Miller-Rabin primality test

13 Primality testing

13.1 Overview of ideas

prime number theorem

Lemma 36. *Let* $\pi(n)$ *be the number of primes* $\leq n$*. Then*

$$\lim_{n \to \infty} \frac{\pi(n)}{n / \ln n} = 1$$

Proof. We won't present it.

13 Primality testing

13.1 Overview of ideas

prime number theorem

Lemma 36. *Let $\pi(n)$ be the number of primes $\leq n$. Then*

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\ln n} = 1$$

Proof. We won't present it.

using Miller-Rabin primality test:

- Suppse we seek a prime n of length β, i.e

$$n \in [0 : 2^{\beta} - 1]$$

- Miller- Rabin: test efficiently ($O(\beta^k) = O(\log n)$ bit operations) and very reliably (error probabilty $< 2^{-s}$), if p is a prime:

13 Primality testing

13.1 Overview of ideas

prime number theorem

Lemma 36. *Let $\pi(n)$ be the number of primes $\leq n$. Then*

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\ln n} = 1$$

Proof. We won't present it.

using Miller-Rabin primality test:

- Suppse we seek a prime n of length β, i.e

$$n \in [0 : 2^{\beta} - 1]$$

- Miller- Rabin: test efficiently ($O(\beta^k) = O(\log n)$ bit operations) and very reliably (error probabilty $< 2^{-s}$), if p is a prime:

Then

- test randomly drawn numbers $n \in [0 : 2^{\beta} - 1]$
- the Miller-Rabin tests cost $O(\beta^{k+1})$ (shown below)
- you get a wrong answer only with probability 2^{-s}.

13 Primality testing

13.1 Overview of ideas

prime number theorem

Lemma 36. *Let $\pi(n)$ be the number of primes $\leq n$. Then*

$$\lim_{n \to \infty} \frac{\pi(n)}{n/\ln n} = 1$$

Proof. We won't present it.

using Miller-Rabin primality test:

- Suppse we seek a prime n of length β, i.e

$$n \in [0 : 2^{\beta} - 1]$$

- Miller- Rabin: test efficiently ($O(\beta^k) = O(\log n)$ bit operations) and very reliably (error probabilty $< 2^{-s}$), if p is a prime:

Then

- test randomly drawn numbers $n \in [0 : 2^{\beta} - 1]$
- the Miller-Rabin tests cost $O(\beta^{k+1})$ (shown below)
- you get a wrong answer only with probability 2^{-s}.

- with k draws the probability not to draw a prime number k times tends to

$$p(n,k) = (\frac{n - \pi(n)}{n})^k = (1 - \frac{1}{\ln n})$$

$k = \ln n$:

$$p(n, \ln n) = (1 - \frac{1}{\ln n})^{\ln n}$$

$$\lim_{n \to \infty} (1 - \frac{1}{\ln n})^{\ln n} = \lim_{x \to \infty} (1 - \frac{1}{x})^x = 1/e$$

13 Primality testing

witnesses for composite numbers n

- lemma 30 (Fermat's theorem). if p is prime, then

  $$a^{p-1} \equiv 1 \bmod p \quad \text{for all } a \in \mathbb{Z}_p^*$$

  Thus

  $$a^{n-1} \not\equiv 1 \,\text{mod} \quad \rightarrow \; n \text{ is composite}$$

13 Primality testing

witnesses for composite numbers n

- lemma 30 (Fermat's theorem). if p is prime, then

  $$a^{p-1} \equiv 1 \bmod p \quad \text{for all } a \in \mathbb{Z}_p^*$$

  Thus

  $$a^{n-1} \not\equiv 1 \,\text{mod} \quad \rightarrow \; n \text{ is composite}$$

- x is a nontrivial square root of 1 iff $x^2 \equiv 1 \bmod n$ and $x \notin \{-1, 1\}$.

  lemma 34: If there exists a nontrivial square root of $n > 1$, then n is composite.

  candidates for such square roots derived from a

13 Primality testing

witnesses for composite numbers n

- lemma 30 (Fermat's theorem). if p is prime, then

  $$a^{p-1} \equiv 1 \bmod p \quad \text{for all } a \in \mathbb{Z}_p^*$$

  Thus

  $$a^{n-1} \not\equiv 1 \,\text{mod} \quad \rightarrow n \text{ is composite}$$

- x is a nontrivial square root of 1 iff $x^2 \equiv 1 \bmod n$ and $x \notin \{-1, 1\}$.

  lemma 34: If there exists a nontrivial square root of $n > 1$, then n is composite.

  candidates for such square roots derived from a

- randomly chosen a is witness if one of the tests succeeds.

13 Primality testing

witnesses for composite numbers n

- lemma 30 (Fermat's theorem). if p is prime, then

$$a^{p-1} \equiv 1 \bmod p \quad \text{for all } a \in \mathbb{Z}_p^*$$

  Thus

$$a^{n-1} \not\equiv 1 \bmod \quad \rightarrow n \text{ is composite}$$

- x is a nontrivial square root of 1 iff $x^2 \equiv 1 \bmod n$ and $x \notin \{-1, 1\}$.

  lemma 34: If there exists a nontrivial square root of $n > 1$, then n is composite.

  candidates for such square roots derived from a

- randomly chosen a is witness if one of the tests succeeds.

bound on accuracy

- with a witness decision 'composite' is always correct.
- with randomly chosen $a \in [1 : n-1]$ no witness may be found although n is composite. Now show:

  The set NW of non-witnesses forms a proper subgroup of $\mathbb{Z}_n^*$.

