A Short History of "PRIMES is in P"

Manindra Agrawal

IIT Kanpur

ICALP 2006

Overview

1. August 1998: A Question
2. August 1998 – January 1999: Primality Testing as Identity Testing
3. February 1999: A Conjecture
4. March 1999 – July 2000: Failed Attempts at Proof
5. August 2000 – December 2002: Experiments
6. January 2002 - July 2002: Another Attempt at Proof

Outline

1. August 1998: A Question
2. August 1998 – January 1999: Primality Testing as Identity Testing
3. February 1999: A Conjecture
4. March 1999 – July 2000: Failed Attempts at Proof
5. August 2000 – December 2002: Experiments
6. January 2002 - July 2002: Another Attempt at Proof

An Intriguing Identity Test

- Let $P(x_1, \ldots, x_n)$ be a degree n polynomial over $\mathbb{Q}$ given as an arithmetic circuit.
- Chen and Kao (1997) showed that there exist, easily computable, irrational numbers α_1, ..., α_n such that

$$P = 0 \;\Leftrightarrow\; P(\alpha_1, \ldots, \alpha_n) = 0.$$

- They also showed that
  - A random rational approximation to α_i's works with high probability.
  - The error can be reduced by increasing the quality of approximation without increasing the number of random bits.
- This yields a novel time-error tradeoff.

An Intriguing Identity Test

- Let $P(x_1, \ldots, x_n)$ be a degree n polynomial over $\mathbb{Q}$ given as an arithmetic circuit.
- Chen and Kao (1997) showed that there exist, easily computable, irrational numbers $\alpha_1, \ldots, \alpha_n$ such that

$$P = 0 \Leftrightarrow P(\alpha_1, \ldots, \alpha_n) = 0.$$

- They also showed that
  - A random rational approximation to α_i's works with high probability.
  - The error can be reduced by increasing the quality of approximation without increasing the number of random bits.
- This yields a novel time-error tradeoff.

An Intriguing Identity Test

- Let $P(x_1, \ldots, x_n)$ be a degree n polynomial over $\mathbb{Q}$ given as an arithmetic circuit.
- Chen and Kao (1997) showed that there exist, easily computable, irrational numbers α_1, ..., α_n such that

$$P = 0 \Leftrightarrow P(\alpha_1, \ldots, \alpha_n) = 0.$$

- They also showed that
  - A random rational approximation to α_i's works with high probability.
  - The error can be reduced by increasing the quality of approximation without increasing the number of random bits.
- This yields a novel time-error tradeoff.

An Intriguing Identity Test

- Let $P(x_1, \ldots, x_n)$ be a degree n polynomial over $\mathbb{Q}$ given as an arithmetic circuit.
- Chen and Kao (1997) showed that there exist, easily computable, irrational numbers α_1, …, α_n such that

$$P = 0 \;\Leftrightarrow\; P(\alpha_1, \ldots, \alpha_n) = 0.$$

- They also showed that
  - A random rational approximation to α_i's works with high probability.
  - The error can be reduced by increasing the quality of approximation without increasing the number of random bits.
- This yields a novel time-error tradeoff.

An Intriguing Identity Test

Somenath Biswas: Professor at IITK

- Lewis and Vadhan (1998) designed a similar test for identities over finite fields.
- Instead of irrational numbers, they used square roots of irreducible polynomials.

A Question

Question. Are there other problems that admit similar time-error tradeoff?

In particular, what about primality testing?

A Question

Question. Are there other problems that admit similar time-error tradeoff?

In particular, what about primality testing?

Outline

FROM PRIMALITY TESTING TO IDENTITY TESTING

A reduction of primality testing to identity testing:

n is prime

iff

$$(x+1)^n = x^n + 1 \ (mod\ n).$$

Unfortunately, the polynomial above has exponential degree and so Lewis-Vadhan algorithm does not work.

From Primality Testing to Identity Testing

A reduction of primality testing to identity testing:

n is prime

iff

$$(x+1)^n = x^n + 1 \ (mod\ n).$$

Unfortunately, the polynomial above has exponential degree and so Lewis-Vadhan algorithm does not work.

A New Identity Testing Algorithm

- Let P be a univariate, degree d polynomial over finite field F_q.
- Let r be a prime such that $\text{ord}_r(q) > \log d$.
- Let $R(y) = y^t + \sum_{i=0}^{\log d} r_i \cdot y^i$ with $r_i \in_R \{0, 1\}$.

Lemma

If $P(x) \neq 0$ then with probability at most $\frac{1}{t}$, $P(x) = 0 \pmod{(R(x))^r - 1}$.

