

# Deterministisk primtalstestning

*Det är lätt att avgöra om ett givet heltal är primtal*

Hans Block

Teorigruppen

# Primalstester på poly-tid

- Agrawal, Kayal och Saxena 2002: Avgör om  $n$  är primtal på  $\tilde{O}(\log^{12} n)$ , djup talteori
- Många har bidragit
- I dag:
  - $\tilde{O}(\log^{10,5} n)$ , elementärt
  - $\tilde{O}(\log^{6+o(1)} n)$ , djup talteori
  - $\tilde{O}(\log^{4+o(1)} n)$ , probabilistiskt

# Deterministisk primtalstestning

- Källor och uppläggnig
- Varför intressant?
- Andra primtalstester
- Karakterisering av primtal, flera satser
- Algoritmer
- Komplexitet
- Resultat från analytisk talteori

# Källor och uppläggning

- Originalartikel, första och andra preprint
- Översiktsartikel av Andrew Granville
  - Trevlig att läsa, men luckor, andra beteckningar och olikhet åt fel håll!
- Daniel J. Bernstein, Riesel, implementation
- Inga bevis för resultat i analytisk talteori
- Bästa resultat bevisas ej
- Huvudpunkter
  - Karakterisering av primtal
  - Algoritmer
  - Komplexitet
  - Analytisk talteori: Frekvenser av vissa primtal

# Varför intressant?

- Industriellt behov av primtal
- Komplexitetsfrågor
  - Skapa algoritmer på poly-tid (t.ex. linjärprogrammering)
- Nya grepp på gammalt område
- Gauss: Vetenskapens värdighet
- Personligt intresse

# Industriellt behov

- Samhällets säkerhet bygger på RSA
- RSA behöver primtal
- Om inte primtal – dechiffkering misslyckas
  - Meddelande  $M$ ,  $n = pqr$ , exponent för kryptering  $e$ , för dekryptering  $d$
  - Vi vill  $ed \equiv 1 \pmod{\text{lcd}(p-1, q-1, r-1)}$
  - Inte säkert sant om  $ed \equiv 1 \pmod{\text{lcd}(p-1, qr-1)}$
- Behov: *Många* slumpmässiga primtal – inte *alla*

# Praktiskt?

- Behov av primtal om c:a 1000 bitar
- Gränser operationer
  - Min PC  $2 \cdot 10^{14}$  per dygn
  - Totalt i historien  $10^{24}$
- $\log^{12} n = 10^{12}$  ,  $\log n = 10$  ,  $n = 2^{10} = 1000$
- $\log^6 n = 10^{12}$  ,  $n = 2^{100} = 10^{30}$  , implementerat
- $\log^4 n$ : 700 siffror på en dag (extrapolerat)
- Här alltid snabb multiplikation  $\tilde{O}(\log n)$
- Torbjörn Granlund: Skolboksmultiplikation lönsamt upp till 1000 bitar
- AKS räknar med snabb multiplikation  $\tilde{O}(\log n)$
- Troligen mycket sämre, även om metoden förbättrats med en faktor 1000 000
- NEJ!

# Komplexitetsfrågor

- Platsar självklart bland komplexitetsfrågor
- Roligt när poly-algoritmer upptäcks
  - Linjärprogrammering (ellipsoider, projektiva avbildningar)
- Vad har vi annars gjort på kursen:  
approximera NP-svåra problem

# Många håller på

- Festligt lösa riktigt gamla problem
- <http://cr.yp.to/primetests.html>

ABSTRACT. “The problem of distinguishing prime numbers from composite numbers, and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. It has engaged the industry and wisdom of ancient and modern geometers to such an extent that it would be superfluous to discuss the problem at length. Nevertheless we must confess that all methods that have been proposed thus far are either restricted to very special cases or are so laborious and difficult that even for numbers that do not exceed the limits of tables constructed by estimable men, they try the patience of even the practiced calculator. And these methods do not apply at all to larger numbers ... It frequently happens that the trained calculator will be sufficiently rewarded by reducing large numbers to their factors so that it will compensate for the time spent. Further, *the dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated ...* It is in the nature of the problem that *any* method will become more complicated as the numbers get larger. Nevertheless, in the following methods the difficulties increase rather slowly ... The techniques that were previously known would require intolerable labor even for the most indefatigable calculator.”