13 Primality testing

witnesses for composite numbers n

- lemma 30 (Fermat's theorem). if p is prime, then

  $$a^{p-1} \equiv 1 \bmod p \quad \text{for all } a \in \mathbb{Z}_p^*$$

  Thus

  $$a^{n-1} \not\equiv 1 \bmod \quad \rightarrow n \text{ is composite}$$

- x is a nontrivial square root of 1 iff $x^2 \equiv 1 \bmod n$ and $x \notin \{-1, 1\}$.

  lemma 34: If there exists a nontrivial square root of $n > 1$, then n is composite.

  candidates for such square roots derived from a

- randomly chosen a is witness if one of the tests succeeds.

bound on accuracy

- with a witness decision 'composite' is always correct.
- with randomly chosen $a \in [1 : n-1]$ no witness may be found although n is composite. Now show:

  The set NW of non-witnesses forms a proper subgroup of $\mathbb{Z}_n^*$.

- recall lemma 13: If H is a proper subroup of finite group g, then $|H| \leq |G|/2$

  then

  $$|NW| \leq |\mathbb{Z}_n^*/2| \leq (n-1)/2$$

  thus probability to miss the witnesses is $< 1/2$

13 Primality testing

witnesses for composite numbers n

- lemma 30 (Fermat's theorem). if p is prime, then

  $$a^{p-1} \equiv 1 \bmod p \quad \text{for all } a \in \mathbb{Z}_p^*$$

  Thus

  $$a^{n-1} \not\equiv 1 \bmod \quad \rightarrow n \text{ is composite}$$

- x is a nontrivial square root of 1 iff $x^2 \equiv 1 \bmod n$ and $x \notin \{-1, 1\}$.

  lemma 34: If there exists a nontrivial square root of $n > 1$, then n is composite.

  candidates for such square roots derived from a

- randomly chosen a is witness if one of the tests succeeds.

bound on accuracy

- with a witness decision 'composite' is always correct.
- with randomly chosen $a \in [1 : n-1]$ no witness may be found although n is composite. Now show:

  The set NW of non-witnesses forms a proper subgroup of $\mathbb{Z}_n^*$.

- recall lemma 13: If H is a proper subroup of finite group g, then $|H| \leq |G|/2$

  then

  $$|NW| \leq |\mathbb{Z}_n^*/2| \leq (n-1)/2$$

  thus probability to miss the witnesses is $< 1/2$

- reduce probability to miss witnesses to 2^{-s} by trying s numbers a.

13 Primality testing

13.2 witness computation (identifying composites)

$witness(a,n)$:

inputs

- $n \in \mathbb{N}$ odd,
- $a \in [1 : n-1]$, possible witness for the fact, that n is composite.

decompose

$$n - 1 = u \cdot 2^t \quad , \quad u\ odd$$

binary representation of $n-1$ has t trailing zeros.

1. $x_0 = a^u \bmod n$; (using modular exponentiation)
2. for $i = 1$ to t
3. $\{x_i = x_{i-1}^2 \bmod n$;
4. if $x_i == 1 \ \wedge \ x_{i-1} \neq 1 \ \wedge \ x_{i-1} \neq n-1$ { return $true$}
   x_{i-1} is nontrivial square root of 1.
   }
5. if $x_t \neq 1$ { return $true$ } else {return $false$ }

13 Primality testing

13.2 witness computation (identifying composites)

witness(a,n):

inputs

- $n \in \mathbb{N}$ odd,
- $a \in [1 : n-1]$, possible witness for the fact, that n is composite.

decompose

$$n - 1 = u \cdot 2^t \quad , \quad u \; odd$$

binary representation of $n-1$ has t trailing zeros.

1. $x_0 = a^u \bmod n$; (using modular exponentiation)
2. for $i = 1$ to t
3. $\{x_i = x_{i-1}^2 \bmod n$;
4. if $x_i == 1 \wedge x_{i-1} \neq 1 \wedge x_{i-1} \neq n-1$ { return $true$}
   x_{i-1} is nontrivial square root of 1.
   }
5. if $x_t \neq 1$ { return $true$ } else {return $false$ }

witness correctly identifies composite n:

Lemma 37. *If $witness(a,n) = true$, the n is composite*

13 Primality testing

13.2 witness computation (identifying composites)

$witness(a,n)$:

inputs

- $n \in \mathbb{N}$ odd,
- $a \in [1 : n-1]$, possible witness for the fact, that n is composite.

decompose

$$n - 1 = u \cdot 2^t \quad , \quad u\ odd$$

binary representation of $n-1$ has t trailing zeros.

