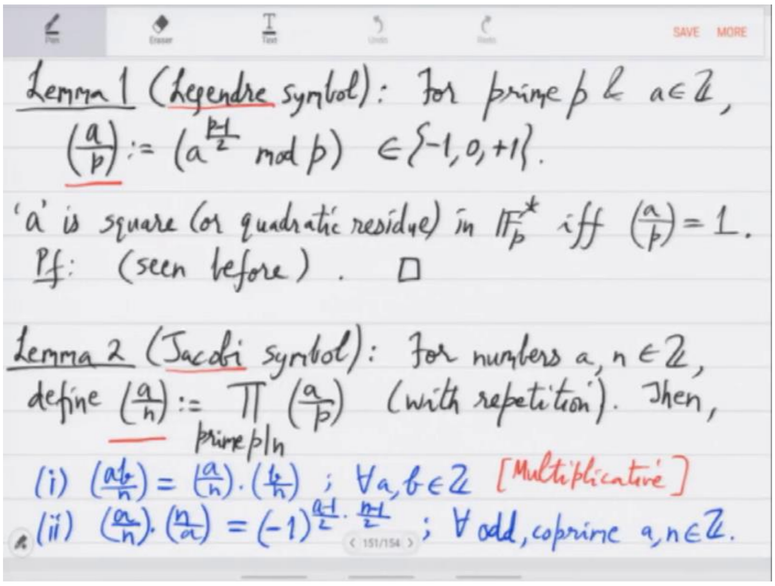
Computational Number Theory and Algebra

Prof. Nitin Saxena
Department of Aerospace Engineering
Indian Institute of Technology - Kanpur

Lecture – 24
Randomized Primality Testing Solovay - Strassen and Miller-Rabin Tests

(Refer Slide Time: 00:16)



Lemma 1 (Legendre symbol): For prime p & $a \in \mathbb{Z}$,
$\left(\frac{a}{p}\right) := \left(a^{\frac{p-1}{2}} \bmod p\right) \in \{-1, 0, +1\}$.

'a' is square (or quadratic residue) in $\mathbb{F}_p^*$ iff $\left(\frac{a}{p}\right) = 1$.
Pf: (seen before). □

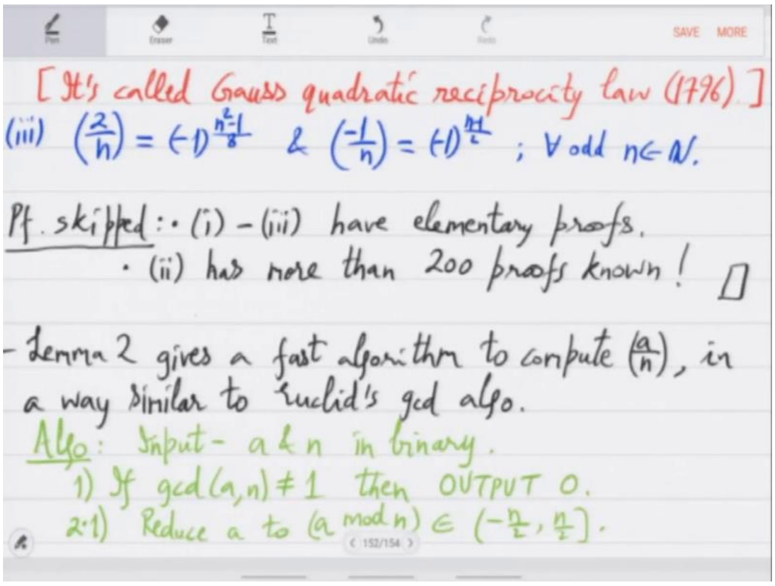
Lemma 2 (Jacobi symbol): For numbers $a, n \in \mathbb{Z}$,
define $\left(\frac{a}{n}\right) := \prod_{\text{prime } p | n} \left(\frac{a}{p}\right)$ (with repetition). Then,

(i) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right)$; $\forall a, b \in \mathbb{Z}$ [Multiplicative]

(ii) $\left(\frac{a}{n}\right) \cdot \left(\frac{n}{a}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{n-1}{2}}$; $\forall$ odd, coprime $a, n \in \mathbb{Z}$.

Last time we looked at the definition of Jacobi symbol and more importantly we looked at these properties in blue. So there is this first property is that it is totally multiplicative b by n factors.

(Refer Slide Time: 00:36)



[It's called Gauss quadratic reciprocity law (1796)]

(iii) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$ & $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$; $\forall$ odd $n \in \mathbb{N}$.

Pf. skipped: • (i) – (iii) have elementary proofs.
• (ii) has more than 200 proofs known! □

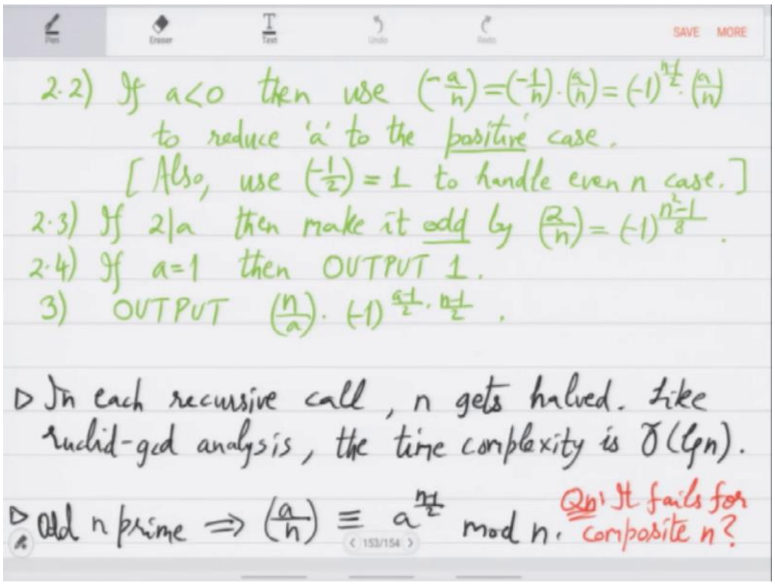
- Lemma 2 gives a fast algorithm to compute $\left(\frac{a}{n}\right)$, in a way similar to Euclid's gcd algo.

