ are pairwise coprime (ie $\gcd(n_i, n_j) = 1 \;\forall i \neq j$). For any sequence $r_1, r_2, \ldots, r_k$ where $r_i \in \mathbb{Z}_{n_i}$ there exists a unique $r \in \mathbb{Z}_n$ s.t.

$$r = r_i \mod n_i \quad \text{for } i = 1 \text{ to } k.$$

Moreover given $r_1, \ldots, r_k$, r can be computed efficiently.

Proof: First we consider showing one r exists. Since $\frac{n}{n_i}$ is coprime to n_i $\exists$ a multiplicative inverse m_i in $\mathbb{Z}_{n_i}^*$ for it. Let m_i be that inverse.

$$\Rightarrow \quad m_i \frac{n}{n_i} \equiv 1 \mod n_i .$$

also $m_i \dfrac{n}{n_i} \equiv 0 \mod n_j \quad j \neq i$

Thus $r = \displaystyle\sum_{i=1}^{k} r_i m_i \frac{n}{n_i} \mod (n)$

satisfies the desired congruences.

To see uniqueness, we do counting argument. How many distinct $r_1, r_2, \ldots, r_k$ are there? $n_1 n_2 \cdots n_k = n$.

For each $\exists$ an $r \in \mathbb{Z}_n$ but there are only n elements in $\mathbb{Z}_n$ and for a given r we have only one $r_1\ r_2 \ldots r_k$.

D.

$\Rightarrow$ $\mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \cdots \times \mathbb{Z}_{n_k}$.

Quadratic residues

Defn: A residue $a \in \mathbb{Z}_m^*$ is a quadratic residue if $\exists$ a number x such that $x^2 \equiv a \bmod m$.

In other words a is a quadratic residue if it has a square root.

Lemma: Let p be ~~a~~ prime and consider generator g for $\mathbb{Z}_p^*$. Then g^k is a quadratic residue iff k is even.

Proof: It is easy to see that if k is even then $g^{\frac{k}{2}}$ is a square root of g^k. Suppose k is odd. If g^k is a quadratic residue then $g^k = x^2 = g^{2l}$ for some l since g is a generator. □.

[Euler]

<u>Corollary</u>: For $a \in \mathbb{Z}_p^*$, a is a quadratic residue iff $a^{\frac{p-1}{2}} \equiv 1 \mod p$.

<u>Proof:</u> $a = g^{2l}$ where g is a generator. $a^{\frac{p-1}{2}} = g^{l(p-1)} = (g^{p-1})^l \equiv 1$.

□

For a generator g, $g^{\frac{p-1}{2}} \equiv -1 \mod p$.

<u>Defn:</u> Legendre Symbol. For prime p and $a \in \mathbb{Z}_p^*$ we define $\left[\frac{a}{p}\right]$ where

$$\left[\frac{a}{p}\right] = \begin{cases} +1 & \text{if } a \text{ is quadratic residue} \\ -1 & \text{if } a \text{ is not a quadratic residue.} \end{cases}$$

Equivalently $a^{\frac{p-1}{2}} \bmod p$ where we interpret $p-1$ as -1.

Now we consider a not-necessarily prime ~~nu~~ number.

<u>Definition</u> [Jacobi Symbol] Let n be an odd number with prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_h^{k_h}$. For $a \in \mathbb{Z}_n^*$

$$\left[\frac{a}{n}\right] = \prod_{i=1}^{h} \left[\frac{a}{p_i}\right]^{k_i}.$$

Note that $\left[\frac{a}{n}\right]$ is the same as the Legendre symbol when n is odd prime. It is also ± 1.

Even though the definition of the Jacobi symbol involves the prime factorization, given a, n one can compute $\left[\frac{a}{n}\right]$ in poly-time.

Theorem: Given a, n when n is odd and $\gcd(a, n) = 1$ there is poly-time alg to compute $\left[\frac{a}{n}\right]$.

One can derive the above from

properties of the Jacobi symbol.

From Motwani Raghavan.