A New Identity Testing Algorithm

- Let P be a univariate, degree d polynomial over finite field F_q.
- Let r be a prime such that $\text{ord}_r(q) > \log d$.
- Let $R(y) = y^t + \sum_{i=0}^{\log d} r_i \cdot y^i$ with $r_i \in_R \{0, 1\}$.

Lemma

If $P(x) \neq 0$ then with probability at most $\frac{1}{t}$, $P(x) = 0 \pmod{(R(x))^r - 1}$.

A New Identity Testing Algorithm

- Let P be a univariate, degree d polynomial over finite field F_q.
- Let r be a prime such that $\text{ord}_r(q) > \log d$.
- Let $R(y) = y^t + \sum_{i=0}^{\log d} r_i \cdot y^i$ with $r_i \in_R \{0, 1\}$.

Lemma

If $P(x) \neq 0$ then with probability at most $\frac{1}{t}$, $P(x) = 0 \ (mod\ (R(x))^r - 1)$.

Outline

A Conjecture

- Polynomial $y^r - 1$ proved very useful in reducing randomness.
- Perhaps it can be used to completely derandomize the special identity for primality testing for a small r with $\text{ord}_r(n)$ large ...

Conjecture. n is prime iff for every r, $1 \leq r \leq \log n$,

$$(x+1)^n = x^n + 1 \ (mod\ n, x^r - 1).$$

A Conjecture

- Polynomial $y^r - 1$ proved very useful in reducing randomness.
- Perhaps it can be used to completely derandomize the special identity for primality testing for a small r with $\text{ord}_r(n)$ large ...

Conjecture. n is prime iff for every r, $1 \le r \le \log n$,

$$(x+1)^n = x^n + 1 \ (mod\ n, x^r - 1).$$

Outline

1. August 1998: A Question
2. August 1998 – January 1999: Primality Testing as Identity Testing
3. February 1999: A Conjecture
4. **March 1999 – July 2000: Failed Attempts at Proof**
5. August 2000 – December 2002: Experiments
6. January 2002 - July 2002: Another Attempt at Proof

First Attempt: Using Complex Roots of Unity

- Let $\omega \in \mathbb{C}, \omega = e^{i\frac{2\pi}{r}}$.
- If $(x+1)^n = x^n + 1 \ (mod\ n, x^r - 1)$ then

$$(\omega^j + 1)^n = \omega^{jn} + 1 \ (mod\ n),$$

  for every j, $0 \leq j < r$.
- This introduces integer linear dependencies between different powers of ω modulo n.
- Can this be exploited?

First Attempt: Using Complex Roots of Unity

- Let $\omega \in \mathbb{C}, \omega = e^{i\frac{2\pi}{r}}$.
- If $(x+1)^n = x^n + 1 \ (mod\ n, x^r - 1)$ then

$$(\omega^j + 1)^n = \omega^{jn} + 1 \ (mod\ n),$$

  for every j, $0 \leq j < r$.
- This introduces integer linear dependencies between different powers of ω modulo n.
- Can this be exploited?

First Attempt: Using Complex Roots of Unity

- Let $\omega \in \mathbb{C}, \omega = e^{i\frac{2\pi}{r}}$.
- If $(x+1)^n = x^n + 1 \ (mod\ n, x^r - 1)$ then

$$(\omega^j + 1)^n = \omega^{jn} + 1 \ (mod\ n),$$

  for every j, $0 \leq j < r$.
- This introduces integer linear dependencies between different powers of ω modulo n.
- Can this be exploited?

Second Attempt: Using Derivatives

- Suppose that n is square-free and p is a prime divisor of n.
- Let $m = \frac{n}{p}$.
- If $(x+1)^n = x^n + 1 \ (mod\ n, x^r - 1)$ then

$$(x+1)^m = x^m + 1 \ (mod\ p, x^r - 1).$$

- Suppose that

$$(x+1)^m = x^m + 1 \ (mod\ p, (x^r - 1)^2).$$

- Differentiating both sides, we get

$$(x+1)^{m-1} = x^{m-1} \ (mod\ p, x^r - 1).$$

Second Attempt: Using Derivatives

- Suppose that n is square-free and p is a prime divisor of n.
- Let $m = \frac{n}{p}$.
- If $(x+1)^n = x^n + 1 \ (mod\ n, x^r - 1)$ then

