Primality Testing : AKS Algorithm

Sumit Sidana, PhD CSE

Paper by
Manindra Aggarwal,
Neeraj Kayal and Nitin Saxena

Outline

1. Idea
2. Algorithm and Its Correctness

Generalization of Fermat's Little Theorem

Important Result

Generalization of Fermat's Little Theorem

Important Result

- Let $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $n \geq 2$, $(a, n) =$ 1.*Then n is prime if and only if* $(X + a)^n = X^n + a(mod\ n)$.
  Proof. For 0<i<n,the coeffecient of x^i in $((X + a)^n - (X^n + a)$ *is* $\binom{n}{i} a^{n-i}$.
  Suppose n is prime.Then $\binom{n}{i} = 0(modn)$ and hence all coeffecients are zero .
  Suppose n is composite. Consider a prime q that is a factor of n and let $q^k | n$ .Then q^k does not divide $\binom{n}{q}$ and is coprime to a^{n-q} and hence the coeffecient of X^q is not zero(mod n).
  Thus $((X + a)^n - (X^n + a)$ is not identically zero over $\mathbb{Z}_n$

Problem

- However , the above test takes time Ω(n) because we need to evaluate n coeffecients in the LHS in the worst case .
- There are two problems which we are facing right now :
  -Evaluating $(X + a)^n$ *requires n multiplications*.
  -$(X + a)^n$ has n+1 coeffecients which take $\omega(n)$ time in worst case to evaluate .

Solutions to Problems

Solutions

Solutions to Problems

Solutions

- Use repeated Squaring to calculate $(X + a)^n$.

Solutions to Problems

Solutions

- Use repeated Squaring to calculate $(X + a)^n$.
- Evaluate both sides of (1) modulo a polynomial of the form $X^r - 1$ for an appropriately chosen r .

Solutions to Problems

Solutions

- Use repeated Squaring to calculate $(X + a)^n$.
- Evaluate both sides of (1) modulo a polynomial of the form $X^r - 1$ for an appropriately chosen r .
- Test if the following equation is satisfied $(X + a)^n = X^n + a(mod\ X^r - 1, n)$

Solutions to Problems

Solutions

- Use repeated Squaring to calculate $(X+a)^n$.
- Evaluate both sides of (1) modulo a polynomial of the form $X^r - 1$ for an appropriately chosen r .
- Test if the following equation is satisfied
  $(X+a)^n = X^n + a(mod\ X^r - 1, n)$
- All Primes n satisfy the equation for all values of a and r .

Solutions to Problems

Solutions

- Use repeated Squaring to calculate $(X + a)^n$.
- Evaluate both sides of (1) modulo a polynomial of the form $X^r - 1$ for an appropriately chosen r .
- Test if the following equation is satisfied $(X + a)^n = X^n + a(mod\ X^r - 1, n)$
- All Primes n satisfy the equation for all values of a and r .
- Problem Now is that some composites n may also satisfy the equation for few values of a and r .

Solution to the above Problem

- We show for an appropriately chosen r if the equation is satisfied for several a's then n must be a prime power .
- The number of a's and the appropriate r are both bounded by a polynomial in log n.

Outline

1. Idea
2. Algorithm and Its Correctness

Algorithm

Algorithm

Input: Integer n $>$ 1 .

1. If $(n = \ a^b \ for \ a \in \mathbb{N} \ and \ b > 1), \ output \ COMPOSITE.$

2.Find the smallest r such that $o_r(n) \ > \ log^2 n.$

3.If 1 $<$(a,n)$<$n for some a$\leq$r output COMPOSITE .

4.If n $\leq$ r ,output PRIME .

5.For a $=$ 1 to $\lfloor 2\sqrt{r} log(n) \rfloor do$

$if \ ((X \ + \ a)^n \neq X^n \ + \ a(mod \ X^r \ - \ 1, n)), output \ COMPOSITE;$

6.Output Prime .

If n is prime then Algorithm Returns Prime .

If n is prime then Algorithm Returns Prime .