Algo: Input - a & n in binary.
1) If $\gcd(a,n) \neq 1$ then OUTPUT 0.
2·1) Reduce a to $(a \bmod n) \in \left(-\frac{n}{2}, \frac{n}{2}\right]$.

Second is reciprocity law and third is some examples of the Jacobi symbols so what is 2 by n what is -1 by n and then based on these properties we gave an algorithm to compute the

Jacobi symbol in an extremely fast way. So the algorithm is in green first you check whether a n are co prime otherwise obviously you factor n, n is composite. Then you so now assuming that a n r co prime reduce a modulo n. So bring the remainder around n by 2 magnitude less than n by 2.

(Refer Slide Time: 01:17)



2.2) If $a<0$ then use $\left(\frac{-a}{n}\right)=\left(\frac{-1}{n}\right)\cdot\left(\frac{a}{n}\right)=(-1)^{\frac{n-1}{2}}\cdot\left(\frac{a}{n}\right)$ to reduce 'a' to the positive case.
[Also, use $\left(\frac{-1}{2}\right)=1$ to handle even n case.]

2.3) If $2|a$ then make it odd by $\left(\frac{2}{n}\right)=(-1)^{\frac{n^2-1}{8}}$.

2.4) If $a=1$ then OUTPUT 1.

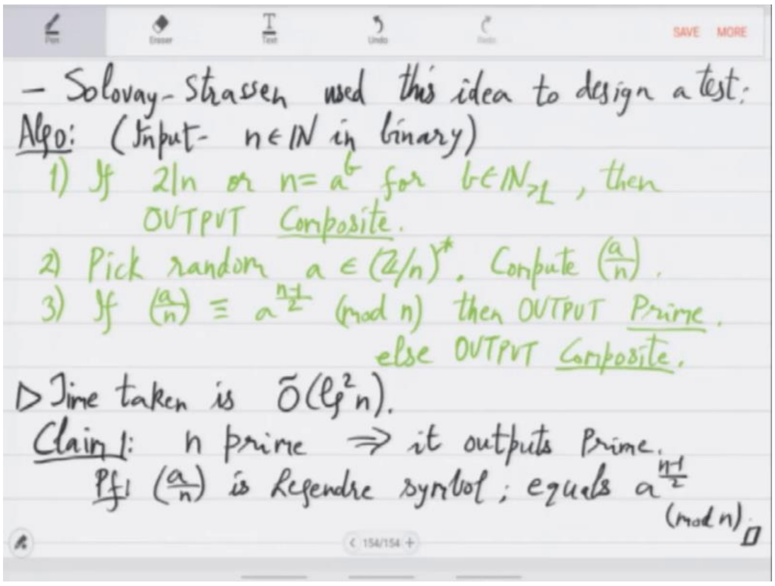
3) OUTPUT $\left(\frac{n}{a}\right)\cdot(-1)^{\frac{a-1}{2}\cdot\frac{n-1}{2}}$.

▷ In each recursive call, n gets halved. Like Euclid-gcd analysis, the time complexity is $\tilde{O}(\lg n)$.

▷ Odd n prime $\Rightarrow \left(\frac{a}{n}\right)\equiv a^{\frac{n-1}{2}}$ mod n. Qn: It fails for composite n?

And basically then you replace a by n by n by a and then when you will again repeat you will be reducing n mod a. So every time n is getting halved that was the main point halving was the main point so this is why it is so similar to Euclid's gcd algorithm division causes the halving and the complexity is o tilde login.

(Refer Slide Time: 01:54)



– Solovay-Strassen used this idea to design a test:

Algo: (Input- $n\in\mathbb{N}$ in binary)

1) If $2|n$ or $n=a^b$ for $b\in\mathbb{N}_{>1}$, then OUTPUT Composite.

2) Pick random $a\in(\mathbb{Z}/n)^*$. Compute $\left(\frac{a}{n}\right)$.

3) If $\left(\frac{a}{n}\right)\equiv a^{\frac{n-1}{2}}$ (mod n) then OUTPUT Prime. else OUTPUT Composite.

▷ Time taken is $\tilde{O}(\lg^2 n)$.

Claim 1: n prime $\Rightarrow$ it outputs Prime.

Pf: $\left(\frac{a}{n}\right)$ is Legendre symbol; equals $a^{\frac{n-1}{2}}$ (mod n). □

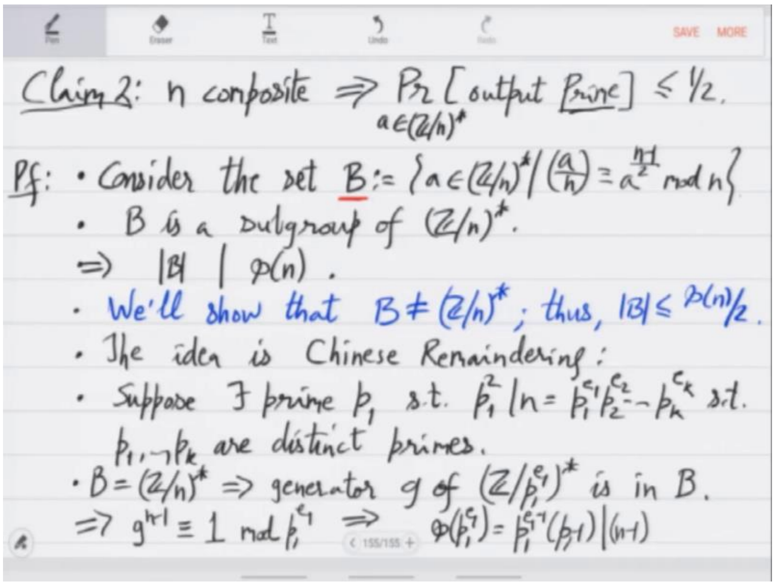
So it is a very fast way to compute the Jacobi symbol based on this the first Primality test was given by Solvay-Strassen to design a test so that is again the input is just a number in given in binary and you want to give a Boolean output 0 or 1 false or true right whether n is composite or n is prime. So the first step is simple you just check whether n is even 2 divides n or n is a perfect power. So check whether these a and b exist such that n is a to the b?