—from article 329 of *Disquisitiones Arithmeticae* (1801) by C. F. Gauss

**SR. HOCHWOHLGEBOREN**

DEM

**HERRN GEHEIMEN HOFRATH**

**CARL FRIEDRICH GAUSS**

DR. PHIL.

COMMANDEUR DES DANEBROG-ORDENS, RITTER DES GUELPHEN-ORDENS, DES  
FRANZÖSISCHEN ORDENS DER EHRENLEGION, DES PREUSSISCHEN CIVILVERDIENST-  
ORDENS UND DES NORDSTERN-ORDENS,

PROFESSOR UND DIRECTOR DER STERNWARTE ZU GÖTTINGEN, MITGLIED DER SOCIETÄTEN DER  
WISSENSCHAFTEN ZU GÖTTINGEN UND LONDON, DER SOCIETA ITALIANA, DER ACADEMIE DER  
WISSENSCHAFTEN IN BERLIN, DER SOC. DER NATURWISSENSCHAFTEN IN MARBURG, DER ACAD.  
DER WISSENSCH. IN NEAPEL, DER ACAD. DER WISSENSCH. IN PARIS UND MÜNCHEN, DER  
ASTRONOMISCHEN GESELLSCHAFT IN LONDON, DER SOC. DER WISS. IN COPENHAGEN, DER ACAD.  
DER WISS. IN STOCKHOLM, DER AMERIKANISCHEN ACAD. DER WISS. U. KÜNSTE, DER ACAD. IN  
PALERMO, DER SOC. DER KÜNSTE IN EDINBURG, DER ACAD. DER WISS. IN BOLOGNA U. TURIN,  
DER BÖHMISCHEN GESELLSCH. IN PRAG, DER ACAD. DER WISS. IN BRÜSSEL, DER CAMBRIDGE  
PHILOSOPHICAL SOCIETY, DER SOCIET. DER WISS. IN UPSALA, DES KÖNIGL. INSTITUTS DER  
NIEDERLANDE, DES ATHENÄUMS IN FLORENZ, UND EHRENMITGLIED DER MATHEMATISCHEN  
GESELLSCHAFT IN HAMBURG, DER CURLÄNDISCHEN GESELLSCHAFT FÜR LITERATUR UND KUNST,  
DER ACAD. DER WISS. IN PETERSBURG, DES PHYSIKALISCHEN VEREINS IN FRANKFURT,

AUS

**INNIGSTER VEREHRUNG**

GEWIDMET

VON

**HEINRICH GOTTLIEB KÖHLER,**

DR. PHIL.

# Tidigare primtalstestning

- Miller - Rabin och slumpen
- Miller och Riemanns generaliserade förmodan:
  - Du klarar Dig nog
  - Går det fel, vinner Du evig ära!
- Cyklotomisk primtalsbevisning Cohen-Lenstra ...  
2000 siffror på  $10^{14}$  klockcykler
- Elliptiska kurvor 2000 siffror på  $10^{15}$  klockcykler

# Agrawal, Kayal och Saxena:

## Sats

Givet ett heltal  $n \geq 2$ . Låt  $r$  vara ett positivt heltal  $< n$ , vars ordning  $n$  modulo  $r$  är  $> \log^2 n$ . Då är  $n$  primtal då och endast då

- $n$  inte är en jämn potens (av primtal)
- $n$  inte har någon primfaktor  $\leq r$
- $(x + a)^n \equiv x^n + a \pmod{(n, x^r - 1)}$  för varje heltal  $a$ ,  $1 \leq a \leq \sqrt{r} \log n$