1. If ($n = a^b$ *for* $a \in \mathbb{N}$ *and* $b > 1$), *output COMPOSITE*.
2. Find the smallest r such that $o_r(n) > log^2 n$.
3. If 1 <(a,n)<n for some a≤r output COMPOSITE .
4. If n $\leq$ r ,output PRIME .
5. For a = 1 to $2\sqrt{r}log(n)do$

   $if\ ((X + a)^n \neq X^n + a(mod\ X^r - 1, n)), output\ COMPOSITE;$
6. Output Prime .

If n is prime then Algorithm Returns Prime .

If n is prime then Algorithm Returns Prime .

1. If $(n = \ a^b \ for \ a \in \mathbb{N} \ and \ b > 1)$, $output \ COMPOSITE$.
2.Find the smallest r such that $o_r(n) \ > \ log^2 n$.
3.If 1 <(a,n)<n for some a≤r output COMPOSITE .
4.If n $\leq$ r ,output PRIME .
5.For a = 1 to $2\sqrt{r}log(n)do$
$if \ ((X \ + \ a)^n \neq X^n \ + \ a(mod \ X^r \ - \ 1, n)), output \ COMPOSITE;$
6.Output Prime .

- If n is prime steps (1),(3) and (5) cannot return Composite .Then Either Step (4) or (6) is going to output prime .

If n is prime then Algorithm Returns Prime .

If n is prime then Algorithm Returns Prime .

1. If ($n = a^b$ *for* $a \in \mathbb{N}$ *and* $b > 1$), *output COMPOSITE*.
2. Find the smallest r such that $o_r(n) > log^2 n$.
3. If 1 <(a,n)<n for some a≤r output COMPOSITE .
4. If n $\leq$ r ,output PRIME .
5. For a = 1 to $2\sqrt{r} log(n) do$
   if $((X + a)^n \neq X^n + a (mod\ X^r - 1, n))$, *output COMPOSITE*;
6. Output Prime .

- If n is prime steps (1),(3) and (5) cannot return Composite .Then Either Step (4) or (6) is going to output prime .
- If step(4) returns prime then n must be prime .

If n is prime then Algorithm Returns Prime .

If n is prime then Algorithm Returns Prime .

1. If $(n = a^b \; for \; a \in \mathbb{N} \; and \; b > 1)$, *output COMPOSITE*.
2.Find the smallest r such that $o_r(n) > log^2 n$.
3.If 1 <(a,n)<n for some a≤r output COMPOSITE .
4.If n $\leq$ r ,output PRIME .
5.For a = 1 to $2\sqrt{r}log(n)do$
$if \; ((X + a)^n \neq X^n + a(mod \; X^r - 1, n)), output \; COMPOSITE;$
6.Output Prime .

- If n is prime steps (1),(3) and (5) cannot return Composite .Then Either Step (4) or (6) is going to output prime .
- If step(4) returns prime then n must be prime .
- If it would not have been prime then step(3) would have found a prime p|n output COMPOSITE.

If n is prime then Algorithm Returns Prime .

If n is prime then Algorithm Returns Prime .

1. If ($n = a^b$ *for* $a \in \mathbb{N}$ *and* $b > 1$), *output COMPOSITE*.
2.Find the smallest r such that $o_r(n) > log^2 n$.
3.If 1 <(a,n)<n for some a≤r output COMPOSITE .
4.If n ≤ r ,output PRIME .
5.For a = 1 to $2\sqrt{r} log(n) do$
$if\ ((X + a)^n \neq X^n + a(mod\ X^r - 1, n)), output\ COMPOSITE;$
6.Output Prime .

- If n is prime steps (1),(3) and (5) cannot return Composite .Then Either Step (4) or (6) is going to output prime .
- If step(4) returns prime then n must be prime .
- If it would not have been prime then step(3) would have found a prime p|n output COMPOSITE.
- Therefore, algorithm returns prime if n is prime .