If yes then clearly n is composite output composite else you continue with the main idea this computation of the Jacobi symbols. So you pick a random a which will be co prime to n if it is not then you factor n and you compute a by n using this Euclid gcd type algorithm you will very quickly get a by n which is plus - 1 and if this a by n is a to the n - 1 by 2 mod n in that case you guess that n is prime.

Otherwise if this congruence fails then you definitely you know that n is composite. So step 2 is very efficient step 1 and step 3 by repeated squaring you can do it in around the log square and time. So this complexity is log square n so it is a quadratic time algorithm to test Primality why does it work right. So we have to now prove those claims so first claim is the easy 1 which is that if n is prime then it outputs prime.

If n is prime then a by n is what; a by n is the Legendre symbol and you know that it is by definition a to the n - 1 by 2. So this is the easy part, this is clear.

(Refer Slide Time: 07:24)



Claim 2: n composite $\Rightarrow \Pr_{a\in(\mathbb{Z}/n)^*}[\text{output Prime}] \leq 1/2$.

Pf: • Consider the set $B := \{a \in (\mathbb{Z}/n)^* \mid \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n\}$

• B is a subgroup of $(\mathbb{Z}/n)^*$.

$\Rightarrow |B| \mid \phi(n)$.

• We'll show that $B \neq (\mathbb{Z}/n)^*$; thus, $|B| \leq \phi(n)/2$.

• The idea is Chinese Remaindering:

• Suppose $\exists$ prime p_1 s.t. $p_1^2 \mid n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ s.t. $p_1, \ldots, p_k$ are distinct primes.

• $B = (\mathbb{Z}/n)^* \Rightarrow$ generator g of $(\mathbb{Z}/p_1^{e_1})^*$ is in B.

$\Rightarrow g^{n-1} \equiv 1 \bmod p_1^{e_1} \Rightarrow \phi(p_1^{e_1}) = p_1^{e_1-1}(p_1-1) \mid (n-1)$

And second claim is the important one that if n is composite then the probability that you get an output prime over is right so over the choice of a the probability that you get a the wrong answer this is bounded by half so thus this is not a deterministic polynomial time algorithm it is a randomized polynomial time algorithm it is always correct on primes. It may make a mistake on composite it may say that a composite number is prime when it is not.

So the idea of the proof is you identify a subgroup and use the property that subgroups of a group cannot be bigger than half. So consider the set of bad is so n is composite and still there are these a's such that a by n is a to the n - 1 by 2 mod n. So collect these is call this set the bad numbers right which are fooling the algorithm. First observation is that B is a subgroup of z n star it is a multiplicative subgroup.

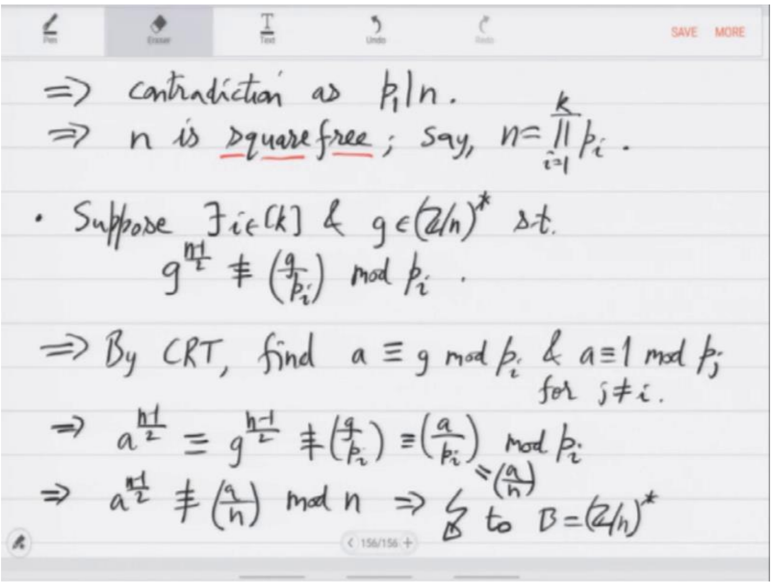
Why? Well because if a is in this and a prime is in this then their product a prime is also in this by multiplicativity of Jacobi symbol. We will show that so well since it is a subgroup it means that the size of B divides phi n so either the size of B is phi n or it is less than equal to half of that. So we need to show will show that B is not the whole set thus B is less than equal to phi n by 2 so that will finish the proof the size of B cannot exceed half of n.

So bad a's are few. How do you show that B is not z n star. So the idea is Chinese remaindering. So let us we will do 2 things first we will show that n is square free and then second is we will do Chinese remaindering. Suppose there exists a prime p 1 dividing n well such that its square divides in n be p 1 e 1 p 2 e 2 p k e k such that p 1 to p k are distinct primes. So suppose a prime square divides in we will rule this out we will show that this cannot happen.

So this cannot happen assuming B is equal to z n star. So B equal to z n star would mean that generator g of z modulo p 1 e 1 star note that z mod p 1 even star is a cyclic group it has a it has many generators. So for a generator g also this Jacobi test, Solvay-Strassen passes right that is what we are assuming. This is also in B so which will mean which means that g raised to n - 1 is 1 mod p 1 e 1.

In fact we knew something stronger than this we knew that g to the n - 1 by 2 is g by n but that is a sign it is + - 1 so we squared it and we reduce this property. So which means that by the order of g phi of p 1 e 1 the Euler torsion function that is the size of the subgroup this is equal to p 1 e 1 - 1 times p 1 - 1 and this divides n – 1. Even -1 is at least 2 so this means that p 1 divides n – 1 and that is a contradiction.

(Refer Slide Time: 15:44)



$\Rightarrow$ contradiction as $p_1 | n$.

$\Rightarrow$ n is square free; say, $n = \prod_{i=1}^{k} p_i$.

- Suppose $\exists i \in [k]$ & $g \in (\mathbb{Z}/n)^*$ s.t. $g^{\frac{n-1}{2}} \not\equiv \left(\frac{g}{p_i}\right) \bmod p_i$.