1. $x_0 = a^u \bmod n$; (using modular exponentiation)
2. for $i = 1$ to t
3. $\{x_i = x_{i-1}^2 \bmod n$;
4. if $x_i == 1 \wedge x_{i-1} \neq 1 \wedge x_{i-1} \neq n-1$ { return $true$}
   x_{i-1} is nontrivial square root of 1.
   }
5. if $x_t \neq 1$ { return $true$ } else {return $false$ }

witness correctly identifies composite n:

Lemma 37. *If $witness(a,n) = true$, the n is composite*

- line 4 returns $true$: apply lemma 34
- for all $i \in [0 : t]$

  $$x_i = a^{u \cdot 2^i} \bmod n$$

  by induction i. Trivial for $i = 0$. Induction step

  $$\begin{aligned} x_i &= x_{i-1}^2 \bmod n \\ &= (a^{u \cdot 2^{i-1}})^2 \bmod n \quad \text{(induction hypothesis)} \\ &= a^{u \cdot 2 \cdot 2^{i-1}} \bmod n \\ &= a^{u \cdot 2^i} \bmod n \end{aligned}$$

- line 5 returns true: $x_t = a^{n-1} \bmod n$. Apply lemma 30

13 Primality testing

13.3 Miller-Rabin primality test

$Miller - Rabin(n,s):$

1. for $j = 1$ to s
2. $\{\ a = random(1, n-1)\ \ ;$
3. if $witness(a,n)$ $\{$ return $composite\}$
   $\}$
   definitely
4. return $prime$

   almost surely

13 Primality testing

13.3 Miller-Rabin primality test

$Miller - Rabin(n, s):$

1. for $j = 1$ to s
2. $\{$ $a = random(1, n-1)$;
3. if $witness(a, n)$ $\{$ return $composite\}$
   $\}$
   definitely
4. return $prime$

   almost surely

number of non witnesses a for composite n :

Lemma 38. *For odd n the set of non witnesses a is contained in a proper subgroup of* $\mathbb{Z}_n^*$

13 Primality testing

13.3 Miller-Rabin primality test

$Miller-Rabin(n,s)$:

1. for $j = 1$ to s
2. $\{ a = random(1, n-1)$;
3. if $witness(a,n)$ $\{$ return $composite\}$
   $\}$
   definitely
4. return $prime$

   almost surely

number of non witnesses a for composite n :

Lemma 38. *For odd n the set of non witnesses a is contained in a proper subgroup of $\mathbb{Z}_n^*$*

- a not witnesess $\rightarrow$ $a \in \mathbb{Z}_n^*$

$$\begin{aligned} a \cdot a^{n-2} &= a^{n-1} \\ &\equiv 1 \bmod n \end{aligned}$$

$$ax \equiv 1 \bmod n \quad \text{solvable by } x = a^{n-2}$$

lemma 19 $\rightarrow$

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

recall: **Lemma 19.** *Let $d = gcd(a,n)$. Then*

$$ax \equiv b \bmod n$$

is solvalble if and only if $d|b$.

13.3 Miller-Rabin primality test

$Miller-Rabin(n,s)$:

1. for $j=1$ to s
2. $\{\ a = random(1,n-1)\ \ ;$
3. if $witness(a,n)$ $\{$ return $composite\}$
   $\}$
   definitely
4. return $prime$

   almost surely

number of non witnesses a for composite n :

Lemma 38. *For odd n the set of non witnesses a is contained in a proper subgroup of* $\mathbb{Z}_n^*$

- a not witnesess $\rightarrow\ a \in \mathbb{Z}_n^*$

$$\begin{aligned} a \cdot a^{n-2} &= a^{n-1} \\ &\equiv 1 \bmod n \end{aligned}$$

$$ax \equiv 1 \bmod n \quad \text{solvable by } x = a^{n-2}$$

  lemma 19 $\rightarrow$

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

- (the easy case) there is witness $x \in \mathbb{Z}_n^*$ with

$$x^{n-1} \neq 1 \bmod n$$

  Set

$$B = \{b \in \mathbb{Z}_n^* \ : \ b^{n-1} \equiv 1 \bmod n\}$$

  - $1 \in B\ \rightarrow B \neq \emptyset$
  - B closed under $\cdot_n$, hence subgroup
  - all non witnesses a satisfy $a^{n-1} \equiv 1 \bmod n$, hence $a \in B$
  - $x \notin B\ \rightarrow$ subgroup is proper

13 Primality testing

number of non witnesses a for composite n :

Lemma 38. *For odd n the set of non witnesses a is contained in a proper subgroup of $\mathbb{Z}_n^*$*

a not witnesess $\rightarrow$ $a \in \mathbb{Z}_n^*$

- (the harder case) for all $x \in \mathbb{Z}_n^*$

$$x^{n-1} \equiv 1 \bmod n$$

  (n is Carmichael number, they are rare)

  - n is no prime power. Assume otherwise $n = p^e$ with $e > 1$ (n is composite).
    lemma 31 $\rightarrow$: $\mathbb{Z}_n^*$ is cyclic with a generator g. With lemma 9

$$ord(g) = |Z_n^*| = \varphi(n) = p^e(1-1/p) = (p-1)p^{e-1}$$

$$\begin{aligned} g^{n-1} &\equiv 1 \bmod n \quad \text{(the hard case)} \\ &= g^0 \bmod n \\ n-1 &\equiv 0 \bmod \varphi(n) \quad \text{(lemma 32, discrete logarithm theorem)} \end{aligned}$$

$$(p-1)p^{e-1} \mid p^e - 1 \quad , \quad p|(p-1)p^e - 1 \text{ but } p \not| \, p^e - 1$$