# Förbättring

- Det sista villkoret kan ersättas med

$$1 \leq a \leq \frac{\sqrt{\phi(r) \cdot \log n}}{\log \phi(r)} + 2$$

–  $\phi$  betyder Eulers funktion

# Liten motivering

- **Påstående.** Antag  $(a, n) = 1$ . Då är  $n$  primtal då och endast då
  - $(x - a)^n \equiv x^n - a \pmod{n}$
- **Bevis.**  $n$  primtal  $\Rightarrow$  kongruensen trivialt.
  - Antag  $q$  primtal,  $q \mid n$ ,  $q^k \parallel n$ .
  - $q^k$  delar inte  $\binom{p}{q}$
  - $(q^k, a^{p-q}) = 1$
  - Koefficienten för  $x^q \neq 0 \pmod{n}$  ♦
- AKS har polynom av mycket lägre gradtal

# Historia

- Augusti 2002-08 Agrawal, Kayal och Saxena
- Lenstra 2002-08
- Macaj, Agrawal 2002-12
- Bernstein, Berrizbeitia, Cheng 2003-01
- Lenstra, Pomerance 2003-03

# Komplexitet

- Avgör om  $n$  är en jämn potens
- Hitta  $r$ ;  $o_r(n) > \log^2 n$
- Avgör om  $\gcd(a, n) > 1$  för något  $a \leq r$
- Gäller barnens binominalteorem?
- $(x + a)^n \equiv x^n + a \pmod{(n, x^r - 1)}$   
– för  $a = 1, 2, \dots, (\sqrt{r} \cdot \log n)$  ?

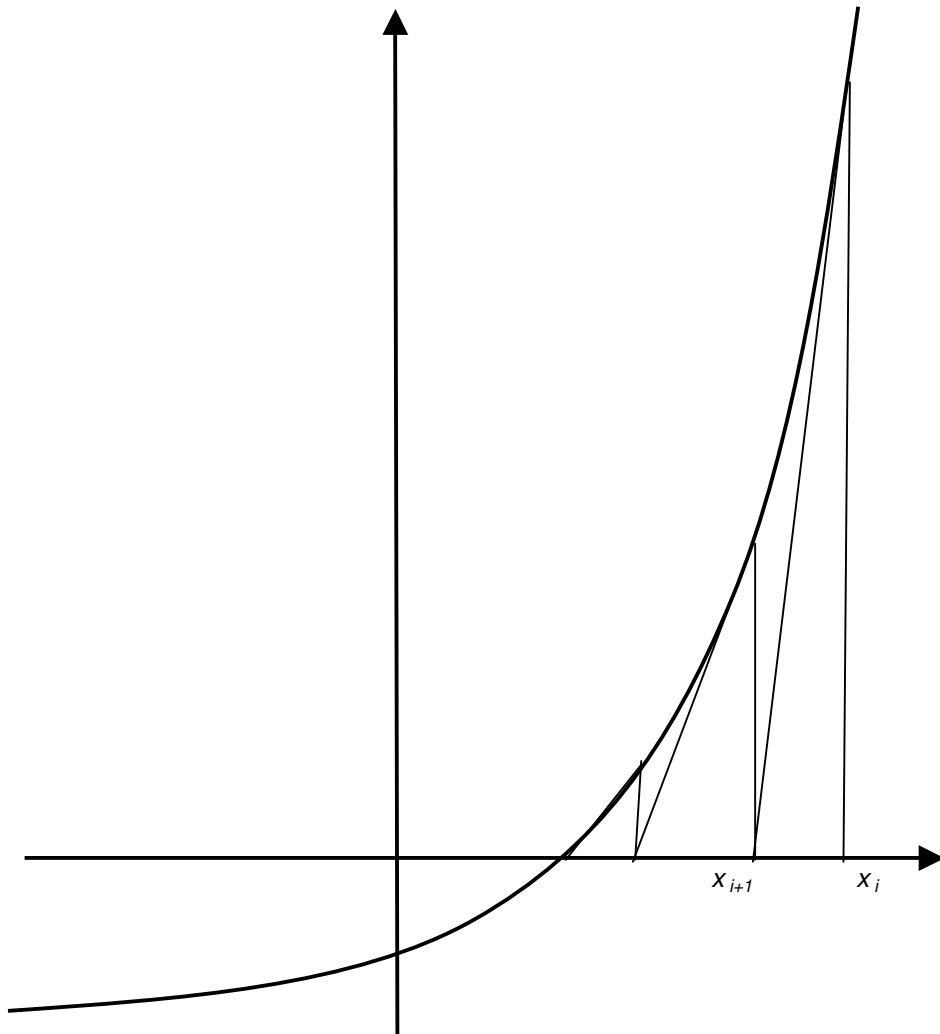
# $n$ jämn potens?