$\Rightarrow$ By CRT, find $a \equiv g \bmod p_i$ & $a \equiv 1 \bmod p_j$ for $j \neq i$.

$\Rightarrow$ $a^{\frac{n-1}{2}} \equiv g^{\frac{n-1}{2}} \not\equiv \left(\frac{g}{p_i}\right) \equiv \underset{= \left(\frac{a}{n}\right)}{\left(\frac{a}{p_i}\right)} \bmod p_i$

$\Rightarrow$ $a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \bmod n$ $\Rightarrow$ ↯ to $B = (\mathbb{Z}/n)^*$

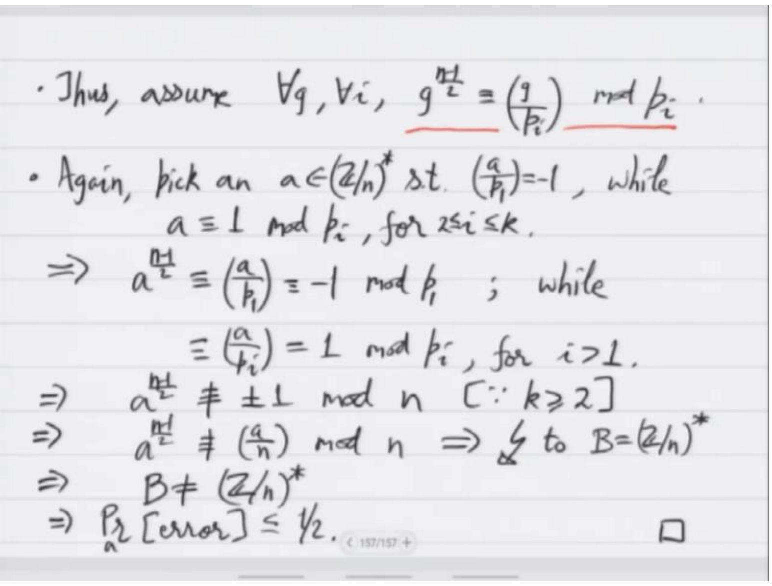
As p 1 divides n obviously it is at least 3. So p 1 cannot divide both n - 1 and n that is a contradiction so this contradiction means that that n is square free so say n is equal to product of these p i's distinct primes their multiplicity is 1 p 1 to p k that was kind of the pre processing part. So what we have deduced is that n is square free so n has these k prime factors distinct. Now suppose there is a prime pi and a number a such that let us call it g.

And a number g such that g raised to n - 1 by 2 is not the same as g over p i mod p i. Suppose there is a number g and an i says that g raised to n - 1 by 2 is not the same as the symbol g over p i mod p i. So then I claim that we will contradict v equal to z n star how is that? Then what you can do is by Chinese remaindering theorem CRT you can find an a which is the same as g mod p i and 1 for the other p j's.

This a will exist now, let us check a raise to n - 1 by 2 mod n now. So this is mod p i what do you get? Mod p i this is g raise to n - 1 by 2 which is not g over p i right. So a raise to n - 1 by 2 is also not a over p i mod p i and what is a over p i well since for other j's a is 1 mod p j this is the same as a by n right. So what you actually get is a raise to n - 1 by 2 is not a by n mod n which leads to a contradiction.

This will contradict b equal to z n star. So then what this means is that this condition is true so this condition is false it is basically for every g and i g raised to n - 1 by 2 has to be equal to g over p i mod p i. This is what we have deduced so let us continue with that.

(Refer Slide Time: 20:46)



- Thus, assume $\forall g, \forall i$, $g^{\frac{n-1}{2}} \equiv \left(\frac{g}{p_i}\right) \bmod p_i$.
- Again, pick an $a \in (\mathbb{Z}/n)^*$ s.t. $\left(\frac{a}{p_1}\right) = -1$, while $a \equiv 1 \bmod p_i$, for $2 \le i \le k$.

$\Rightarrow$ $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{p_1}\right) \equiv -1 \bmod p_1$; while $\equiv \left(\frac{a}{p_i}\right) = 1 \bmod p_i$, for $i > 1$.

$\Rightarrow$ $a^{\frac{n-1}{2}} \not\equiv \pm 1 \bmod n$ $[\because k \geq 2]$

$\Rightarrow$ $a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \bmod n \Rightarrow \lightning$ to $B = (\mathbb{Z}/n)^*$

$\Rightarrow$ $B \neq (\mathbb{Z}/n)^*$

$\Rightarrow$ $\Pr_a[\text{error}] \leq 1/2$. □

So assume that for all g for all i g raised to n - 1 by 2 is the same as g over p i mod p i right. In the next step now we will get a contradiction even with that. So we will use this to our advantage and get again a contradiction. So again pick an a such that a over p 1 is - 1 while a over p i or in fact let just take the simple root a is 1 mod p i for i 2 to k for the rest. So you is a non residue mod p 1 but for the other p i's it is just one.

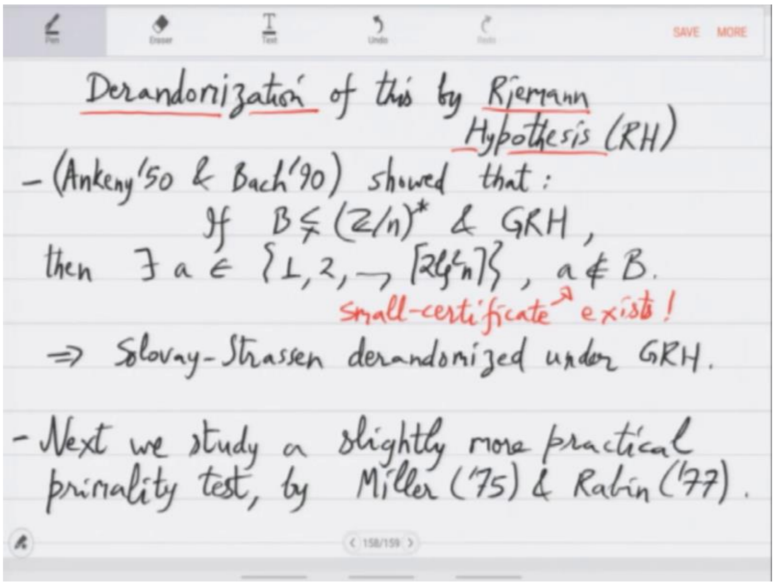
So by CRT again by CRT pick this a so by the red condition what you will get is e raised to n - 1 by 2 is a over p 1 which is -1 mod p 1 while it is e over p i which is 1 mod p i right. So e raised to n - 1 by 2 in Chinese remaindering is + - 1 for mod for p 1 it is - 1 for the rest it is 1 which means that e raised to n - 1 by 2 cannot be +- 1 mod n because if it was +1 then it will contradict mod p 1 if it was -1 it will contradict mod p 2.