Theorem 14.29: *The Jacobi symbol satisfies the following properties whenever it is defined for the specified arguments. Using these, a polynomial time algorithm can be devised for computing the Jacobi symbol, given only a and n.*

1. $\left[\frac{ab}{n}\right] = \left[\frac{a}{n}\right]\left[\frac{b}{n}\right]$.

2. For $a \equiv b \pmod{n}$, $\left[\frac{a}{n}\right] = \left[\frac{b}{n}\right]$.

3. For odd coprimes a and n, $\left[\frac{a}{n}\right] = (-1)^{\frac{a-1}{2}\frac{n-1}{2}}\left[\frac{n}{a}\right]$.

4. $\left[\frac{1}{n}\right] = 1$.

5. $\left[\frac{2}{n}\right] = \begin{cases} -1 & \text{for } n \equiv 3 \text{ or } 5 \pmod 8 \\ 1 & \text{for } n \equiv 1 \text{ or } 7 \pmod 8 \end{cases}$

Defn: For an odd number n define

$$J_n = \left\{ a \in \mathbb{Z}_n^* \;\middle|\; \left[\frac{a}{n}\right] = a^{\frac{n-1}{2}} \bmod n \right\}$$

Note that $|J_n| = |\mathbb{Z}_n^*|$ when n is prime.

A key observation is that

Lemma: J_n is a subgroup of $\mathbb{Z}_n^*$ and is a proper subgroup if n is composite. Hence if n is composite $|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$.

The preceding observation leads to first RP-algorithm for compositeness due to Solovay and Strassen.

Alg: input $n > 2$

- If n is even output "Composite"
- Pick a random $a \in \{1, 2, .., n-1\}$
- If $\gcd(a, n) \neq 1$ output "Composite"
- Compute $a^{\frac{n-1}{2}} \bmod n$
- Compute $\left[\frac{a}{n}\right]$

- If $\left[\frac{a}{n}\right] \neq a^{\frac{n-1}{2}} \bmod n$ then output "Composite".

- Else
  Output "PRIME".

It is clear that algorithm outputs prime for a prime but for a composite it will err with prob $\frac{1}{2}$.

<u>Theorem</u>: COMPOSITE $\in$ RP.

By repeating we can reduce the error.

Miller-Rabin Test

We will assume n is odd and ≥ 5.

Simplest randomized test is to pick a number $a \in \{2, .., n-2\}$ and

check if $\gcd(a, n) \neq 1$.

Test will succeed with prob $1 - \frac{\varphi(n)}{n}$

but we can have $\frac{\varphi(n)}{n} \to 1$.

For instance $n = pq$ where p, q are prime. then $\varphi(n) = (p-1)(q-1)$.

So we need some property

Fermat Test

- Pick $a \in \{2, \ldots, n-2\}$ randomly
- if $(a^{n-1} \not\equiv 1 \mod n)$ output

Composite

else

prime.

If n is prime then correctly says it is prime and if it says it is composite then it is correct but it may say prime even when n is composite.

What is the probability?

Let $F_n = \{ a \in \mathbb{Z}_n^* \mid a^{n-1} \equiv 1 \mod n \}$

<u>Claim:</u> F_n is a subgroup of $\mathbb{Z}_n^*$.

<u>Proof:</u> If $a, b \in F_n$ $ab \in F_n$.

Also a^{n-2} is inverse of a and $a^{n-2} \in F_n$.

17.

Suppose F_n is a <u>proper</u> subgroup of $\mathbb{Z}_n^*$.

Then $\dfrac{|F_n|}{|\mathbb{Z}_n^*|} \leq \dfrac{1}{2}$ by Lagrange's theorem.

And algorithm will have constant probability of success.

But: what if $F_n = \mathbb{Z}_n^*$?

Are there any such composite #s?

Yes they are called <u>Carmichael</u> #s.

There are infinitely many.

Smallest is $561 = 3 \cdot 11 \cdot 17$.

Thus we need a test that handles Carmichael numbers.

Another property of primes is that $\mathbb{Z}_p^*$ is a field and

$x^2 - 1 = 0$ has only two roots

± 1 $\quad +1 = 1$ and $-1 \equiv p-1$..