- Hur många potenser?
  - Högst  $\lg n$  stycken
  - Bara primtalsexponenter skall testas
  - Inga faktorer i  $n < \log^2 n$

$$(\log^2 n)^k = n; \quad k = \frac{\log n}{2 \log \log n}$$

- Antal potenser  $k = \frac{\log n}{2(\log \log n)^2}$

Lös ekvationen  $f(x) = x^k - n = 0$



$$x_{i+1} = x_i - \frac{f(x_i)}{f'(x_i)}$$

# Newton – Raphsons iteration

$$x_{i+1} = x_i - \frac{f(x_i)}{f'(x_i)}$$

$$x_{i+1} - x = x_i - x - \frac{0 + (x_i - x) \cdot f'(x) + \frac{(x_i - x)^2}{2} \cdot f''(x) + \dots}{f'(x) + (x_i - x) \cdot f''(x) + \dots}$$

$$x_{i+1} - x = (x_i - x)^2 \cdot \frac{f''(x)}{2f'(x)} + \dots$$

- Kvadratisk konvergens!

# Newton – Raphson, heltal

- Välj startvärde med flytande räkning
- $f$  konvex medför  $\{x_i\}$  avtagande  $> x$
- Avrunda  $x_{i+1}$  nedåt till heltal
  - Avrundade sviten än mer avtagande
  - Är ett värde  $< x$ , så beror det på avrundningen
  - $x - 1 < y :=$  sista avrundade värdet av  $x_j \leq x$
  - Nästa värde är större än det föregående
- Stoppa när sviten inte minskar
- Testa om  $y^k = n$

# Slutsats och förenkling

- $x$  heltal  $\Leftrightarrow$  sista avrundade gissningen uppfyller  $y^k = n$
- Om  $y$  har små primfaktorer behöver vi inte räkna ut potensen, för vi letar efter primtalspotenser

# Hur lång tid?

- Multiplikation och division  $\tilde{O}(\log n)$
- Kvadratisk konvergens
  - $O(\log \log n)$  steg
  - Räkna bara med de siffror som behövs
  - $\tilde{O}(\log k \cdot \log n)$  tid / potens
  - $\tilde{O}(\log^2 n)$  tid totalt
- MEN: Stor konstant, dåligt startvärde!

# Riktiga uppskattningar

$$\begin{aligned}x_{i+1} - x &= x_i - x - \frac{f(x_i)}{f'(x_i)} = \\&= x_i - x - \frac{x_i^k - x^k}{k \cdot x_i^{k-1}} = \\&= (x_i - x) \cdot \left( 1 - \frac{x_i^{k-1} + x_i^{k-1} \cdot x + \dots + x^{k-1}}{k \cdot x_i^{k-1}} \right) < \\&< (x_i - x) \cdot \left( 1 - \frac{k \cdot x^{k-1}}{k \cdot x_i^{k-1}} \right) = (x_i - x) \cdot \left( 1 - \left( \frac{x}{x_i} \right)^{k-1} \right)\end{aligned}$$

# Måttligt stora $n$

- Geometrisk konvergens

Sista faktorn är  $< 1/2$  om  $\left(\frac{x}{x_i}\right)^k > 1/2$        $k < \frac{\ln 2}{\ln(x_i / x)}$

- Flytande räkning:  $\ln(x_0 / x) > 2^{-62}$

$$\log n < \frac{\ln 2}{2^{-62}} < 2^{62} \quad n < 2^{2^{62}}$$

- I så fall tid högst  $\tilde{O}(\log^3 n)$

# Ännu strängare

$$x_{i+1} - x < (x_i - x) \cdot \left(1 - \frac{x_i^{k-1}}{k \cdot x_i^{k-1}}\right) = (x_i - x) \cdot \left(1 - \frac{1}{k}\right)$$

- $k = O(\log n)$  ger att  $\left(1 - \frac{1}{k}\right)^{\log^2 n} = O(1/n)$

$$x_i - x < O(1)$$

- Hela beräkningen går på  $\tilde{O}(\log^4 n)$
- Svårigheten ligger inte här!