So here actually we are using the fact that there are at least 2 primes this tells you that a raised to n - 1 by 2 cannot be +1 or -1 which means that e raised to m n - 1 by 2 in particular cannot be a by n which again contradicts this is contradiction to be equal to z n star so which means that b is not z n star that is what we have shown. So we started with the assumption that b is equal to z n star that is what we assumed here.

We started with this assumption and we got n to be square free and then we actually constructed either some g or some a in these 2 cases that finishes the proof. So what this means that the probability is at most half. So let us write that down. The probability over a is of error is less than equal to half. So this is the first randomized polynomial time Primality test with an elementary proof.

So, what next? So next we will just quickly we will quickly remark that you can also ask the question whether there is a deterministic polynomial time algorithm for Primality.

(Refer Slide Time: 26:44)



Derandomization of this by Riemann Hypothesis (RH)

- (Ankeny'50 & Bach'90) showed that:

If $B \subsetneq (\mathbb{Z}/n)^*$ & GRH,

then $\exists a \in \{1, 2, \to \lceil 2\lg^2 n \rceil\}$, $a \notin B$.

small-certificate exists!

$\Rightarrow$ Solovay-Strassen derandomized under GRH.

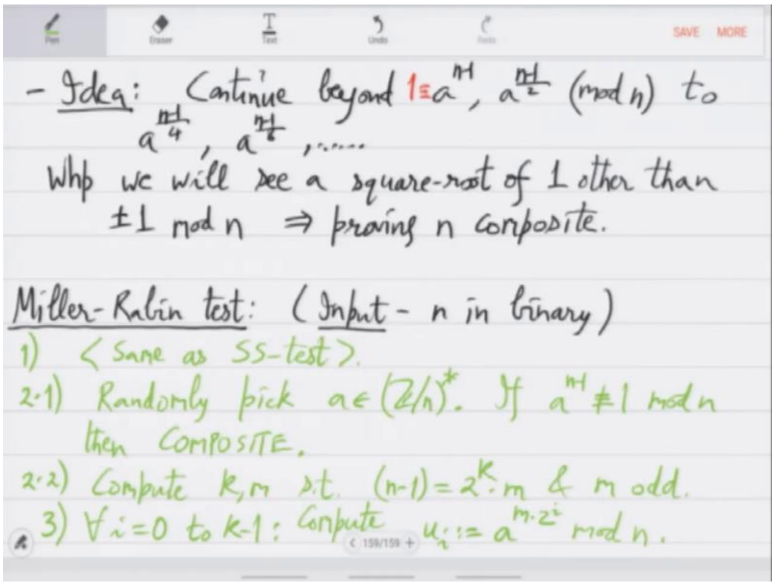
- Next we study a slightly more practical primality test, by Miller ('75) & Rabin ('77).

And there is a there is a way to de-randomize Solvay-Strassen also. So derandomization of this can be done by something called Riemann hypothesis. So Riemann hypothesis is a conjecture in analysis complex analysis it is a very old conjecture. It also carries an award of 1 billion dollars. Our interest in that is which was first shown by Ankeny and improved by Bach. So in the end what you get is they showed that if B is a proper subgroup of z n star like we had defined B to be the bad is and we showed that it is a proper subgroup.

And a generalized version of Riemann hypothesis holds GRH holds then there exists a small a, 1 to up to 2 log square n there exist a small a which is not in B. So what this is saying is that there will always be a small certificate. So if n is composite then there will be a small certificate a which you can find by just looking at the first around log square and numbers. So you do not need to pick a randomly.

So this will immediately derandomize the previous randomized test. So, the Solvay-Strassen can be derandomized that was a detour. So next we will study a more practical algorithm a slightly more practical algorithm which was given by Miller. Miller was the first 1 to propose in 75 and Robin made it probabilistic and practical few years later. This is the most popular Primality test.

(Refer Slide Time: 31:04)



- Idea: Continue beyond $1 \equiv a^{n-1}, a^{\frac{n-1}{2}} \pmod{n}$ to $a^{\frac{n-1}{4}}, a^{\frac{n-1}{8}}, \ldots\ldots$

Whp we will see a square-root of 1 other than ± 1 mod n $\Rightarrow$ proving n composite.

Miller-Rabin test: (Input - n in binary)

1) < Same as SS-test >.

2.1) Randomly pick $a \in (\mathbb{Z}/n)^*$. If $a^{n-1} \not\equiv 1$ mod n then COMPOSITE.

2.2) Compute k, m s.t. $(n-1) = 2^k \cdot m$ & m odd.

3) $\forall i = 0$ to $k-1$: Compute $u_i := a^{m \cdot 2^i}$ mod n.

So the idea of this is kind of taking square roots so you you had a to the n - 1 then you took a square root of that you got a raise to n - 1 by 2. Now you take square root of this as well and continue so then what you will get is a to the n - 1 by 4 and then you will get n - 1 by 8 and so on. So, with high probability we will see r square root of well so either a raise to n - 1 was not 1 in which case you already know this is Fermat's test.