If n is composite then there can be non-trivial square roots. Ex $n = 91$ then $1, 27, 60, 90$ are all square roots of 1. If we find a non-trivial square of 1 mod n then n is composite.

If $n = pq$ then by CRT only

4 non-trivial square roots.

Euler Test:

Pick $a \in_R \{2, \dots, n-2\}$.

if $a^{\frac{n-1}{2}} \equiv \pm 1 \mod n$. output

prime

else

composite.

At least as good as Fermat test.

But why only $a^{\frac{n-1}{2}}$ and not $a^{\frac{n-1}{4}}$?

First $\frac{n-1}{2}$ may not be even but if

it is then we can try.

Rabin-Miller Test

Assume n is odd

Write $n = 2^u k$ where k is odd.

Pick $a \in_R \{2, \ldots, n-2\}$

if $\gcd(a, n) \neq 1$ output composite

$b_0 = a^u \bmod n$

If $b_0 = \pm 1$ output prime

for $i = 1$ to $u-1$ do

  $b_i = b_{i-1}^2 \bmod n$

  if $b_i \equiv -1$ output prime

  if $b_i \equiv 1$ return composite

return composite. [Since $b_k = a^{n-1} \neq 1 \bmod n$.
or $b_k = 1$ and
$b_{k-1} \neq \pm 1$].

<u>Theorem:</u> If n is prime alg outputs prime with prob 1. If n is composite alg outputs prime with prob $\leq \frac{1}{4}$.

<u>Sketch of the analysis</u>

Fix $a \in \mathbb{Z}_n^*$.

Let $b_0 = a^k \bmod n$

$b_1 = a^{k \cdot 2} = (a^k)^2 \bmod n$

$b_2 = a^{k \cdot 2^2} = ((a^k)^2)^2 \bmod n$

$b_u = a^{2^u k} = a^{n-1} \bmod n.$

If b_i becomes ± 1 then $b_{i+1}, \ldots, b_k$ are 1. When do we find a non-trivial square root of 1?

If $b_i = 1$ and $b_{i-1} \neq -1$.

This is precisely when the alg outputs composite. Also if $b_k = a^{n-1} \neq 1$.

<u>Ex:</u>

$n = 325 = 5^2 \cdot 13 \qquad n-1 = 324 = 81 \cdot 2^2.$

a	$b_0 = a^{81}$	$b_1 = a^{162}$	$b_2 = a^{324}$
2	252	129	66
7	307	324	1
32	57	324	1
49	324	1	1
65	0	0	0

126	1	1	1
201	226	51	1
224	274	1	1

Defn: Let $n \geq 3$ be an odd #.

Let $n-1 = u\,2^k$ u odd $k \geq 1$.

A number a, $1 \leq a < n$ is an RM-witness for n if $a^u \bmod n \neq 1$ and $a^{u \cdot 2^i} \bmod n \neq -1$ $\forall i$ $0 \leq i < k$.

If n is composite and a is not a RM-witness for n then a is a RM-liar for n.

Lemma: If a is an RM-witness for n then n is composite.

Analysis

We will prove a weaker theorem.

Theorem: Let $n \geq 3$ be odd composite and let L_n^{RM} ~~but~~ be the set of RM-liars for n. Then $|L_n^{RM}| \leq \frac{|\mathbb{Z}_n^*|}{2}$.

The difficulty is that L_n^{RM} is not a subgroup of $\mathbb{Z}_n^*$. Thus to prove the theorem we identify a proper subgroup S of $\mathbb{Z}_n^*$ and argue that $L_n^{RM} \subseteq S$.

We consider two cases.

Case 1: n is not a Carmichael number. If a is a RM-liar then it is also a Fermat-liar and we argued that $|F_n| \leq \frac{|\mathbb{Z}_n^*|}{2}$ when n is not a Carmichael #.

Case 2: n is a Carmichael number.

However this requires us to understand Carmichael #s. We will state and not prove.

Theorem: Suppose $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$ where each p_i is an odd prime.

(a) n is Carmichael iff
$\varphi(p_i^{k_i}) \mid n-1$ for $1 \leq i \leq t$.