$$(x+1)^m = x^m + 1 \ (mod\ p, x^r - 1).$$

- Suppose that

$$(x+1)^m = x^m + 1 \ (mod\ p, (x^r - 1)^2).$$

- Differentiating both sides, we get

$$(x+1)^{m-1} = x^{m-1} \ (mod\ p, x^r - 1).$$

Second Attempt: Using Derivatives

- Suppose that n is square-free and p is a prime divisor of n.
- Let $m = \frac{n}{p}$.
- If $(x+1)^n = x^n + 1 \ (mod\ n, x^r - 1)$ then

$$(x+1)^m = x^m + 1 \ (mod\ p, x^r - 1).$$

- Suppose that

$$(x+1)^m = x^m + 1 \ (mod\ p, (x^r - 1)^2).$$

- Differentiating both sides, we get

$$(x+1)^{m-1} = x^{m-1} \ (mod\ p, x^r - 1).$$

Second Attempt: Using Derivatives

- Suppose that n is square-free and p is a prime divisor of n.
- Let $m = \frac{n}{p}$.
- If $(x+1)^n = x^n + 1 \ (mod\ n, x^r - 1)$ then

$$(x+1)^m = x^m + 1 \ (mod\ p, x^r - 1).$$

- Suppose that

$$(x+1)^m = x^m + 1 \ (mod\ p, (x^r - 1)^2).$$

- Differentiating both sides, we get

$$(x+1)^{m-1} = x^{m-1} \ (mod\ p, x^r - 1).$$

Second Attempt: Using Derivatives

- Since the coefficient of x^0 and x^{m-1} must be the same modulo $x^r - 1$, it follows that r divides $m - 1$.
- Since $m < n$, one of the first $\log n$ numbers will not divide $m - 1$.
- This is precisely what we need!
- Unfortunately, it is not clear how to test if

$$(x+1)^m = x^m + 1 \ (mod\ p, (x^r - 1)^2).$$

- Testing

$$(x+1)^n = x^n + 1 \ (mod\ n, (x^r - 1)^2)$$

only implies

$$(x+1)^n = x^n + 1 \ (mod\ p, x^r - 1)!$$

Second Attempt: Using Derivatives

- Since the coefficient of x^0 and x^{m-1} must be the same modulo $x^r - 1$, it follows that r divides $m - 1$.
- Since $m < n$, one of the first $\log n$ numbers will not divide $m - 1$.
- This is precisely what we need!
- Unfortunately, it is not clear how to test if

$$(x+1)^m = x^m + 1 \ (mod\ p, (x^r - 1)^2).$$

- Testing

$$(x+1)^n = x^n + 1 \ (mod\ n, (x^r - 1)^2)$$

only implies

$$(x+1)^n = x^n + 1 \ (mod\ p, x^r - 1)!$$

Second Attempt: Using Derivatives

- Since the coefficient of x^0 and x^{m-1} must be the same modulo $x^r - 1$, it follows that r divides $m - 1$.
- Since $m < n$, one of the first $\log n$ numbers will not divide $m - 1$.
- This is precisely what we need!
- Unfortunately, it is not clear how to test if

$$(x+1)^m = x^m + 1 \ (mod\ p, (x^r - 1)^2).$$

- Testing

$$(x+1)^n = x^n + 1 \ (mod\ n, (x^r - 1)^2)$$

only implies

$$(x+1)^n = x^n + 1 \ (mod\ p, x^r - 1)!$$

Second Attempt: Using Derivatives

- Since the coefficient of x^0 and x^{m-1} must be the same modulo $x^r - 1$, it follows that r divides $m - 1$.
- Since $m < n$, one of the first $\log n$ numbers will not divide $m - 1$.
- This is precisely what we need!
- Unfortunately, it is not clear how to test if

$$(x+1)^m = x^m + 1 \ (mod\ p, (x^r - 1)^2).$$

- Testing

$$(x+1)^n = x^n + 1 \ (mod\ n, (x^r - 1)^2)$$

only implies

$$(x+1)^n = x^n + 1 \ (mod\ p, x^r - 1)!$$

Third Attempt: Increasing Moduli Power

- Suppose one can prove that if

$$(x+1)^n = x^n + 1 \ (mod\ n, x^{r_1} - 1),$$

and

$$(x+1)^n = x^n + 1 \ (mod\ n, x^{r_2} - 1),$$

then

$$(x+1)^n = x^n + 1 \ (mod\ n, x^{lcm(r_1,r_2)} - 1).$$

- Then, the equation holding for $1 < r \leq \log n$ implies that

$$(x+1)^n = x^n + 1 \ (mod\ n, x^{lcm(1,2,\ldots,\log n)} - 1) = x^n + 1 \ (mod\ n)$$

since $lcm(1, 2, \ldots, \log n) > n$.