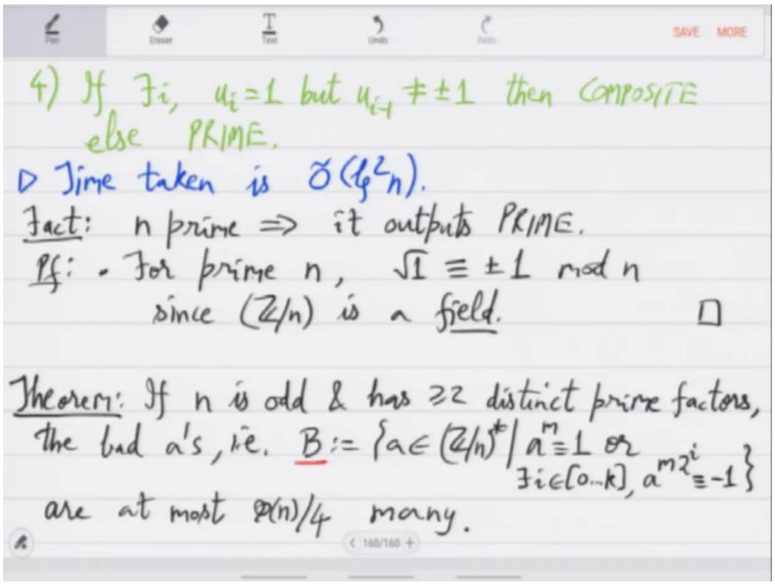
So you will already know that n is composite, so let us start with 1. So you are you are basically taking square root of 1 every time and with high probability you will see a square root of 1 other than +- 1. Proving that n is composite. Because if n was prime then the only square roots of 1 are plus and minus one right.

So that is the basic idea it is already an algorithm but let us anyways give the formal steps of the algorithm. So again input is binary n steps are just the basic idea extended. Step 1 is same as Solvay-Stassen test which is either n is even or n is a perfect power then you will output composite. Next step is randomly choose a 1 to n - 1 in fact let me just say in z n star because otherwise if it is it shares a factor with n then you factor in that will be a certificate of compositeness.

So randomly pick an a which is co prime to n. Now if a raised to n - 1 is not 1 then you will simply output composite. So let us assume it to be 1. So a raised to n - 1 is 1 and compute k m such that n - 1 is 2 raised to k times m and m is odd. Basically 2 raised to k is the highest power of 2 dividing n - 1. So compute these quantities and then you compute the so called square roots. So for all i 0 to k - 1 compute these square roots so a m times 2 raised to i mod n.

Now note that for i equal to 0 this is a raise to m you can compute a raise to m mod n then you compute a raised to 2 m a raised to 4 m and for i equal to k - 1 this is a raise to n - 1 by 2. So we are computing this square root thing but in reverse order starting from m and doubling it so that will give you these u i's.

(Refer Slide Time: 36:49)



4) If $\exists i$, $u_i = 1$ but $u_{i-1} \not\equiv \pm 1$ then COMPOSITE else PRIME.

▷ Time taken is $\tilde{O}(\lg^2 n)$.

Fact: n prime ⇒ it outputs PRIME.

Pf: • For prime n, $\sqrt{1} \equiv \pm 1 \bmod n$ since $(\mathbb{Z}/n)$ is a field. □

Theorem: If n is odd & has ≥2 distinct prime factors, the bad a's, i.e. $\underline{B} := \{a \in (\mathbb{Z}/n)^* \mid a^m \equiv 1$ or $\exists i \in [0..k], a^{m2^i} \equiv -1\}$ are at most $\varphi(n)/4$ many.

And finally check in the sequence of u i's check for an anomaly right square root of 1 which is other than + - 1. So if there exists an i such that u i is 1 but its square root u i - 1 is not + - 1 then you will output composite else you will output prime. So only when you see a square root of 1 other than + - 1 you are saying composite and you are correct in the other case you are just guessing prime.

And we have to see the error probability. So again since we are doing repeated squaring for a raise to m and then we are doubling this you can show is doable in log squaring. So the time complexity is o tilde log square n. So this is definitely polynomial time in fact it is very fast like solid stars and its quadratic time. The first observation is as before that if n is prime then it outputs prime why is that?

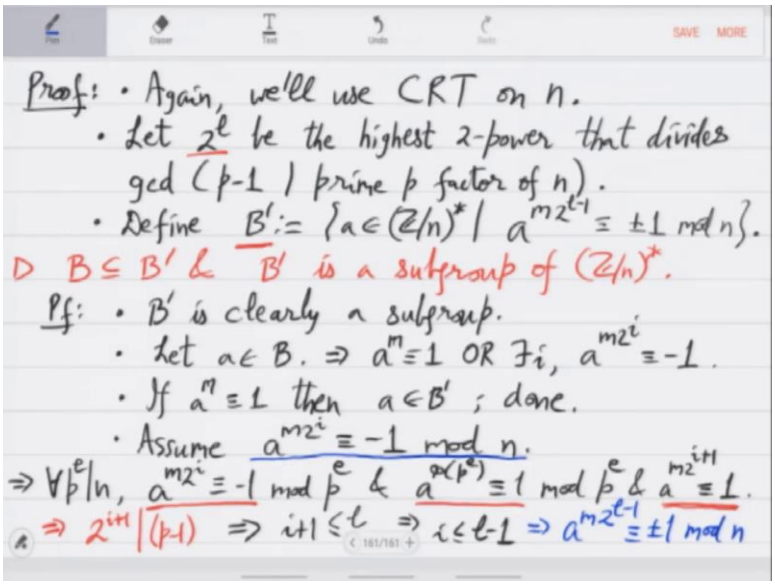
Well as I already said 1 has only 2 square roots modulo prime square root of 1 is only + - 1 there cannot be a third square root. Since z mod n is a field because of that. So step 4 cannot give cannot say positive and in the previous steps 2.1 also cannot say composite because a raise to n - 1 will be 1 mod n by 4 Fermat's little theorem for any a. So and step 1 also cannot say composite.

So the main thing that we have to show and analyze is what happens when n is composite and this algorithm outputs prime what is the chance of that. So if n is odd and has at least 2 distinct prime factors which is being checked already in step 1. So, suppose n is odd and there are at least 2 distinct prime factors then the bad a's that is in z n star for which the test is failing. When test is failing as in for which the algorithm is saying prime right. So for them a raised to m was 1 which means that all these u i's they were 1 or somewhere - 1 appeared and after that sequence of 1's.