More Observations

Observations

1. If $(n = \ a^b \ for \ a \in \mathbb{N} \ and \ b > 1), \ output \ COMPOSITE.$
2.Find the smallest r such that $o_r(n) \ > \ log^2 n.$
3.If 1 <(a,n)<n for some a$\leq$r output COMPOSITE .
4.If n $\leq$ r ,output PRIME .
5.For a = 1 to $2\sqrt{r}log(n)do$
$if \ ((X \ + \ a)^n \neq X^n \ + \ a(mod \ X^r \ - \ 1, n)), output \ COMPOSITE;$
6.Output Prime .

More Observations

Observations

1. If ($n = \ a^b$ *for* $a \in \mathbb{N}$ *and* $b > 1$), *output COMPOSITE*.
2.Find the smallest r such that $o_r(n) \ > \ log^2 n$.
3.If 1 <(a,n)<n for some a≤r output COMPOSITE .
4.If n $\leq$ r ,output PRIME .
5.For a = 1 to $2\sqrt{r} log(n) do$
if $((X \ + \ a)^n \neq X^n \ + \ a(mod \ X^r \ - \ 1, n))$, *output COMPOSITE*;
6.Output Prime .

- If the algorithm does not halt after step(3) or step(4) then following observations are evident :

More Observations

Observations

1. If $(n = a^b$ for $a \in \mathbb{N}$ and $b > 1)$, $output$ $COMPOSITE$.
2.Find the smallest r such that $o_r(n) > log^2 n$.
3.If 1 <(a,n)<n for some a≤r output COMPOSITE .
4.If n ≤ r ,output PRIME .
5.For a = 1 to $2\sqrt{r} log(n) do$
if $((X + a)^n \neq X^n + a(mod\ X^r - 1, n)), output\ COMPOSITE;$
6.Output Prime .

- If the algorithm does not halt after step(3) or step(4) then following observations are evident :
- n > r

More Observations

Observations

1. If $(n = \ a^b \ for \ a \in \mathbb{N} \ and \ b > 1), \ output \ COMPOSITE.$
2.Find the smallest r such that $o_r(n) \ > \ log^2 n.$
3.If 1 <(a,n)<n for some a≤r output COMPOSITE .
4.If n ≤ r ,output PRIME .
5.For a = 1 to $2\sqrt{r}log(n)do$
$if \ ((X \ + \ a)^n \neq X^n \ + \ a(mod \ X^r \ - \ 1, n)), output \ COMPOSITE;$
6.Output Prime .

- If the algorithm does not halt after step(3) or step(4) then following observations are evident :
- n > r
- There must exist a prime divisor p of n such that p> r.

More Observations

Observations

1. If $(n = \ a^b \ for \ a \in \mathbb{N} \ and \ b > 1), \ output \ COMPOSITE.$
2.Find the smallest r such that $o_r(n) \ > \ log^2 n.$
3.If 1 <(a,n)<n for some a$\leq$r output COMPOSITE .
4.If n $\leq$ r ,output PRIME .
5.For a = 1 to $2\sqrt{r} log(n) do$
$if \ ((X \ + \ a)^n \neq X^n \ + \ a(mod \ X^r \ - \ 1, n)), output \ COMPOSITE;$
6.Output Prime .

- If the algorithm does not halt after step(3) or step(4) then following observations are evident :
- n > r
- There must exist a prime divisor p of n such that p> r.
- (n,r) = 1 $\Rightarrow \ p, n \in Z_r^*$

More Observations

Observations

1. If ($n = a^b$ *for* $a \in \mathbb{N}$ *and* $b > 1$), *output COMPOSITE*.
2. Find the smallest r such that $o_r(n) > log^2 n$.
3. If 1 <(a,n)<n for some a$\leq$r output COMPOSITE .
4. If n $\leq$ r ,output PRIME .
5. For a = 1 to $2\sqrt{r}log(n) do$
   if $((X + a)^n \neq X^n + a(mod\ X^r - 1, n)), output\ COMPOSITE;$
6. Output Prime .

- If the algorithm does not halt after step(3) or step(4) then following observations are evident :
- n > r
- There must exist a prime divisor p of n such that p> r.
- (n,r) = 1 $\Rightarrow$ $p, n \in Z_r^*$
- Also let $l = 2\sqrt{r}log\ n$.