13 Primality testing

number of non witnesses a for composite n :

Lemma 38. *For odd n the set of non witnesses a is contained in a proper subgroup of $\mathbb{Z}_n^*$*

a not witnesess $\rightarrow$ $a \in \mathbb{Z}_n^*$

- (the harder case) for all $x \in \mathbb{Z}_n^*$

$$x^{n-1} \equiv 1 \bmod n$$

  (n is Carmichael number, they are rare)

  - n is no prime power. Assume otherwise $n = p^e$ with $e > 1$ (n is composite).
    lemma 31 $\rightarrow$: $\mathbb{Z}_n^*$ is cyclic with a generator g. With lemma 9

$$ord(g) = |Z_n^*| = \varphi(n) = p^e(1-1/p) = (p-1)p^{e-1}$$

$$\begin{aligned} g^{n-1} &\equiv 1 \bmod n \quad \text{(the hard case)} \\ &= g^0 \bmod n \\ n-1 &\equiv 0 \bmod \varphi(n) \quad \text{(lemma 32, discrete logarithm theorem)} \end{aligned}$$

$$(p-1)p^{e-1} \mid p^e - 1 \quad , \quad p|(p-1)p^e - 1 \text{ but } p \not| p^e - 1$$

  - decompose $n = n_1 n_2$ with $gcd(n_1, n_2) = 1$:

$$n = \prod_{i=1}^{r} p_i^{r_i}, \quad , \quad n_1 = p_1^{e_1} \quad , \quad n_2 = \prod_{i=2}^{r} p_i^{r_i}$$

13 Primality testing

number of non witnesses a for composite n :

Lemma 38. *For odd n the set of non witnesses a is contained in a proper subgroup of $\mathbb{Z}_n^*$*

a not witnesess $\rightarrow$ $a \in \mathbb{Z}_n^*$

- (the harder case) for all $x \in \mathbb{Z}_n^*$

$$x^{n-1} \equiv 1 \bmod n$$

(n is Carmichael number, they are rare)

- n is no prime power. Assume otherwise $n = p^e$ with $e > 1$ (n is composite).
  lemma 31 $\rightarrow$: $\mathbb{Z}_n^*$ is cyclic with a generator g. With lemma 9

$$ord(g) = |Z_n^*| = \varphi(n) = p^e(1 - 1/p) = (p-1)p^{e-1}$$

$$\begin{aligned} g^{n-1} &\equiv 1 \bmod n \quad \text{(the hard case)} \\ &= g^0 \bmod n \\ n-1 &\equiv 0 \bmod \varphi(n) \quad \text{(lemma 32, discrete logarithm theorem)} \end{aligned}$$

$$(p-1)p^{e-1} \mid p^e - 1 \quad , \quad p|(p-1)p^e - 1 \text{ but } p \not| \, p^e - 1$$

- decompose $n = n_1 n_2$ with $gcd(n_1, n_2) = 1$:

$$n = \prod_{i=1}^{r} p_i^{r_i}, \quad , \quad n_1 = p_1^{e_1} \quad , \quad n_2 = \prod_{i=2}^{r} p_i^{r_i}$$

- $witness(a,n)$ with $n - 1 = 2^t u$ and u odd computes $\bmod n$ sequence

$$X(a) = (a^u, a^{2u}, \ldots, a^{2^j u}, \ldots, a^{2^t u})$$

For $j, v \in \mathbb{Z}$ define

$$(v, j) \text{ acceptable } \leftrightarrow v \in \mathbb{Z}_n^* \wedge j \in [0:t] \wedge v^{2^j u} \equiv -1 \bmod n$$

$(n-1, 0)$ acceptable:

$$\begin{aligned} (n-1)^{2^0 u} &\equiv (-1)^u \bmod n \\ &= -1 \quad (u \text{ odd}) \end{aligned}$$

define

$$j = \max\{j \,:\, \exists v.\ (v, j) \text{ acceptable}\}$$

define

$$B = \{x \in \mathbb{Z}_n^* \,:\, x^{2^j u} \equiv \pm 1 \bmod n\}$$

closed under $\cdot_n$, subgroup of $\mathbb{Z}_n^*$, $|B|$ divides $|Z_n^*|$.

13 Primality testing

- decompose $n = n_1 n_2$ with $gcd(n_1, n_2) = 1$:

$$n = \prod_{i=1}^{r} p_i^{r_i}, \quad , \quad n_1 = p_1^{e_1} \quad , \quad n_2 = \prod_{i=2}^{r} p_i^{r_i}$$

- $witness(a,n)$ with $n-1 = 2^t u$ and u odd computes $\bmod n$ sequence

$$X(a) = (a^u, a^{2u}, \ldots, a^{2^j u}, \ldots, a^{2^t u})$$

For $j, v \in \mathbb{Z}$ define

$$(v, j) \text{ acceptable } \leftrightarrow \ v \in \mathbb{Z}_n^* \ \wedge \ j \in [0:t] \ \wedge \ v^{2^j u} \equiv -1 \bmod n$$

$(n-1, 0)$ acceptable:

$$\begin{aligned} (n-1)^{2^0 u} &\equiv (-1)^u \bmod n \\ &= -1 \quad (u \text{ odd}) \end{aligned}$$

define

$$j = \max\{j \ : \ \exists v. \ (v, j) \text{ acceptable}\}$$

define

$$B = \{x \in \mathbb{Z}_n^* \ : \ x^{2^j u} \equiv \pm 1 \bmod n\}$$

closed under $\cdot_n$, subgroup of $\mathbb{Z}_n^*$, $|B|$ divides $|Z_n^*|$.