So this is the set B the bad a's so either all the u i's are 1 or the sequence of u i's have some somewhere there is a - 1 then the test will say algorithm will say prime although n is not prime. So the bad is are at most phi n by 4 many. So the bound that you will get here is slightly better than solo wish does not there you had phi n by 2 here phi n by 4 so the probability of error is even smaller its 1 4th right.

So there is a 75% chance of success, so give it composite in the input it will output composite prime it will obviously output prime. So let us try to prove this of it now.

(Refer Slide Time: 43:42)



Proof: • Again, we'll use CRT on n.

• Let $\underline{2^{\ell}}$ be the highest 2-power that divides gcd (p-1 | prime p factor of n).

• Define $\underline{B'} := \{a \in (\mathbb{Z}/n)^* \mid a^{m2^{\ell-1}} \equiv \pm 1 \bmod n\}$.

▷ $B \subseteq B'$ & B' is a subgroup of $(\mathbb{Z}/n)^*$.

Pf: • B' is clearly a subgroup.

• Let $a \in B$. $\Rightarrow a^m \equiv 1$ OR $\exists i$, $a^{m2^i} \equiv -1$.

• If $a^m \equiv 1$ then $a \in B'$; done.

• Assume $\underline{a^{m2^i} \equiv -1 \bmod n}$.

$\Rightarrow \forall p^e | n$, $\underline{a^{m2^i} \equiv -1} \bmod p^e$ & $\underline{a^{\phi(p^e)} \equiv 1} \bmod p^e$ & $\underline{a^{m2^{i+1}} \equiv 1}$.

$\Rightarrow 2^{i+1} | (p-1) \Rightarrow i+1 \leq \ell \Rightarrow i \leq \ell - 1 \Rightarrow a^{m2^{\ell-1}} \equiv \pm 1 \bmod n$

So again we will use Chinese remaindering on n so note that this B this may not be a subgroup of z n star right this may not be a sub group because - 1 times - 1 becomes 1. So that is a problem so we will actually first identify a subgroup and then was to analyze that. So let us to move in that direction let us say 2 raised to l let this be the highest 2 power that divides all the p – 1’s prime p.

So let 2 raise to l divide each of these since n is odd p is odd so p - 1 is even so let 2 raise to l be the highest power dividing all of them and then define a different set B prime we will call it which will contain is such that a raised to m 2 l - 1 is plus - 1 mod n. And the advantage of this a is that it is a subgroup. So b is a subset of b prime and b prime is a subgroup of z n star that is the advantage. So we have identified actually a bigger set than b and it is a sub group so we will now actually show that B prime times B is more.

So this sub group B prime how big is this let us study this in fact first of all why is it why is it why does it contain b that is an important proof. So B prime is clearly a subgroup that is not the problem. Problem is why how why is B contained in B prime. So let a be in b which means that either a raise to m is 1 or there exist an i such that a raised to m 2 raised 2 i is - 1. Now if a raise to m is 1 then a is also in B prime.

Because the definition of B prime includes that a raised to m 1 right a raised to m 1 would mean that a raised to m times 2 raised to l - 1 is also 1. So that is that is a done case. So let us assume that a raised to m 2 raised to i is - 1 mod n. So this means that for all primes p that divide n in fact prime power p dividing in a raise to m 2 raise to i is - 1 mod p raised to e. Now let us again invoke this property that z mod p raised to e star is cyclic of order phi p raised to e.

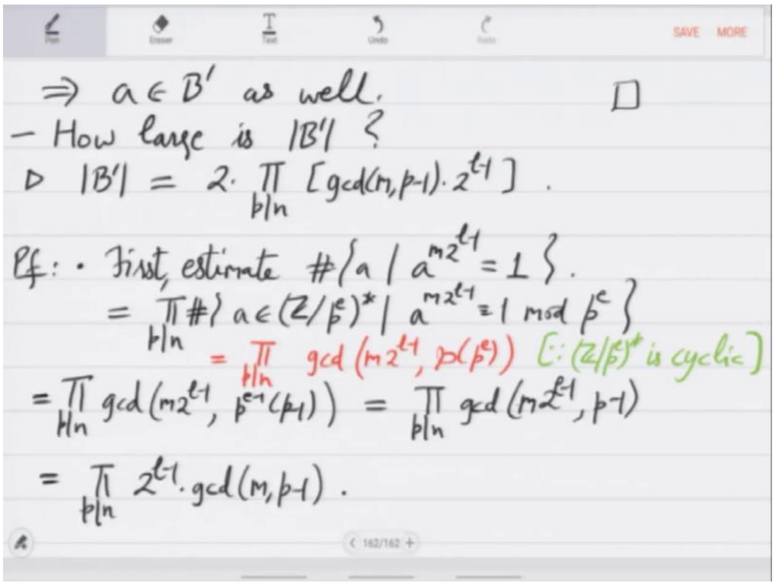
So since it is cyclic what can you say about p - 1 so you know that a raised to phi p raised to e is 1 mod p raised to e right and one thing more you can write which is obvious that e raised to m 2 i plus 1 is 1. So you know these 3 things you know that m 2 raise to i is - 1 hence you know that m 2 raised to i + 1. So square of the previous thing is 1 and you know that this group z mod z mod p raised to e star has size phi of p raise to e and it is a cyclic group so a raise to that is 1.

Now from these 3 conditions what can you these 3 properties what can you deduce? So we deduce that 2 raise 2 i + 1 divides p - 1. So p - 1 is the only even part of phi of p raised to e right suppose, suppose not; suppose something smaller than suppose 2 raised to i + 1 does not divide p - 1 only 2 raised to i divides the highest power is only 2 raised to i so in that case e raised to m 2 raised to i should have been 1 as well.

So if you look at this third property this tells you that a 2 raised to i + 1 is necessary and sufficient to get 1. So p - 1 has to be divisible by 2 raised to i + 1 and once you reduce this you are good because now you are now i relates to l right l was the 2 raise to l was the highest 2 power so it means that i + 1 has to be less than equal to l which means that i is less than equal to l – 1.

So now since already you have this green property you have this green property a m 2i equal to - 1 you learn that a raise 2 m 2 raised to l - 1 which is at least i this value will also come out to be + - 1 that is what you reduce and this means what this means that a is in b prime.