General Definitions

Introspective Numbers

Call a number m introspective if
$(X + a)^m = X^m + a(mod\ X^r - 1, p) \forall 1 \leq a \leq l.$

General Definitions

Introspective Numbers

Call a number m introspective if
$(X + a)^m = X^m + a(mod\ X^r - 1, p) \forall 1 \leq a \leq l.$

- If m_1 *and* m_2 are introspective numbers then so is $m_1 m_2$

General Definitions

Introspective Numbers

Call a number m introspective if
$(X + a)^m = X^m + a(mod\ X^r - 1, p) \forall 1 \leq a \leq l.$

- If $m_1\ and\ m_2$ are introspective numbers then so is $m_1 m_2$
- Proof-
  $(X + a)^{m_2} - (X^{m_2} + a) = (X^r - 1)g(x)\ +\ p.h(x)$ for some g(x),p(x)

$$\begin{aligned} \Rightarrow & (X^{m_1} + a)^{m_2} - (X^{m_1 m_2} + a) \\ & = (X^{m_1 r} - 1)g(X^{m_1}) +\ p.h(X^{m_1}) \\ & = 0(mod\ X^r - 1, p) \end{aligned}$$

$$\Rightarrow (X + a)^{m_1 m_2} = (X^{m_1} + a)^{m_2}$$

p and n as Introspective Numbers .

Numbers of the form $p^i n^j$

p and n as Introspective Numbers .

Numbers of the form $p^i n^j$

- If algorithm outputs Composite at step (5) then we are done .

p and n as Introspective Numbers .

Numbers of the form $p^i n^j$

- If algorithm outputs Composite at step (5) then we are done .
- If the algorithm does not output Composite at step(5) then such n has verified l equations .

p and n as Introspective Numbers .

Numbers of the form $p^i n^j$

- If algorithm outputs Composite at step (5) then we are done .
- If the algorithm does not output Composite at step(5) then such n has verified l equations .
- $(X + a)^n = X^n + a(mod\ X^r - 1, n) 0 \leq a \leq l.$

p and n as Introspective Numbers .

Numbers of the form $p^i n^j$

- If algorithm outputs Composite at step (5) then we are done .
- If the algorithm does not output Composite at step(5) then such n has verified l equations .
- $(X + a)^n = X^n + a(mod\ X^r - 1, n) 0 \leq a \leq l.$
- This implies $(X + a)^n = X^n + a(mod\ X^r - 1, p)$

p and n as Introspective Numbers .

Numbers of the form $p^i n^j$

- If algorithm outputs Composite at step (5) then we are done .
- If the algorithm does not output Composite at step(5) then such n has verified l equations .
- $(X+a)^n = X^n + a(mod\ X^r - 1, n) 0 \leq a \leq l.$
- This implies $(X+a)^n = X^n + a(mod\ X^r - 1, p)$
- and For Prime Factor of n ,p we have : $(X+a)^p = X^p + a(mod\ X^r - 1, p).$

p and n as Introspective Numbers .

Numbers of the form $p^i n^j$

- If algorithm outputs Composite at step (5) then we are done .
- If the algorithm does not output Composite at step(5) then such n has verified l equations .
- $(X+a)^n = X^n + a(mod\ X^r - 1, n) 0 \leq a \leq l.$
- This implies $(X+a)^n = X^n + a(mod\ X^r - 1, p)$
- and For Prime Factor of n ,p we have : $(X+a)^p = X^p + a(mod\ X^r - 1, p).$
- Hence for each m of the form $p^i n^j$ we have $(X+a)^m = X^m + a\ for\ a = 1...l$

Two sets I and P

We now define two sets I and P .

- $I \quad = (n^i.p^j | i, j \geq 0)$.

Two sets I and P

We now define two sets I and P .

- $I \ = (n^i.p^j|i,j \geq 0)$.
- $P = \ (\prod_{a=0}^{l}(X+a)^{e_a}|e_a \geq 0)$.

Two sets I and P

We now define two sets I and P .