- Can one prove the above product property of exponents?

Third Attempt: Increasing Moduli Power

- Suppose one can prove that if

$$(x+1)^n = x^n + 1 \ (mod\ n, x^{r_1} - 1),$$

and

$$(x+1)^n = x^n + 1 \ (mod\ n, x^{r_2} - 1),$$

then

$$(x+1)^n = x^n + 1 \ (mod\ n, x^{lcm(r_1,r_2)} - 1).$$

- Then, the equation holding for $1 < r \leq \log n$ implies that

$$(x+1)^n = x^n + 1 \ (mod\ n, x^{lcm(1,2,\ldots,\log n)} - 1) = x^n + 1 \ (mod\ n)$$

since $lcm(1, 2, \ldots, \log n) > n$.

- Can one prove the above product property of exponents?

Third Attempt: Increasing Moduli Power

- Suppose one can prove that if

$$(x+1)^n = x^n + 1 \ (mod\ n, x^{r_1} - 1),$$

and

$$(x+1)^n = x^n + 1 \ (mod\ n, x^{r_2} - 1),$$

then

$$(x+1)^n = x^n + 1 \ (mod\ n, x^{lcm(r_1,r_2)} - 1).$$

- Then, the equation holding for $1 < r \leq \log n$ implies that

$$(x+1)^n = x^n + 1 \ (mod\ n, x^{lcm(1,2,\ldots,\log n)} - 1) = x^n + 1 \ (mod\ n)$$

since $lcm(1, 2, \ldots, \log n) > n$.

- Can one prove the above product property of exponents?

Outline

Aug'00-Apr'01: Experiments on the Conjecture

Rajat Bhattacharjee: Doing PhD at Stanford

- Rajat Bhattacharjee tested the equation

$$(x+1)^n = x^n + 1 \ (mod\ n, x^r - 1)$$

for all $n \leq 10^8$ and $r \leq 100$.

- He found that for composite n, all r's that satisfy the equation satisfy

$$n^2 = 1 \ (mod\ r).$$

Aug'00-Apr'01: Experiments on the Conjecture

Rajat Bhattacharjee: Doing PhD at Stanford

- Rajat Bhattacharjee tested the equation

$$(x+1)^n = x^n + 1 \ (mod\ n, x^r - 1)$$

for all $n \leq 10^8$ and $r \leq 100$.

- He found that for composite n, all r's that satisfy the equation satisfy

$$n^2 = 1 \ (mod\ r).$$

Aug'01-Dec'01: Experiments on the Conjecture

Neeraj Kayal and Nitin Saxena: Finishing PhD at IITK

- Neeraj Kayal and Nitin Saxena continued with the experiments.
- They went up to $n \leq 10^{10}$ and found the same property.

Aug'01-Dec'01: Experiments on the Conjecture

Neeraj Kayal and Nitin Saxena: Finishing PhD at IITK

- Neeraj Kayal and Nitin Saxena continued with the experiments.
- They went up to $n \leq 10^{10}$ and found the same property.

Outline

Jan'02: Studying Exponents Satisfying the Equation

- Let p be a prime divisor of n.
- Let I be the set of numbers m satisfying

$$(x+1)^m = x^m + 1 \ (mod \ p, x^r - 1).$$

- Let d be the order of p in F_r^*.
- Let O be the order of $x+1$ in the group $[F_p[x]/(x^r-1)]^*$.

Lemma

Let $m_1, m_2 \in I$. Then $m_1 = m_2 \ (mod \ r)$ iff $m_1 = m_2 \ (mod \ O)$.

Jan'02: Studying Exponents Satisfying the Equation

- Let p be a prime divisor of n.
- Let I be the set of numbers m satisfying

$$(x+1)^m = x^m + 1 \ (mod \ p, x^r - 1).$$

- Let d be the order of p in F_r^*.
- Let O be the order of $x+1$ in the group $[F_p[x]/(x^r-1)]^*$.

Lemma

Let $m_1, m_2 \in I$. Then $m_1 = m_2 \ (mod \ r)$ iff $m_1 = m_2 \ (mod \ O)$.

Jan'02: Studying Exponents Satisfying the Equation

- Let p be a prime divisor of n.
- Let I be the set of numbers m satisfying

$$(x+1)^m = x^m + 1 \ (mod\ p, x^r - 1).$$

- Let d be the order of p in F_r^*.
- Let O be the order of $x+1$ in the group $[F_p[x]/(x^r-1)]^*$.