13 Primality testing

- decompose $n = n_1 n_2$ with $gcd(n_1,n_2) = 1$:

$$n = \prod_{i=1}^{r} p_i^{r_i} \quad , \quad n_1 = p_1^{e_1} \quad , \quad n_2 = \prod_{i=2}^{r} p_i^{r_i}$$

- $witness(a,n)$ with $n-1 = 2^t u$ and u odd computes $\bmod n$ sequence

$$X(a) = (a^u, a^{2u}, \ldots, a^{2^j u}, \ldots, a^{2^t u})$$

For $j, v \in \mathbb{Z}$ define

$$(v, j) \text{ acceptable } \leftrightarrow \ v \in \mathbb{Z}_n^* \wedge j \in [0:t] \wedge v^{2^j u} \equiv -1 \bmod n$$

$(n-1, 0)$ acceptable:

$$\begin{aligned} (n-1)^{2^0 u} &\equiv (-1)^u \bmod n \\ &= -1 \quad (u \text{ odd}) \end{aligned}$$

define

$$j = \max\{j \ : \ \exists v. \ (v, j) \text{ acceptable}\}$$

define

$$B = \{x \in \mathbb{Z}_n^* \ : \ x^{2^j u} \equiv \pm 1 \bmod n\}$$

closed under $\cdot_n$, subgroup of $\mathbb{Z}_n^*$, $|B|$ divides $|Z_n^*|$.

- a not witness $\rightarrow$ $a \in B$:

  $X(a)$ has -1 at position $j' \leq j$ (maximality of j) or $X(a) = (1, \ldots, 1)$

13 Primality testing

- decompose $n = n_1 n_2$ with $gcd(n_1, n_2) = 1$:

$$n = \prod_{i=1}^{r} p_i^{r_i} \quad , \quad n_1 = p_1^{e_1} \quad , \quad n_2 = \prod_{i=2}^{r} p_i^{r_i}$$

- $witness(a,n)$ with $n-1 = 2^t u$ and u odd computes $\bmod n$ sequence

$$X(a) = (a^u, a^{2u}, \dots, a^{2^j u}, \dots, a^{2^t u})$$

For $j, v \in \mathbb{Z}$ define

$$(v, j) \text{ acceptable } \leftrightarrow v \in \mathbb{Z}_n^* \wedge j \in [0:t] \wedge v^{2^j u} \equiv -1 \bmod n$$

$(n-1, 0)$ acceptable:

$$\begin{aligned} (n-1)^{2^0 u} &\equiv (-1)^u \bmod n \\ &= -1 \quad (u \text{ odd}) \end{aligned}$$

define

$$j = \max\{j \,:\, \exists v.\ (v, j) \text{ acceptable}\}$$

define

$$B = \{x \in \mathbb{Z}_n^* \,:\, x^{2^j u} \equiv \pm 1 \bmod n\}$$

closed under $\cdot_n$, subgroup of $\mathbb{Z}_n^*$, $|B|$ divides $|Z_n^*|$.

- a not witness $\to$ $a \in B$:

  $X(a)$ has -1 at position $j' \leq j$ (maximality of j) or
  $X(a) = (1, \dots, 1)$

- $\exists w \in \mathbb{Z}_n \setminus B$

  Using corollaries of Chinese remainder theorem

$$\begin{aligned} v^{2^j} &\equiv -1 \bmod n \\ v^{2^j} &\equiv -1 \bmod n_1 \quad \text{(lemma 28)} \end{aligned}$$

13 Primality testing

- decompose $n = n_1 n_2$ with $gcd(n_1, n_2) = 1$:

$$n = \prod_{i=1}^{r} p_i^{r_i} \quad , \quad n_1 = p_1^{e_1} \quad , \quad n_2 = \prod_{i=2}^{r} p_i^{r_i}$$

- $witness(a,n)$ with $n-1 = 2^t u$ and u odd computes $\bmod n$ sequence

$$X(a) = (a^u, a^{2u}, \ldots, a^{2^j u}, \ldots, a^{2^t u})$$

For $j, v \in \mathbb{Z}$ define

$$(v, j) \text{ acceptable } \leftrightarrow \ v \in \mathbb{Z}_n^* \wedge \ j \in [0:t] \ \wedge \ v^{2^j u} \equiv -1 \bmod n$$

$(n-1, 0)$ acceptable:

$$\begin{aligned} (n-1)^{2^0 u} &\equiv (-1)^u \bmod n \\ &= -1 \quad (u \text{ odd}) \end{aligned}$$

define

$$j = \max\{j \ : \ \exists v. \ (v, j) \text{ acceptable}\}$$

define

$$B = \{x \in \mathbb{Z}_n^* \ : \ x^{2^j u} \equiv \pm 1 \bmod n\}$$

closed under $\cdot_n$, subgroup of $\mathbb{Z}_n^*$, $|B|$ divides $|Z_n^*|$.