- $I \;\; = (n^i.p^j | i, j \geq 0)$.
- $P = \;\; (\prod_{a=0}^{l} (X + a)^{e_a} | e_a \geq 0)$.
- Clearly ,Every member of set I is introspective for every member of set P .

Two sets I and P

We now define two sets I and P .

- $I \; = (n^i.p^j | i,j \geq 0)$.
- $P = \; (\prod_{a=0}^{l} (X+a)^{e_a} | e_a \geq 0)$.
- Clearly ,Every member of set I is introspective for every member of set P .
- Also, let Î$= p^i n^j | 0 \leq i,j \leq \sqrt{t}$.

Groups G and field F

- We define a group G $= n^i p^j$ $modulo$ r and let t be the order of this group .

Groups G and field F

- We define a group G = $n^i p^j$ $modulo$ r and let t be the order of this group .
- Let $Q_r(X)$ be the r^th cyclotomic polynomial over F_p.

Groups G and field F

- We define a group G = $n^i p^j$ *modulo* r and let t be the order of this group .
- Let $Q_r(X)$ be the r^th cyclotomic polynomial over F_p.
- Polynomial $Q_r(X)$ divides $X^r - 1$ and factors into irreducible factors of degree $o_r(p)$.

Groups G and field F

- We define a group G = $n^i p^j$ *modulo* r and let t be the order of this group .
- Let $Q_r(X)$ be the r^th cyclotomic polynomial over F_p.
- Polynomial $Q_r(X)$ divides $X^r - 1$ and factors into irreducible factors of degree $o_r(p)$.
- Let h(x) be one such irreducible factor .

Groups G and field F

- We define a group G $= n^i p^j$ *modulo* r and let t be the order of this group .
- Let $Q_r(X)$ be the $r^t h$ cyclotomic polynomial over F_p.
- Polynomial $Q_r(X)$ divides $X^r - 1$ and factors into irreducible factors of degree $o_r(p)$.
- Let h(x) be one such irreducible factor .
- Since $o_r(p) > 1$,degree of h(X) is greater than 1 .

Groups G and field F

- We define a group G = $n^i p^j$ *modulo* r and let t be the order of this group .
- Let $Q_r(X)$ be the $r^t h$ cyclotomic polynomial over F_p.
- Polynomial $Q_r(X)$ divides $X^r - 1$ and factors into irreducible factors of degree $o_r(p)$.
- Let h(x) be one such irreducible factor .
- Since $o_r(p) > 1$,degree of h(X) is greater than 1 .
- Let F be field which consists of the set of all residues of Polynomials in P modulo h(X) .

Some Results

- Clearly, $t \geq ord_r(n)$

Some Results

- Clearly, $t \geq ord_r(n)$
- Any $m \in \hat{I}$ is atmost $n^{2\sqrt{t}}$

Some Results

- Clearly, $t \geq ord_r(n)$
- Any $m \in \hat{\mathrm{I}}$ is atmost $n^{2\sqrt{t}}$
- $|\hat{\mathrm{I}}| = (\sqrt{t}+1)^2 > t.$

Some Results

- Clearly, $t \geq ord_r(n)$
- Any $m \in$Î is atmost $n^{2\sqrt{t}}$
- $|$Î$| = (\sqrt{t} + 1)^2 > t$.
- Since |G| =t ,at least two numbers in Î must be equal modulo r .$\Rightarrow m_1 = m_2 + kr$

Some Results

- Clearly, $t \geq ord_r(n)$
- Any $m \in$Î is atmost $n^{2\sqrt{t}}$
- $|$Î$| = (\sqrt{t}+1)^2 > t.$
- Since $|$G$|$ =t ,at least two numbers in Î must be equal modulo r .$\Rightarrow m_1 = m_2 + kr$
- $(X+a)^{m_1} = (X^{m_1}+a) = (X^{m_2+kr}+a) = X^{m_2}+a = (X+a)^{m_2} (mod\ X^r\ -\ 1, p)$