Lemma

Let $m_1, m_2 \in I$. Then $m_1 = m_2 \ (mod\ r)$ iff $m_1 = m_2 \ (mod\ O)$.

Jan'02: Studying Exponents Satisfying the Equation

- So there exist **at most** r numbers in I modulo O.
- Some of these are $1, p, p^2, \ldots, p^{d-1}$.
- If n satisfies the equation, then $n, n^2, n^3, \ldots$ also belong to I.

Jan'02: Studying Exponents Satisfying the Equation

- So there exist at most r numbers in I modulo O.
- Some of these are 1, p, p^2, ..., p^{d-1}.
- If n satisfies the equation, then n, n^2, n^3, ... also belong to I.

Jan'02: Studying Exponents Satisfying the Equation

- So there exist at most r numbers in I modulo O.
- Some of these are 1, p, p^2, ..., p^{d-1}.
- If n satisfies the equation, then n, n^2, n^3, ... also belong to I.

Feb'02: If Only ...

- Suppose that $d = r - 1$ for r prime, $r > \log n$.
- And $O > p^{r-2}$.
- Now,

$$(x+1)^n = x^n + 1 \ (mod\ n, x^r - 1)$$

implies that

$$n = p^j \ (mod\ O)$$

for some $j < r - 1$.

- This gives

$$n = p^j!$$

Feb'02: If Only ...

- Suppose that $d = r - 1$ for r prime, $r > \log n$.
- And $O > p^{r-2}$.
- Now,

$$(x+1)^n = x^n + 1 \ (mod\ n, x^r - 1)$$

  implies that

$$n = p^j \ (mod\ O)$$

  for some $j < r - 1$.
- This gives

$$n = p^j!$$

Feb'02: If Only ...

- Suppose that $d = r - 1$ for r prime, $r > \log n$.
- And $O > p^{r-2}$.
- Now,

$$(x+1)^n = x^n + 1 \ (mod\ n, x^r - 1)$$

implies that

$$n = p^j \ (mod\ O)$$

for some $j < r - 1$.

- This gives

$$n = p^j!$$

Feb'02: If Only ...

- Suppose that $d = r - 1$ for r prime, $r > \log n$.
- And $O > p^{r-2}$.
- Now,

$$(x+1)^n = x^n + 1 \ (mod\ n, x^r - 1)$$

  implies that

$$n = p^j \ (mod\ O)$$

  for some $j < r - 1$.
- This gives

$$n = p^j!$$

Feb'02: If Only ...

- How can one ensure both the properties?
- To make $d = r - 1$, p must be a generator for F_r^*.
  - Artin's conjecture implies that there are several small r's for which this is the case.
  - However, proving it appears very difficult.
- To make $O > p^{r-2}$, p must be a generator for F_r^* and order of $x + 1$ in $[F_p[x]/(1 + x + \cdots + x^{r-1})]^*$ must be nearly maximum.
  - This is even harder to prove!

FEB'02: IF ONLY ...

- How can one ensure both the properties?
- To make $d = r - 1$, p must be a generator for F_r^*.
  - Artin's conjecture implies that there are several small r's for which this is the case.
  - However, proving it appears very difficult.
- To make $O > p^{r-2}$, p must be a generator for F_r^* and order of $x + 1$ in $[F_p[x]/(1 + x + \cdots + x^{r-1})]^*$ must be nearly maximum.
  - This is even harder to prove!

Feb'02: If Only ...

- How can one ensure both the properties?
- To make $d = r - 1$, p must be a generator for F_r^*.
  - Artin's conjecture implies that there are several small r's for which this is the case.
  - However, proving it appears very difficult.
- To make $O > p^{r-2}$, p must be a generator for F_r^* and order of $x + 1$ in $[F_p[x]/(1 + x + \cdots + x^{r-1})]^*$ must be nearly maximum.
  - This is even harder to prove!

Feb'02: If Only ...

- How can one ensure both the properties?
- To make $d = r - 1$, p must be a generator for F_r^*.
  - Artin's conjecture implies that there are several small r's for which this is the case.
  - However, proving it appears very difficult.
- To make $O > p^{r-2}$, p must be a generator for F_r^* and order of $x + 1$ in $[F_p[x]/(1 + x + \cdots + x^{r-1})]^*$ must be nearly maximum.
  - This is even harder to prove!

Mar'02-Apr'02: How Large d Can One Provably Get?