$\Rightarrow$ (b) If n is Carmichael iff
$n = p_1 p_2 \cdots p_t$ s.t. $(p_i - 1) \mid (n-1)$ $\forall i$. In particular $t \geq 3$.

Our goal is to find a proper subgroup S of $\mathbb{Z}_n^*$ s.t. $L_n^{RM} \subseteq S$.

Let i_0 be maximal $i \geq 0$ such that there is some RM-liar a_0 with $a_0^{u 2^i} \bmod n = -1$. Since u is odd $(-1)^u = -1$ so i_0 exists.

Since n is a Carmichael #
$a_0^{n-1} = a_0^{u 2^k} = 1 \bmod n$ and hence $0 \leq i_0 < k$.

Let $B_n = \{ a \mid 1 \leq a < n, \ a^{u 2^{i_0}} \in \{+1, -1\} \bmod n \}$.

Lemma:

(i) $L_n^{RM} \subseteq B_n$

(ii) B_n is a subgroup of $\mathbb{Z}_n^*$

(iii) $\mathbb{Z}_n^* - B_n \neq \phi$.

Proof: (i) Let $a \in L_n^{RM}$

Case 1: $a^u \bmod n = 1$ Then

$a^{u 2^{i_0}} \bmod n = 1$ hence $a \in B_n$

Case 2: $a^{u 2^i} \bmod n = -1$ for some i

By defn i_0 $0 \le i \le i_0$. If $i = i_0$

then $a \in B_n$.

If $i < i_0$ $a^{u 2^{i+1}} \bmod n = 1$

and hence $a^{u \cdot 2^{i_0}} \bmod n = 1$.

and hence $a \in B_n$.

(ii) B_n is a subgroup.

$1 \in B_n$ trivially.

if $a \in B_n$ $b \in B_n$ $ab \in B_n$

easy.

(iii) We know that n has at least 3 prime factors hence

$n = n_1 n_2$ where n_1, n_2 odd

and $\gcd(n_1, n_2) = 1$.

Recall a_0 is a RM-liar with

$$a_0^{u 2^{i_0}} \equiv -1 \mod n.$$

Let $a_1 = a_0 \mod n_1$

By CRT $\exists$ unique $a \in \mathbb{Z}_n$ s.t.

$a \equiv a_1 \mod n_1$ and $a \equiv 1 \mod n_2$

We claim $a \in \mathbb{Z}_n^* - B_n$.

Calculating mod n_1, since $n_1 | n$.

$$a^{u \cdot 2^{i_0}} \equiv -1 \mod n_1 \quad (1)$$

Calculating mod n_2, since $a \mod n_2 = 1$

$$a^{u\, 2^{i_0}} = 1^{u \cdot 2^{i_0}} \equiv 1 \mod n_2. \quad (2)$$

$$(1) \Rightarrow a^{u \cdot 2^{i_0}} \not\equiv 1 \mod n$$

and $(2) \Rightarrow a^{u \cdot 2^{i_0}} \not\equiv -1 \mod n$

$\Rightarrow a \notin B_n$.

Further $a^{u \cdot 2^{i_0+1}} \mod n_1 = 1$ and

$$a^{u \cdot 2^{i_0+1}} \mod n_2 = 1$$

$\Rightarrow$ by CRT $a^{u \cdot 2^{i_0+1}} \mod n \equiv 1$.

$\Rightarrow \quad a \cdot a^{u \cdot 2^{i_0}} \bmod n \equiv 1$

$\Rightarrow \gcd(a, n) = 1 \quad \Rightarrow \quad a \in \mathbb{Z}_n^*$.

$\square$.

The preceding proof used characterization of Carmichael #s and is from Dietzfelbinger's book.

We give an alternate proof from the notes of Keith Conrad that avoids the use of Carmichael #s.

We again consider 2 cases.

Case 1: $n = p^\alpha$ for $\alpha \geq 2$ ie prime power. We claim n is not

Carmichael $\Rightarrow$ we can use the fact that $F_n \leq \frac{|\mathbb{Z}_n^*|}{2}$.

To see this it suffices to exhibit some $a \in \mathbb{Z}_n^*$ such that

$a^{n-1} \not\equiv 1 \mod n$.