# Hitta $r$ ; $o_r(n) > \log^2 n$

- Prova för heltal  $q > \log^2 n$ :
  - Beräkna  $n^j \pmod{q}$  för  $j = 1, \dots, \lceil \log^2 n \rceil$
- Sluta då alla dessa rester är  $\neq 1$
- Sätt  $r = q$
- Starttid per  $q$ :  $\tilde{O}(\log n)$
- Tid per potens:  $\tilde{O}(\log r)$
- Total tid:  $\tilde{O}(r \cdot \log^2 n)$

$\gcd(a, n) > 1$  för något  $a \leq r$ ?

- Dividera med primtal  $< r$ 
  - $\tilde{O}(r \cdot \log n)$
- Gcd-beräkning:
  - En division  $\log n$
  - Sedan  $\log r$  bitar
  - I varje steg blir talen någon bit kortare
  - Med snabb division  $\tilde{O}(\log^2 r)$
  - Hela beräkningen  $\tilde{O}(r \cdot \log n)$

# Barnens binominalteorem?

- $(x + a)^n \equiv x^n + a \pmod{(n, x^r - 1)}$  för varje heltal  $a$ ,  $1 \leq a \leq \sqrt[r]{r \cdot \log n}$
- Upphöj polynom till  $n$  genom
  - Successiva kvadreringar
  - Multiplicera polynom av grad  $r$  med varandra
  - Reducera
- Titta på koefficienter

# Största arbete, naivt

- Antal kongruenser  $\sqrt{r} \cdot \log n$
- Antal multiplikationer per kongr.  $\log n$
- Operationer per polynom  $r^2$
- Bitoperationer per multiplikation  $\log^2 n$
- Totalt  $r^{2,5} \cdot \log^4 n$

# Multiplikation av polynom

- Enpunktsevaluering: Polynomet
- $a(x) = \sum_{i=0}^{r-1} a_i x^i \in Z[x]: -A < a_i \leq A$  för alla  $i$
- är entydigt bestämt av värdet i  $2A$
- Algoritm: Räkna ut  $a_0, a_1, \dots$
- Evaluera  $a$  och  $b$  i  $2A$
- Multiplicera  $a(2A) \cdot b(2A)$
- Återskapa  $ab$

# Multiplikation i $(\mathbb{Z}/n)/(x^r - 1)$

- $k = \lceil \lg rn^2 \rceil$
- Lyft till  $\mathbb{Z}[x]/(x^r - 1)$
- Produktens koefficienter  $< 2^k$
- Avbilda till  $\mathbb{Z}/(2^{kr} - 1)$       tid  $O(kr)$
- Multiplicera i  $\mathbb{Z}/(2^{kr} - 1)$       tid  $\tilde{O}(kr) = \tilde{O}(r \cdot \log n)$
- Hitta produkten i  $\mathbb{Z}[x]/(x^r - 1)$  tid  $O(kr)$
- Reducera koeff. mod  $n$       tid  $\tilde{O}(r \cdot \log n)$

# Största arbetet, listigt

- Antal kongruenser  $\sqrt{r} \cdot \log n$
- Antal multiplikationer per kon.  $\log n$
- Multiplikation av polynom  $r \cdot \log n$
- Totalt  $r^{1,5} \cdot \log^3 n$
- **Totalt algoritmen  $r^{1,5} \cdot \log^3 n$**

# Storleken av $r$

- $r > \log^2 n$ 
  - Tiden minst  $O(\log^6 n)$
- Ofta finner vi  $r < 2 \log^2 n$ , men kan inte bevisa det
- Elementärt (Chebyshev)  $r = O(\log^5 n)$ 
  - Ger tid  $\tilde{O}(\log^{10,5} n)$
- Fouvry:  $r = O(\log^3 n)$ 
  - Ger tid  $\tilde{O}(\log^{7,5} n)$