- Consider primes r with $r-1$ containing a prime factor $q_r \geq \sqrt{r}$.
- If q_r divides $\mathrm{ord}_r(n)$ then q_r will divide at least one of $\mathrm{ord}_r(p)$ for prime divisors p of n.
- In addition, there are not many r's for which q_r does not divide $\mathrm{ord}_r(n)$.
- Easy estimates on prime densities show that there exists an $r = \log^{O(1)} n$ and a prime divisor p of n such that $d = \mathrm{ord}_r(p) \geq \sqrt{r}$.

Mar'02-Apr'02: How Large d Can One Provably Get?

- Consider primes r with $r-1$ containing a prime factor $q_r \geq \sqrt{r}$.
- If q_r divides $\text{ord}_r(n)$ then q_r will divide at least one of $\text{ord}_r(p)$ for prime divisors p of n.
- In addition, there are not many r's for which q_r does not divide $\text{ord}_r(n)$.
- Easy estimates on prime densities show that there exists an $r = \log^{O(1)} n$ and a prime divisor p of n such that $d = \text{ord}_r(p) \geq \sqrt{r}$.

Mar'02-Apr'02: How Large d Can One Provably Get?

- Consider primes r with $r-1$ containing a prime factor $q_r \geq \sqrt{r}$.
- If q_r divides $\mathrm{ord}_r(n)$ then q_r will divide at least one of $\mathrm{ord}_r(p)$ for prime divisors p of n.
- In addition, there are not many r's for which q_r does not divide $\mathrm{ord}_r(n)$.
- Easy estimates on prime densities show that there exists an $r = \log^{O(1)} n$ and a prime divisor p of n such that $d = \mathrm{ord}_r(p) \geq \sqrt{r}$.

May'02: How Large O Can One Provably Get?

- Obtaining any reasonable lower bound on O appears hard.
- It becomes easy if one changes the view slightly:
  - Instead of testing the equation only for $x+1$, test it for $x+a$ for several a's.
- A similar equation will now hold for all products of $x+a$'s as well!

May'02: How Large O Can One Provably Get?

- Obtaining any reasonable lower bound on O appears hard.
- It becomes easy if one changes the view slightly:
  - Instead of testing the equation only for $x + 1$, test it for $x + a$ for several a's.
- A similar equation will now hold for all products of $x + a$'s as well!

May'02: How Large O Can One Provably Get?

- Obtaining any reasonable lower bound on O appears hard.
- It becomes easy if one changes the view slightly:
  - Instead of testing the equation only for $x + 1$, test it for $x + a$ for several a's.
- A similar equation will now hold for all products of $x + a$'s as well!

May'02: How Large O Can One Provably Get?

- Let $F = F_p[x]/(h(x))$ where $h(x)$ is an irreducible factor of $1 + x + \cdots + x^{r-1}$.
- Since $\mathrm{ord}_r(p) = d$, degree of h equals d.
- All $d - 1$ products of $x + a$'s are therefore distinct in F.
- The numbers of these products is at least 2^d provided at least d $x + a$'s are used.
- The product group is cyclic in F^* and so there is a generator $g(x)$.
- Redefine O to be the order of $g(x)$ instead of $x + 1$.
- Then, $O \geq 2^d$.

May'02: How Large O Can One Provably Get?

- Let $F = F_p[x]/(h(x))$ where $h(x)$ is an irreducible factor of $1 + x + \cdots + x^{r-1}$.
- Since $\text{ord}_r(p) = d$, degree of h equals d.
- All $d - 1$ products of $x + a$'s are therefore distinct in F.
- The numbers of these products is at least 2^d provided at least d $x + a$'s are used.
- The product group is cyclic in F^* and so there is a generator $g(x)$.
- Redefine O to be the order of $g(x)$ instead of $x + 1$.
- Then, $O \geq 2^d$.

May'02: How Large O Can One Provably Get?

- Let $F = F_p[x]/(h(x))$ where $h(x)$ is an irreducible factor of $1 + x + \cdots + x^{r-1}$.
- Since $\text{ord}_r(p) = d$, degree of h equals d.
- All $d - 1$ products of $x + a$'s are therefore distinct in F.
- The numbers of these products is at least 2^d provided at least d $x + a$'s are used.
- The product group is cyclic in F^* and so there is a generator $g(x)$.
- Redefine O to be the order of $g(x)$ instead of $x + 1$.
- Then, $O \geq 2^d$.

May'02: How Large O Can One Provably Get?

- Let $F = F_p[x]/(h(x))$ where $h(x)$ is an irreducible factor of $1 + x + \cdots + x^{r-1}$.
- Since $\text{ord}_r(p) = d$, degree of h equals d.
- All $d - 1$ products of $x + a$'s are therefore distinct in F.
- The numbers of these products is at least 2^d provided at least d $x + a$'s are used.
- The product group is cyclic in F^* and so there is a generator $g(x)$.
- Redefine O to be the order of $g(x)$ instead of $x + 1$.
- Then, $O \geq 2^d$.