- a not witness $\rightarrow \ a \in B$:

  $X(a)$ has -1 at position $j' \leq j$ (maximality of j) or
  $X(a) = (1, \ldots, 1)$

- $\exists w \in \mathbb{Z}_n \setminus B$

  Using corollaries of Chinese remainder theorem

$$\begin{aligned} v^{2^j} &\equiv -1 \bmod n \\ v^{2^j} &\equiv -1 \bmod n_1 \quad \text{(lemma 28)} \end{aligned}$$

  Lemma 27 $\rightarrow \exists w$:

$$\begin{aligned} w &\equiv v \bmod n_1 \\ w &\equiv 1 \bmod n_2 \end{aligned}$$

$$\begin{aligned} w^{2^j u} &\equiv -1 \bmod n_1 \\ w^{2^j u} &\equiv 1 \bmod n_2 \end{aligned}$$

13 Primality testing

- decompose $n = n_1 n_2$ with $gcd(n_1, n_2) = 1$:

$$n = \prod_{i=1}^{r} p_i^{r_i} \quad , \quad n_1 = p_1^{e_1} \quad , \quad n_2 = \prod_{i=2}^{r} p_i^{r_i}$$

- $witness(a,n)$ with $n-1 = 2^t u$ and u odd computes $\bmod n$ sequence

$$X(a) = (a^u, a^{2u}, \ldots, a^{2^j u}, \ldots, a^{2^t u})$$

For $j, v \in \mathbb{Z}$ define

$$(v,j) \text{ acceptable } \leftrightarrow \; v \in \mathbb{Z}_n^* \wedge j \in [0:t] \wedge v^{2^j u} \equiv -1 \bmod n$$

$(n-1, 0)$ acceptable:

$$\begin{aligned} (n-1)^{2^0 u} &\equiv (-1)^u \bmod n \\ &= -1 \quad (u \text{ odd}) \end{aligned}$$

define

$$j = \max\{j \, : \, \exists v. \, (v,j) \text{ acceptable}\}$$

define

$$B = \{x \in \mathbb{Z}_n^* \, : \, x^{2^j u} \equiv \pm 1 \bmod n\}$$

closed under $\cdot_n$, subgroup of $\mathbb{Z}_n^*$, $|B|$ divides $|Z_n^*|$.

- a not witness $\rightarrow \; a \in B$:

  $X(a)$ has -1 at position $j' \leq j$ (maximality of j) or $X(a) = (1, \ldots, 1)$

- $\exists w \in \mathbb{Z}_n \setminus B$

  Using corollaries of Chinese remainder theorem

$$\begin{aligned} v^{2^j} &\equiv -1 \bmod n \\ v^{2^j} &\equiv -1 \bmod n_1 \quad \text{(lemma 28)} \end{aligned}$$

  Lemma 27 $\rightarrow \exists w$:

$$\begin{aligned} w &\equiv v \bmod n_1 \\ w &\equiv 1 \bmod n_2 \end{aligned}$$

$$\begin{aligned} w^{2^j u} &\equiv -1 \bmod n_1 \\ w^{2^j u} &\equiv 1 \bmod n_2 \end{aligned}$$

  Lemma 28:

$$w^{2^j u} \not\equiv 1 \bmod n_1 \; \rightarrow \; w^{2^j u} \not\equiv 1 \bmod n$$

$$w^{2^j u} \not\equiv -1 \bmod n_2 \; \rightarrow \; w^{2^j u} \not\equiv -1 \bmod n$$

$$w^{2^j u} \not\equiv \pm 1 \bmod n \, , \; w \notin B$$

Lemma 27. *Let*

$$n = n_1 n_2 \dots n_k \quad , \quad i \neq j \rightarrow gcd(n_i, n_j) = 1 \text{ (pairwise relatively prime)}$$

and

$$(a_1, \dots, a_k) \in \mathbb{N}^k$$

Then the set of equations

$$x \equiv a_i \bmod n_i \ , \ 1 \leq i \leq k$$

has a unique solution in Z_n

Lemma 28. *Let*

$$n = n_1 n_2 \dots n_k \quad , \quad i \neq j \rightarrow gcd(n_i, n_j) = 1 \text{ (pairwise relatively prime)}$$

and

$$a, x \in \mathbb{Z}$$

then

$$x \equiv a \bmod n_i \text{ for all } i \in [1:k] \quad \leftrightarrow \quad x \equiv a \bmod n$$