# Bevis för AKS:s sats

- Ena hållet trivialt
- Givet  $n$ . Antag
  - $r$  heltal  $< n$
  - $d := o_r(n) > \log^2 n$
  - $n$  ej primtal
  - $n$  saknar delare  $< r$
  - $n$  ej jämn potens av primtal
  - $(x + a)^n \equiv x^n + a \pmod{(n, x^r - 1)} \forall a; 1 \leq a \leq \sqrt{r} \cdot \log n$
- Hitta motsägelse

# Cyklotomiska polynom

- Först i  $\mathbb{C}$ 
  - Enhetsrötter: Rötter till  $x^r = 1$ 
    - $e_k = e^{2\pi i k/r}$ ,  $k = 1, 2, \dots, r - 1$
  - Primitiv enhetsrot ordning  $r$ :
    - $e_k^r = 1$ ,  $e_k^{r/d} \neq 1 \ \forall d \mid r, d < r$
    - d.v.s.  $e^{2\pi i k/r}$ ,  $(k, r) = 1$
  - Cyklotomiskt polynom ordning  $d$ :
    - Har de primitiva  $d$ :te enhetsrötterna
    - $\text{grad}(\Phi_d(x)) = \phi(d)$  (Eulers funktion)

$$x^r - 1 = \prod_{d \mid r} \Phi_d(x)$$

# Exempel

$$\begin{aligned}x^{15} - 1 &= (x^3 - 1) \cdot (x^{12} + x^9 + x^6 + x^3 + 1) \\ &= (x^5 - 1) \cdot (x^{10} + x^5 + 1) \\ x^5 - 1 &= (x - 1) \cdot (x^4 + x^3 + x^2 + x + 1) \\ x^3 - 1 &= (x - 1) \cdot (x^2 + x + 1) \\ x^{15} - 1 &= (x - 1) \cdot (x^2 + x + 1) \cdot (x^4 + x^3 + x^2 + x + 1) \cdot \\ &\quad \cdot (x^8 - x^7 + x^5 - x^4 + x^3 - x + 1) \\ &= \Phi_1(x) \cdot \Phi_3(x) \cdot \Phi_5(x) \cdot \Phi_{15}(x)\end{aligned}$$

# Alla $\Phi_d$ har heltalskoefficienter

- Bevis. Sant för  $d = 1$ . Antag sant för  $d' \mid d$ .
- $\Phi_{d'}(x) \mid x^{d'} - 1 \mid x^d - 1$
- Polynomen relativt prima, moniska

$$\prod_{d' \mid d} \Phi_{d'}(x) \mid x^d - 1$$
$$\mid \frac{x^d - 1}{\prod_{d' \mid d} \Phi_{d'}(x)} = \Phi_d(x)$$

- Alltså heltalskoefficienter

# Mera cyklotomiskt

- Alla  $\Phi_d(x)$  är irreducibla över  $\mathcal{Q}[x]$  (*behövs ej*)
- Man kan definiera  $\Phi_d(x)$  över  $F_p$
- $\Phi_{d'}(x)$  och  $\Phi_{d''}(x)$  är relativt prima över  $F_p$ 
  - $x^{\text{lcd}(d', d'')} - 1$ ,  $d' \neq d''$ , har ingen faktor gemensam med sin derivata, alltså inga multipla faktorer
- $\Phi_d(x)$  behöver inte vara irreducibla över  $F_p$
- Om  $r$  är primtal, så har alla irreducibla faktorer av  $\Phi_r(x)$  graden  $o_r(p)$  (*behövs i AKS 1, 2*)