Jun'02: What Now?

- One can get $d \geq \sqrt{r}$ and $O \geq 2^d \geq 2^{\sqrt{r}}$.
- One needs to find a relationship between powers of n and p modulo r.
  - This translates to a relationship modulo O.
  - If the numbers involved are smaller than O, one gets a relationship over integers.
- One type of relationship is $n = p^j \ (mod\ r)$ for some j.
- This holds provided $d = r - 1$, and we then need $O > \max\{n, p^j\}$ and j can be $r - 2$.
- Is there a way to keep the numbers small?

Jun'02: What Now?

- One can get $d \geq \sqrt{r}$ and $O \geq 2^d \geq 2^{\sqrt{r}}$.
- One needs to find a relationship between powers of n and p modulo r.
  - This translates to a relationship modulo O.
  - If the numbers involved are smaller than O, one gets a relationship over integers.
- One type of relationship is $n = p^j \ (mod\ r)$ for some j.
- This holds provided $d = r - 1$, and we then need $O > \max\{n, p^j\}$ and j can be $r - 2$.
- Is there a way to keep the numbers small?

Jun'02: What Now?

- One can get $d \geq \sqrt{r}$ and $O \geq 2^d \geq 2^{\sqrt{r}}$.
- One needs to find a relationship between powers of n and p modulo r.
  - This translates to a relationship modulo O.
  - If the numbers involved are smaller than O, one gets a relationship over integers.
- One type of relationship is $n = p^j \ (mod\ r)$ for some j.
- This holds provided $d = r - 1$, and we then need $O > \max\{n, p^j\}$ and j can be $r - 2$.
- Is there a way to keep the numbers small?

Jun'02: What Now?

- One can get $d \geq \sqrt{r}$ and $O \geq 2^d \geq 2^{\sqrt{r}}$.
- One needs to find a relationship between powers of n and p modulo r.
  - This translates to a relationship modulo O.
  - If the numbers involved are smaller than O, one gets a relationship over integers.
- One type of relationship is $n = p^j \ (mod\ r)$ for some j.
- This holds provided $d = r - 1$, and we then need $O > \max\{n, p^j\}$ and j can be $r - 2$.
- Is there a way to keep the numbers small?

Jun'02: What Now?

- One can get $d \geq \sqrt{r}$ and $O \geq 2^d \geq 2^{\sqrt{r}}$.
- One needs to find a relationship between powers of n and p modulo r.
  - This translates to a relationship modulo O.
  - If the numbers involved are smaller than O, one gets a relationship over integers.
- One type of relationship is $n = p^j \ (mod\ r)$ for some j.
- This holds provided $d = r - 1$, and we then need $O > \max\{n, p^j\}$ and j can be $r - 2$.
- Is there a way to keep the numbers small?

Jun'02: What Now?

- One can get $d \geq \sqrt{r}$ and $O \geq 2^d \geq 2^{\sqrt{r}}$.
- One needs to find a relationship between powers of n and p modulo r.
  - This translates to a relationship modulo O.
  - If the numbers involved are smaller than O, one gets a relationship over integers.
- One type of relationship is $n = p^j \ (mod\ r)$ for some j.
- This holds provided $d = r - 1$, and we then need $O > \max\{n, p^j\}$ and j can be $r - 2$.
- Is there a way to keep the numbers small?

July'02: Yes, There Is!

- Consider products of the form $n^i p^j$ for $0 \le i, j \le \sqrt{r}$.
- Two of these are equal modulo r, and the maximum value is at most $n^{2\sqrt{r}}$.
- Therefore, if $O > n^{2\sqrt{r}}$, we are done.
- The bound on O is: $O \ge 2^d \ge 2^{\sqrt{r}}$ since $d \ge \sqrt{r}$.
- However, if one can prove $d \ge r^{\frac{1}{2}+\epsilon}$ for any $\epsilon > 0$ then:

$$O \ge 2^{r^{\frac{1}{2}+\epsilon}} > n^{2\sqrt{r}}$$

provided one chooses $r > \log^{\frac{1}{\epsilon}} n$.

July'02: Yes, There Is!