- claim: $w \in \mathbb{Z}_n^*$ (hence $w \in \mathbb{Z}_n^* \setminus B$ and B is proper subgroup)

$$v \in \mathbb{Z}_n^* \quad , \quad gcd(v,n) = 1 \quad , \quad gcd(v,n_1) = 1$$

$$w \equiv v \text{ mod } n_1 \;\rightarrow\; gcd(w,n_1) = 1$$

$$\text{as } d \mid n_1 \;\wedge\; d \mid v + kn_1 \;\rightarrow\; d \mid v$$

$$w \equiv 1 \text{ mod } n_2 \;\rightarrow\; gcd(w,n_2) = 1$$

$$\text{as } d \mid n_2 \wedge\; d \mid 1 + kn_2 \;\rightarrow\; d \mid 1$$

Lemma 3:

$$gcd(w,n_1n_2) = gcd(w,n) = 1 \quad , \; w \in \mathbb{Z}_n^*$$

13.4 interlude: Bayes's theorem

$W = (S, p)$ probability space, $A, B \subseteq S$ events

$$p(A|B) = \frac{p(A \cap B)}{p(B)} \quad \text{(def. of conditional prob.)}$$

$$\begin{aligned} p(A \cap B) &= p(B)p(A|B) \\ &= P(A)p(B|A) \end{aligned}$$

13.4 interlude: Bayes's theorem

$W = (S, p)$ probability space, $A, B \subseteq S$ events

$$p(A|B) = \frac{p(A \cap B)}{p(B)} \quad \text{(def. of conditional prob.)}$$

$$\begin{aligned} p(A \cap B) &= p(B)p(A|B) \\ &= P(A)p(B|A) \end{aligned}$$

Bayes's theorem

Lemma 39.

$$p(A|B) = \frac{p(A)p(B|A)}{p(B)}$$

13.4 interlude: Bayes's theorem

$W = (S, p)$ probability space, $A, B \subseteq S$ events

$$p(A|B) = \frac{p(A \cap B)}{p(B)} \quad \text{(def. of conditional prob.)}$$

$$\begin{aligned} p(A \cap B) &= p(B)p(A|B) \\ &= P(A)p(B|A) \end{aligned}$$

Bayes's theorem

Lemma 39.

$$p(A|B) = \frac{p(A)p(B|A)}{p(B)}$$

$$B = (B \cap A) \cup (B \cap \overline{A}) \quad , \quad (B \cap A) \cap (B \cap \overline{A} = \emptyset$$

$$\begin{aligned} p(B) &= p(B \cap A) + p(B \cap \overline{A}) \\ &= p(A)p(B|A) + p(\overline{A})p(B|\overline{A}) \end{aligned}$$

13.4 interlude: Bayes's theorem

$W = (S, p)$ probability space, $A, B \subseteq S$ events

$$p(A|B) = \frac{p(A \cap B)}{p(B)} \quad \text{(def. of conditional prob.)}$$

$$\begin{aligned} p(A \cap B) &= p(B)p(A|B) \\ &= P(A)p(B|A) \end{aligned}$$

Bayes's theorem

Lemma 39.

$$p(A|B) = \frac{p(A)p(B|A)}{p(B)}$$

$$B = (B \cap A) \cup (B \cap \overline{A}) \quad , \quad (B \cap A) \cap (B \cap \overline{A} = \emptyset$$

$$\begin{aligned} p(B) &= p(B \cap A) + p(B \cap \overline{A}) \\ &= p(A)p(B|A) + p(\overline{A})p(B|\overline{A}) \end{aligned}$$

Lemma 40.

$$p(A|B) = \frac{p(A)p(B|A)}{p(A)p(B|A) + p(\overline{A})p(B|\overline{A})}$$

13.4 interlude: Bayes's theorem

$W = (S, p)$ probability space, $A, B \subseteq S$ events

$$p(A|B) = \frac{p(A \cap B)}{p(B)} \quad \text{(def. of conditional prob.)}$$

$$\begin{aligned} p(A \cap B) &= p(B)p(A|B) \\ &= P(A)p(B|A) \end{aligned}$$

Bayes's theorem

Lemma 39.

$$p(A|B) = \frac{p(A)p(B|A)}{p(B)}$$

$$B = (B \cap A) \cup (B \cap \overline{A}) \quad , \quad (B \cap A) \cap (B \cap \overline{A} = \emptyset$$

$$\begin{aligned} p(B) &= p(B \cap A) + p(B \cap \overline{A}) \\ &= p(A)p(B|A) + p(\overline{A})p(B|\overline{A}) \end{aligned}$$

Lemma 40.

$$p(A|B) = \frac{p(A)p(B|A)}{p(A)p(B|A) + p(\overline{A})p(B|\overline{A})}$$

13.5 probability to declare a composite number a prime

Let β length of $bin(n)$.

$$W = (S, p) \ , \ S = [0 : 2^\beta - 1] \ , \ p(n) = 1/2^\beta$$

$$A = \{n \in S \ : \ n \text{ prime}\}$$

prime number theorem $\rightarrow$

$$p(A) \approx 1/\ln n$$

$$e^{\ln n} = n = 2^{\log n} = e^{(\ln 2)\log n}$$

$$\ln n = (\ln 2)\log n \approx 0.693 \log n$$

13.5 probability to declare a composite number a prime

Let β length of $bin(n)$.

$$W = (S, p)\ ,\ S = [0 : 2^\beta - 1]\ ,\ p(n) = 1/2^\beta$$

$$A = \{n \in S\ :\ n \text{ prime}\}$$

prime number theorem $\rightarrow$

$$p(A) \approx 1/\ln n$$

$$e^{\ln n} = n = 2^{\log n} = e^{(\ln 2)\log n}$$

$$\ln n = (\ln 2)\log n \approx 0.693\log n$$

$$1/\ln n = 1/((\ln 2))\log n) \approx 1.443/\beta$$

$$p(A) \approx 1.443/\beta$$

13.5 probability to declare a composite number a prime

Let β length of $bin(n)$.