Consider $1 + p^{\alpha-1}$.

$(1+p^{\alpha-1})^{n-1}$ by Binomial expansion

$$= 1 + \binom{n-1}{1} p^{\alpha-1} + p^{2\alpha-2}[\ldots]$$

Hence $(1+p^{\alpha-1}) \mod p^{\alpha}$

$$= 1 + (p^{\alpha}-1)p^{\alpha-1} \mod p^{\alpha}$$

$$= 1 - p^{\alpha-1} \mod p^{\alpha}$$

$$\equiv p^{\alpha} - p^{\alpha-1} + 1 \mod p^{\alpha}$$

1.

<u>Case 2:</u> n is not a prime power.

$\Rightarrow$ $n = p^{\alpha} n_2$ where p does not divide n_2

So $n = n_1 n_2$ where n_1, n_2 odd and $n_1\ n_2$ relatively prime.

Let i_0 be maximal in $\{0, \ldots, u-1\}$ such that there is some $a_0 \in \mathbb{Z}$ such that $a_0^{2^{i_0}} \equiv -1 \mod n$. Since $(-1)^{2^0} \equiv -1 \mod n$ i_0 exists. and $a_0 \in \mathbb{Z}_n^*$.

Let $B_n = \{ 1 \leq a \leq n \mid a^{2^{i_0} k} \equiv \pm 1 \mod n \}$.

Lemma:

(i) $L_n^{RM} \subseteq B_n$

(ii) B_n is a subgroup of $\mathbb{Z}_n^*$

(iii) $\mathbb{Z}_n^* - B_n \neq \phi$.

Proof: (i) Let $a \in L_n^{RM}$

Case 1: $a^u \bmod n = 1$ Then

$a^{u2^{i_0}} \bmod n = 1$ hence $a \in B_n$

Case 2: $a^{u2^i} \bmod n = -1$ for some i

By defn i_0 $0 \leq i \leq i_0$. If $i = i_0$

then $a \in B_n$.

If $i < i_0$ $a^{u2^{i+1}} \bmod n = 1$

and hence $a^{u \cdot 2^{i_0}} \bmod n = 1$.

and hence $a \in B_n$.

(ii) B_n is a subgroup.

$1 \in B_n$ trivially.

if $a \in B_n$ $b \in B_n$ $ab \in B_n$

easy.

(iii) $n = n_1 n_2$ where n_1, n_2 odd

and $\gcd(n_1, n_2) = 1$.

Recall a_0 is a RM-liar with

$$a_0^{u 2^{i_0}} \equiv -1 \mod n.$$

Let $a_1 = a_0 \mod n_1$

By CRT $\exists$ unique $a \in \mathbb{Z}_n$ s.t.

$a \equiv a_1 \mod n_1$ and $a \equiv 1 \mod n_2$

We claim $a \in \mathbb{Z}_n^* - B_n$.

Calculating mod n_1, since $n_1 | n$.

$$a^{u \cdot 2^{i_0}} \equiv -1 \mod n_1 \qquad (1)$$

Calculating mod n_2, since $a \mod n_2 = 1$

$$a^{u 2^{i_0}} = 1^{u \cdot 2^{i_0}} \equiv 1 \mod n_2. \qquad (2)$$

$$(1) \Rightarrow a^{u \cdot 2^{i_0}} \not\equiv 1 \mod n$$

and $(2) \Rightarrow a^{u \cdot 2^{i_0}} \not\equiv -1 \mod n$

$\Rightarrow a \notin B_n$.

Further $a^{u \cdot 2^{i_0+1}} \mod n_1 = 1$ and

$$a^{u \cdot 2^{i_0+1}} \mod n_2 = 1$$

$\Rightarrow$ by CRT $a^{u \cdot 2^{i_0+1}} \mod n \equiv 1$.

$\Rightarrow \quad a \cdot a^{u \cdot 2^{i_0}} \bmod n \equiv 1$

$\Rightarrow \gcd(a, n) = 1 \quad \Rightarrow \quad a \in \mathbb{Z}_n^*$.

$\square$