(Refer Slide Time: 53:42)



$\Rightarrow a \in B'$ as well. $\square$

– How large is $|B'|$?

▷ $|B'| = 2 \cdot \prod_{p|n} [\gcd(m, p-1) \cdot 2^{l-1}]$.

Pf: • First, estimate $\#\{a \mid a^{m2^{l-1}} = 1\}$.

$= \prod_{p|n} \#\{a \in (\mathbb{Z}/p^e)^* \mid a^{m2^{l-1}} \equiv 1 \bmod p^e\}$

$= \prod_{p|n} \gcd(m2^{l-1}, \varphi(p^e))$ $[\because (\mathbb{Z}/p^e)^* \text{ is cyclic}]$

$= \prod_{p|n} \gcd(m2^{l-1}, p^{e-1}(p-1)) = \prod_{p|n} \gcd(m2^{l-1}, p-1)$

$= \prod_{p|n} 2^{l-1} \cdot \gcd(m, p-1)$.

So B is a subset of B prime and B prime is a subgroup so that is something very good. Now let us move to the size so how large is B prime? So we will show that first we will prove a structural property that size of b prime is 2 times the product over all the primes dividing in this basically it is you are we are multiplying over the primes p dividing n for a prime p we have this gcd times 2 raised to l - 1 number this may seem very mysterious.

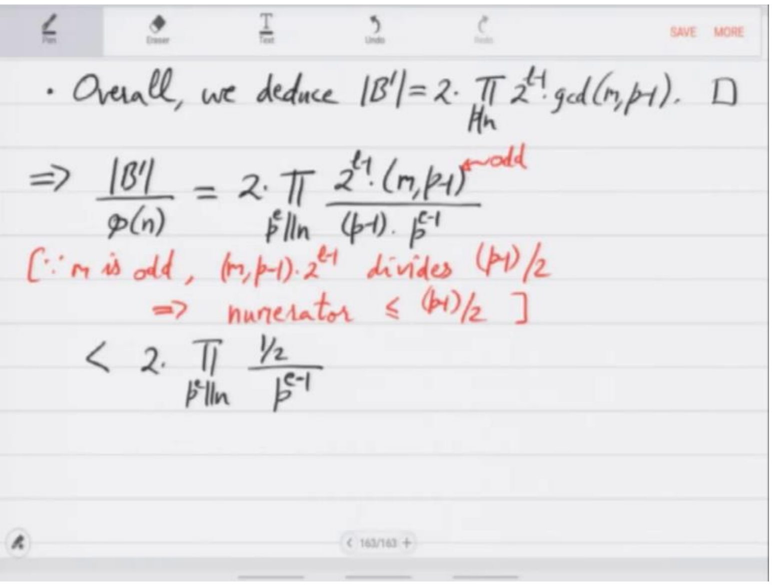
It will actually follow from we will follow Chinese remaindering theorem to get this. First analyze or estimate the number of a's such that a m 2 l - 1 is 1 and then we will estimate equal to - 1 these are the 2 options right. So what is this? And What is this? This is let us go over different primes and do Chinese remaindering so this will be a mod p raise to e star how many a's are there in this subgroup?

This is a subgroup of z mod and z mod n star right so we are doing Chinese remaindering. So how many a's are in this such that a raised 2 m 2 l - 1 is 1 mod p raised to e product over this number. Here it will be important that z mod p raised to e star is cycling so this number will come out to be basically think of a generator of z mod p raise to e star and it will have order phi of p raise to e.

So take the gcd of this with phi of p raise to e. So generator g has order phi of p raised to e how many powers of that will give you such a's that is the question. And you will get it by taking the gcd with m 2 raised to l - 1 you can show this as an exercise. Since this is cyclic. So that is why this is a very precise estimate which we can further simplify. So now we take product of primes over n primes dividing n so you get gcd of m 2 raised to l - 1 and p raised to e - 1 p - 1. Well p is co prime to both m and 2 so this can be dropped periods 2 - 1 can be dropped first.

And next thing is what to do with 2 raise to l - 1 does it divide p - 1 yes in fact 2 raised to l divides all the p - 1's right. So 2 raised to l - 1 divides p - 1 so we can further simplify this as this so we have estimated the number of aces that a raise to that exponent is 1 mod n. Find how many of these will be – 1? So the -1 number actually will also come out to be the same. So we just have to double this.

(Refer Slide Time: 01:00:38)



- Overall, we deduce $|B'| = 2 \cdot \prod_{p|n} 2^{\ell-1} \cdot \gcd(m, p-1)$. □

$$\Rightarrow \frac{|B'|}{\varphi(n)} = 2 \cdot \prod_{p^e \| n} \frac{2^{\ell-1} \cdot (m, p-1)}{(p-1) \cdot p^{e-1}} \leftarrow \text{odd}$$

[$\because m$ is odd, $(m, p-1) \cdot 2^{\ell-1}$ divides $(p-1)/2$

$\Rightarrow$ numerator $\leq (p-1)/2$]

$$< 2 \cdot \prod_{p^e \| n} \frac{1/2}{p^{e-1}}$$

So overall we deduce that the size of b prime is twice what we just calculated. So that is the expression. Now let us look at the ratio of this B prime size with phi n what is the ratio. So phi n can also be factored over the primes. So what you will get is 2 raised to l - 1 times the gcd of m and p - 1 in the numerator and in the denominator you will get p raised to e – 1. So we are actually doing it over prime powers.

Prime powers that exactly divide n so since m is odd note that m, p - 1 so m comma p - 1 times 2 raised to l - 1 will divide p - 1 by 2 because p - 1 by 2 is divisible by 2 raised to l - 1 which is all that appears in numerator 2 is 12 - 1 appears the remaining part is odd so this part is odd so hence the numerator divides p - 1 by 2 so which means that so it is smaller than p - 1 by 2 right.

So from since the numerator is smaller than p - 1 by 2 we actually get an estimate of this we put half here and p raised to e - 1 here. So we will proceed in the next class. Soon we will get that this number this you can see that it is it seems to be quite small. We will just have to look at some cases and actually formally prove that in all cases it is less than at most 1 by 4.