Some Results

- Clearly, $t \geq ord_r(n)$
- Any $m \in$Î is atmost $n^{2\sqrt{t}}$
- $|\hat{I}| = (\sqrt{t}+1)^2 > t$.
- Since |G| =t ,at least two numbers in Î must be equal modulo r .$\Rightarrow m_1 = m_2 + kr$
- $(X+a)^{m_1} = (X^{m_1}+a) = (X^{m_2+kr}+a) = X^{m_2}+a = (X+a)^{m_2}(mod\ X^r\ -\ 1, p)$
- Consider the Polynomial $Z^{m_1} - Z^{m_2}$ has several roots namely, X+a , for a = 1,2,...,l .

Some Results

- Clearly, $t \geq ord_r(n)$
- Any $m \in$Î is atmost $n^{2\sqrt{t}}$
- $|$Î$| = (\sqrt{t} + 1)^2 > t$.
- Since $|$G$|$ =t ,at least two numbers in Î must be equal modulo r .$\Rightarrow m_1 = m_2 + kr$

- $(X + a)^{m_1} = (X^{m_1} + a) = (X^{m_2+kr} + a) = X^{m_2} + a = (X + a)^{m_2} (mod\ X^r\ -\ 1, p)$
- Consider the Polynomial $Z^{m_1} - Z^{m_2}$ has several roots namely, X+a , for a = 1,2,...,l .
- If $m_1, m_2 \in$ Î are such that $(X + a)^{m_1} = (X + a)^{m_2} (mod\ X^r - 1, p)$ for a = 1,2,...,l then we want conditions under which $m_1 = m_2$

- We want to show that it has more roots than its degree .If we can show that ,we will force $m_1 = m_2$.
- In a field , a non zero polynomial of degree d has atmost d roots .
- If we show $m_1 = m_2$ then $p^{i1}n^{j1} = p^{i2}n^{j2} \Rightarrow$ n is a prime power.

Forcing $m_1 = m_2$

- If η is the primitive r^{th} root of unity , then $\eta + a$ is the root of the equation $h(Z) = Z^{m_1} - Z^{m_2}$.

Forcing $m_1 = m_2$

- If η is the primitive r^{th} root of unity , then $\eta + a$ is the root of the equation $h(Z) = Z^{m_1} - Z^{m_2}$.
- Also note that if α and β are the roots of h then so are $\alpha\beta$.

Forcing $m_1 = m_2$

- If η is the primitive r^{th} root of unity , then $\eta\ +\ a$ is the root of the equation $h(Z) = Z^{m_1} - Z^{m_2}$.
- Also note that if α and β are the roots of h then so are $\alpha\beta$.
- Let S $= (\prod_{a=1}^{l}(\eta\ +\ a)^{e_a} | e_a \in 0, 1)$

Forcing $m_1 = m_2$

- If η is the primitive r^{th} root of unity , then $\eta \ + \ a$ is the root of the equation $h(Z) = Z^{m_1} - Z^{m_2}$.
- Also note that if α and β are the roots of h then so are $\alpha\beta$.
- Let S $= (\prod_{a=1}^{l} (\eta \ + \ a)^{e_a} | e_a \in 0, 1)$
- Each element of S is the root of h .

Forcing $m_1 = m_2$

- If η is the primitive r^{th} root of unity , then $\eta + a$ is the root of the equation $h(Z) = Z^{m_1} - Z^{m_2}$.
- Also note that if α and β are the roots of h then so are $\alpha\beta$.
- Let S $= (\prod_{a=1}^{l}(\eta + a)^{e_a} | e_a \in 0, 1)$
- Each element of S is the root of h .
- If we force number of roots to be greater than degree we get $2^l > n^{2\sqrt{t}} \Rightarrow l > 2\sqrt{t} log\ n$ Then we force $m_1 = m_2$.