$$W = (S, p)\ ,\ S = [0 : 2^{\beta} - 1]\ ,\ p(n) = 1/2^{\beta}$$

$$A = \{n \in S\ :\ n \text{ prime}\}$$

prime number theorem $\rightarrow$

$$p(A) \approx 1/\ln n$$

$$e^{\ln n} = n = 2^{\log n} = e^{(\ln 2)\log n}$$

$$\ln n = (\ln 2)\log n \approx 0.693 \log n$$

$$1/\ln n = (1/(\ln 2))\log n \approx 1.443/\beta$$

$$p(A) \approx 1.443/\beta$$

$$p(\overline{A})/p(A) \approx (1 - 1/\ln n) \cdot \ln n = \ln n - 1$$

13.5 probability to declare a composite number a prime

Let β length of $bin(n)$.

$$W = (S, p)\ ,\ S = [0 : 2^{\beta} - 1]\ ,\ p(n) = 1/2^{\beta}$$

$$A = \{n \in S\ :\ n \text{ prime}\}$$

prime number theorem $\rightarrow$

$$p(A) \approx 1/\ln n$$

$$e^{\ln n} = n = 2^{\log n} = e^{(\ln 2)\log n}$$

$$\ln n = (\ln 2)\log n \approx 0.693 \log n$$

$$1/\ln n = (1/(\ln 2))\log n \approx 1.443/\beta$$

$$p(A) \approx 1.443/\beta$$

$$p(\overline{A})/p(A) \approx (1 - 1/\ln n) \cdot \ln n = \ln n - 1$$

$$B = \{n \in S\ :\ Miller - Rabin(n, s) = prime\}$$

- $p(\overline{B}|A) = 0$ as there are no witnesses.

$$p(B|A) = 1$$

- $p(B|\overline{A}) \leq 2^{-s}$ probability to declare a composite a prime after s tests.
- $p(A|B)$ probability the a number declared prime is indeed prime

13.5 probability to declare a composite number a prime

Let β length of $bin(n)$.

$$W = (S,p)\ ,\ S = [0 : 2^{\beta} - 1]\ ,\ p(n) = 1/2^{\beta}$$

$$A = \{n \in S\ :\ n \text{ prime}\}$$

prime number theorem $\rightarrow$

$$p(A) \approx 1/\ln n$$

$$e^{\ln n} = n = 2^{\log n} = e^{(\ln 2)\log n}$$

$$\ln n = (\ln 2)\log n \approx 0.693 \log n$$

$$1/\ln n = (1/(\ln 2))\log n \approx 1.443/\beta$$

$$p(A) \approx 1.443/\beta$$

$$p(\overline{A})/p(A) \approx (1 - 1/\ln n) \cdot \ln n = \ln n - 1$$

$$B = \{n \in S\ :\ Miller - Rabin(n,s) = prime\}$$

- $p(\overline{B}|A) = 0$ as there are no witnesses.

$$p(B|A) = 1$$

- $p(B|\overline{A}) \leq 2^{-s}$ probability to declare a composite a prime after s tests.
- $p(A|B)$ probability the a number declared prime is indeed prime

Lemma 40:

$$\begin{aligned} p(A|B) &= \frac{p(A)p(B|A)}{p(A)p(B|A) + p(\overline{A})p(B|\overline{A})} \\ &= \frac{p(A)}{p(A) + p(\overline{A})p(B|\overline{A})} \\ &\approx \frac{1}{1 + 2^{-s}(\ln n - 1)} \end{aligned}$$

13.5 probability to declare a composite number a prime

Let β length of $bin(n)$.

$$W = (S, p)\ ,\ S = [0 : 2^\beta - 1]\ ,\ p(n) = 1/2^\beta$$

$$A = \{n \in S\ :\ n \text{ prime}\}$$

prime number theorem $\rightarrow$

$$p(A) \approx 1/\ln n$$

$$e^{\ln n} = n = 2^{\log n} = e^{(\ln 2)\log n}$$

$$\ln n = (\ln 2)\log n \approx 0.693 \log n$$

$$1/\ln n = (1/(\ln 2))\log n \approx 1.443/\beta$$

$$p(A) \approx 1.443/\beta$$

$$p(\overline{A})/p(A) \approx (1 - 1/\ln n) \cdot \ln n = \ln n - 1$$

$$B = \{n \in S\ :\ Miller-Rabin(n,s) = prime\}$$

- $p(\overline{B}|A) = 0$ as there are no witnesses.

$$p(B|A) = 1$$

- $p(B|\overline{A}) \leq 2^{-s}$ probability to declare a composite a prime after s tests.
- $p(A|B)$ probability the a number declared prime is indeed prime

Lemma 40:

$$\begin{aligned} p(A|B) &= \frac{p(A)p(B|A)}{p(A)p(B|A) + p(\overline{A})p(B|\overline{A})} \\ &= \frac{p(A)}{p(A) + p(\overline{A})p(B|\overline{A})} \\ &\approx \frac{1}{1 + 2^{-s}(\ln n - 1)} \end{aligned}$$

$\beta = 1024$:

$$\log(\ln n - 1) \approx \log(\beta/1.443) \approx 9$$

[CLRS]: choose $s = 50$