- Consider products of the form $n^i p^j$ for $0 \leq i, j \leq \sqrt{r}$.
- Two of these are equal modulo r, and the maximum value is at most $n^{2\sqrt{r}}$.
- Therefore, if $O > n^{2\sqrt{r}}$, we are done.
- The bound on O is: $O \geq 2^d \geq 2^{\sqrt{r}}$ since $d \geq \sqrt{r}$.
- However, if one can prove $d \geq r^{\frac{1}{2}+\epsilon}$ for any $\epsilon > 0$ then:

$$O \geq 2^{r^{\frac{1}{2}+\epsilon}} > n^{2\sqrt{r}}$$

provided one chooses $r > \log^{\frac{1}{\epsilon}} n$.

July'02: Yes, There Is!

- Consider products of the form $n^i p^j$ for $0 \leq i, j \leq \sqrt{r}$.
- Two of these are equal modulo r, and the maximum value is at most $n^{2\sqrt{r}}$.
- Therefore, if $O > n^{2\sqrt{r}}$, we are done.
- The bound on O is: $O \geq 2^d \geq 2^{\sqrt{r}}$ since $d \geq \sqrt{r}$.
- However, if one can prove $d \geq r^{\frac{1}{2}+\epsilon}$ for any $\epsilon > 0$ then:

$$O \geq 2^{r^{\frac{1}{2}+\epsilon}} > n^{2\sqrt{r}}$$

provided one chooses $r > \log^{\frac{1}{\epsilon}} n$.

July'02: Yes, There Is!

- Consider products of the form $n^i p^j$ for $0 \leq i, j \leq \sqrt{r}$.
- Two of these are equal modulo r, and the maximum value is at most $n^{2\sqrt{r}}$.
- Therefore, if $O > n^{2\sqrt{r}}$, we are done.
- The bound on O is: $O \geq 2^d \geq 2^{\sqrt{r}}$ since $d \geq \sqrt{r}$.
- However, if one can prove $d \geq r^{\frac{1}{2}+\epsilon}$ for any $\epsilon > 0$ then:

$$O \geq 2^{r^{\frac{1}{2}+\epsilon}} > n^{2\sqrt{r}}$$

provided one chooses $r > \log^{\frac{1}{\epsilon}} n$.

July'02: Fouvry's Theorem

- E. Fouvry (1985) showed that primes r such that $r - 1$ has a prime factor $q_r > r^{\frac{2}{3}}$ have constant density.
- This implies that d can be made $> r^{\frac{2}{3}}$.
- So $\epsilon = \frac{1}{6}$ and we need to choose $r > \log^6 n$.

July'02: Fouvry's Theorem

- E. Fouvry (1985) showed that primes r such that $r-1$ has a prime factor $q_r > r^{\frac{2}{3}}$ have constant density.
- This implies that d can be made $> r^{\frac{2}{3}}$.
- So $\epsilon = \frac{1}{6}$ and we need to choose $r > \log^6 n$.

July'02: Fouvry's Theorem

- E. Fouvry (1985) showed that primes r such that $r - 1$ has a prime factor $q_r > r^{\frac{2}{3}}$ have constant density.
- This implies that d can be made $> r^{\frac{2}{3}}$.
- So $\epsilon = \frac{1}{6}$ and we need to choose $r > \log^6 n$.

Observations

- The proof above does not prove the conjecture proposed earlier since $r = \omega(\log n)$ and the equation is tested for several $x + a$'s instead of only $x + 1$.
- It can be viewed as a derandomization of the identity test given earlier for the special case of primality identity.

Observations

- The proof above does not prove the conjecture proposed earlier since $r = \omega(\log n)$ and the equation is tested for several $x + a$'s instead of only $x + 1$.
- It can be viewed as a derandomization of the identity test given earlier for the special case of primality identity.

Observations

Identity Test With Less Randomness: Test if $P(x) = 0$ modulo $(R(x))^r - 1$ for a small r that gives rise to a large extension field and $R(x)$ nearly random.

Primality Test With No Randomness: Test if $(x+1)^n - x^n - 1 = 0$ modulo n and $(R(x))^r - 1$ for a small r that gives rise to a large extension field and $R(x) = x - a$ for $1 \leq a \leq r$.

Observations

Identity Test With Less Randomness: Test if $P(x) = 0$ modulo $(R(x))^r - 1$ for a small r that gives rise to a large extension field and $R(x)$ nearly random.

Primality Test With No Randomness: Test if $(x+1)^n - x^n - 1 = 0$ modulo n and $(R(x))^r - 1$ for a small r that gives rise to a large extension field and $R(x) = x - a$ for $1 \leq a \leq r$.

Epilogue

- On August 4, 2002 we distributed the paper.
- Due to a clock error in my brain, it was dated August 6!