Forcing $m_1 = m_2$

- If η is the primitive r^{th} root of unity , then $\eta + a$ is the root of the equation $h(Z) = Z^{m_1} - Z^{m_2}$.
- Also note that if α and β are the roots of h then so are $\alpha\beta$.
- Let S = $(\prod_{a=1}^{l}(\eta + a)^{e_a} | e_a \in 0, 1)$
- Each element of S is the root of h .
- If we force number of roots to be greater than degree we get $2^l > n^{2\sqrt{t}} \Rightarrow l > 2\sqrt{t}log\ n$ Then we force $m_1 = m_2$.
- Now we need to force each root of S to be distinct for above claim to be true .

Background for Bounds on r

- If we take our earlier $P = \prod_{a=0}^{l}(X+a)^{e_a} | e_a \geq 0$ they are all distinct polynomials of $F_p[X]$ if a=1....l do not divide n (and p)

Background for Bounds on r

- If we take our earlier $P = \prod_{a=0}^{l}(X + a)^{e_a} | e_a \geq 0$ they are all distinct polynomials of $F_p[X]$ if a=1....l do not divide n (and p)
- But this can be shown : $l = 2\sqrt(r) log\ n \leq r\ and\ p > r$.

Background for Bounds on r

- If we take our earlier $P = \prod_{a=0}^{l}(X+a)^{e_a}|e_a \geq 0$ they are all distinct polynomials of $F_p[X]$ if a=1....l do not divide n (and p)
- But this can be shown : $l = 2\sqrt{(}r)log\ n \leq r\ and\ p > r.$
- We also need to show : If $f(X)\ and\ g(X)$ are two distinct elements of P ,then so are $g(\eta)\ andf(\eta)$

Background for Bounds on r

- If we take our earlier $P = \prod_{a=0}^{l}(X+a)^{e_a}|e_a \geq 0$ they are all distinct polynomials of $F_p[X]$ if a=1....l do not divide n (and p)
- But this can be shown : $l = 2\sqrt(r)log\ n \leq r\ and\ p > r.$
- We also need to show : If $f(X)\ and\ g(X)$ are two distinct elements of P ,then so are $g(\eta)\ andf(\eta)$
- Proof - For every $m = p^i n^j,\ g(X)^m = g(X^m)(modX^r - 1, p)$. Hence if $f(X)$ and $g(X)$ are two distinct elements of P such that $f(\eta) = g(\eta) \Rightarrow g(\eta)^m = g(\eta^m) = f(\eta)^m = f(\eta^m)$

Background for Bounds on r

- If we take our earlier $P = \prod_{a=0}^{l}(X+a)^{e_a} | e_a \geq 0$ they are all distinct polynomials of $F_p[X]$ if a=1....l do not divide n (and p)
- But this can be shown : $l = 2\sqrt(r)log\ n \leq\ r\ and\ p > r.$
- We also need to show : If $f(X)\ and\ g(X)$ are two distinct elements of P ,then so are $g(\eta)\ andf(\eta)$
- Proof - For every $m = p^i n^j,\ g(X)^m = g(X^m)(modX^r - 1, p)$. Hence if $f(X)$ and $g(X)$ are two distinct elements of P such that $f(\eta) = g(\eta) \Rightarrow g(\eta)^m = g(\eta^m) = f(\eta)^m = f(\eta^m)$
- This shows η^m is the root of $Q(X) = f(X) - g(X)\ for\ every\ m \in G$.

Background for Bounds on r

- If we take our earlier $P = \prod_{a=0}^{l}(X+a)^{e_a} | e_a \geq 0$ they are all distinct polynomials of $F_p[X]$ if a=1....l do not divide n (and p)
- But this can be shown : $l = 2\sqrt(r) log\ n \leq r\ and\ p > r$.
- We also need to show : If $f(X)\ and\ g(X)$ are two distinct elements of P ,then so are $g(\eta)\ andf(\eta)$
- Proof - For every $m = p^i n^j,\ g(X)^m = g(X^m)(modX^r - 1, p)$. Hence if $f(X)$ and $g(X)$ are two distinct elements of P such that $f(\eta) = g(\eta) \Rightarrow g(\eta)^m = g(\eta^m) = f(\eta)^m = f(\eta^m)$
- This shows η^m is the root of $Q(X) = f(X) - g(X)\ for\ every\ m \in G$.
- So there are at least t roots of Q(X) in F.

- Since these polynomials are of degree atmost l If we ensure that t > l ,we show Q(X) = 0⇒ f(X) = g(X)
- We want to ensure t > $l \;=\; 2\sqrt{r} log\;\; n > 2\sqrt{t} log\;\; n \Rightarrow t > 4(log^2 n) + 2 \;and\; since\; t \;\;>\;\; ord_r(n)$
- It is enough to show $ord_r(n) > 4(log^2 n) + 2$.

Finding such an r

- LCM of 1,2,3,.....2k+1 numbers is at least 2^{2k}.

Finding such an r

- LCM of 1,2,3,.....2k+1 numbers is at least 2^{2k}.
- Suppose we run through all r till some odd number say R and fail to get one such that $ord_r(n) > T = 4(log^2 n) + 2$.

Finding such an r

- LCM of 1,2,3,.....2k+1 numbers is at least 2^{2k}.
- Suppose we run through all r till some odd number say R and fail to get one such that $ord_r(n) > T = 4(log^2 n) + 2$.
- $\Rightarrow \ for\ each\ r \ \leq \ R\ n^i mod\ r \ = \ 1\ for\ some\ i \ < \ R$

Finding such an r

- LCM of 1,2,3,.....2k+1 numbers is at least 2^{2k}.
- Suppose we run through all r till some odd number say R and fail to get one such that $ord_r(n) > T = 4(log^2 n) + 2$.
- $\Rightarrow$ *for each* $r \leq R$ $n^i mod\ r = 1$ *for some* $i < R$
- Each $r \leq R$ divides $\prod_{i=0}^{T}(n^i - 1) \leq n^{T^2}$ and hence LCM of all r $\leq$ R divides it .

Finding such an r

- LCM of 1,2,3,.....2k+1 numbers is at least 2^{2k}.
- Suppose we run through all r till some odd number say R and fail to get one such that $ord_r(n) > T = 4(log^2 n) + 2$.
- $\Rightarrow$ *for each* $r \leq R$ $n^i mod\ r = 1$ *for some* $i < R$
- Each $r \leq R$ divides $\prod_{i=0}^{T}(n^i - 1) \leq n^{T^2}$ and hence LCM of all r $\leq$ R divides it .
- By the first result on LCM $2^{R-1} \leq n^{T^2}$ that is $R \leq T^2 log\ n + 1$.

Finding such an r

- LCM of 1,2,3,.....2k+1 numbers is at least 2^{2k}.
- Suppose we run through all r till some odd number say R and fail to get one such that $ord_r(n) > T = 4(log^2 n) + 2$.
- $\Rightarrow$ *for each* $r \leq R\ n^i mod\ r = 1$ *for some* $i < R$
- Each $r \leq R$ divides $\prod_{i=0}^{T}(n^i - 1) \leq n^{T^2}$ and hence LCM of all r $\leq$ R divides it .
- By the first result on LCM $2^{R-1} \leq n^{T^2}$ that is $R \leq T^2 log\ n + 1$.
- Therefore if we take $r > T^2 log\ n + 1$,we are sure to r such that $ord_r(n) \geq T = 4log^2\ n + 2$.

Finding such an r

- LCM of 1,2,3,.....2k+1 numbers is at least 2^{2k}.
- Suppose we run through all r till some odd number say R and fail to get one such that $ord_r(n) > T = 4(log^2 n) + 2$.
- $\Rightarrow$ *for each* $r \leq R \; n^i mod \; r = 1$ *for some* $i < R$
- Each $r \leq R$ divides $\prod_{i=0}^{T}(n^i - 1) \leq n^{T^2}$ and hence LCM of all r $\leq$ R divides it .
- By the first result on LCM $2^{R-1} \leq n^{T^2}$ that is $R \leq T^2 log \; n + 1$.
- Therefore if we take $r > T^2 log \; n + 1$,we are sure to r such that $ord_r(n) \geq T = 4log^2 \; n + 2$.
- Hence there is a number r $=$ O($log^5 \; n) \geq T$.