# Skapa en grupp

- $r$  enligt förutsättningarna,  $d := o_r(n)$ ,  $p \mid n$
- $A := \lceil \sqrt{r} \cdot \log n \rceil$
- $h(x)$  irreducibel faktor till  $\Phi_r(x)$ ,  $m := \text{grad}(h)$
- $(x + a)^n \equiv x^n + a \pmod{(n, x^r - 1)} \Rightarrow$
- $(x + a)^n \equiv x^n + a \pmod{(p, h(x))}$
- $\mathcal{F} := \mathbb{Z}[x] / (p, h(x))$  är en kropp
- $x$  har ordning  $r$  i  $\mathcal{F}$ 
  - $x^r \equiv 1 \pmod{h(x)}$  enligt def.
  - $x^d \equiv 1, d \mid r \Rightarrow h(x) \mid x^d - 1 = \prod_{d' \mid d} \Phi_{d'}(x)$
  - $\Phi_{d'}(x)$  relativt prima  $\Rightarrow h(x) \mid \Phi_{d'}(x)$  för något  $d' \mid r \Rightarrow r \mid d$
- $r \mid p^m - 1$  (antalet element i gruppen  $\mathcal{F}^*$ )

# Skapa en grupp

- $H$ : elementen mod  $(p, x^r - 1)$  genererade av  $x, x + 1, x + 2, \dots, x + A$
- $G$ : cykliska undergruppen till  $\mathcal{F}^*$  genererad av  $x, x + 1, x + 2, \dots, x + A$
- Alla element i  $G \neq 0$ 
  - $x + a = 0 \Rightarrow (x + a)^n = 0 \Rightarrow x^n + a = 0 \Rightarrow$
  - $x^n = -a = x \Rightarrow$
  - $h(x) \mid x^n - x, r = o(x) \Rightarrow r \mid n - 1 \Rightarrow n \equiv 1 \pmod{r} \Rightarrow$
  - $d = 1$  Motsägelse.

# Skapa en grupp

- $g(x) \in H \Rightarrow g(x)^n \equiv g(x^n) \pmod{(p, x^r - 1)}$ 
  - ty sant för varje faktor i  $g(x)$  enligt antagandet

$$S = \left\{ k; g(x^k) \equiv g(x)^k \pmod{(p, x^r - 1)} \forall g \in H \right\}$$

- $p, n \in S$ 
  - $p$  enligt Fermats lilla sats,  $n$  enl. förutsättning
- Hitta motsägelse för storleken av  $G$ !

# Övre begränsning för $|G|$

- **Lemma 1.** Om  $a, b \in S$ , så  $ab \in S$ 
  - *Definition och insättning:*
  - $g(x)^{ab} \equiv (g(x)^a)^b \equiv g(x^a)^b \equiv g((x^a)^b) \equiv g(x^{ab}) \pmod{(p, x^r - 1)}$  ♦

# Övre begränsning för $|G|$

- **Lemma 2.** Om  $a, b \in S$  och  $a \equiv b \pmod{r}$ , så  $a \equiv b \pmod{|G|}$ .
  - $u - v \mid g(u) - g(v) \quad \forall g(x) \in \mathcal{Z}[x]$
  - $x^r - 1 \mid x^{a-b} - 1 \mid x^a - x^b \mid g(x^a) - g(x^b)$
  - $g(x) \in H \Rightarrow g(x)^a \equiv g(x^a) \equiv g(x^b) \equiv g(x)^b \pmod{(p, x^r - 1)}$
  - $g(x) \in G \Rightarrow g(x)^{a-b} \equiv 1 \text{ i } \mathcal{F}$
  - $G$  cyklisk, välj  $g$  till generator  $\Rightarrow |G| \mid (a - b)$  ♦

# En övre begränsning av $|G|$

- $n$  ej jämn potens, ej primtal
- $\Rightarrow n^i p^j; i, j \geq 0$  alla olika
- $(n, r) = 1 \Rightarrow (p, r) = 1 \Rightarrow$
- $R = \{n^i p^j \text{ mod } r\}$  blir grupp
- Fler än  $|R|$  sådana med  $0 \leq i, j \leq \sqrt{|R|} \Rightarrow$
- Två måste vara kongruenta mod  $r$
- Skillnaden delbar med  $|G| \Rightarrow$
- $|G| \leq |n^i p^j - n^l p^j| \leq (np)^{\sqrt{|R|}} - 1 < n^{2\sqrt{|R|}} - 1$

# Förbättring

- Visa att  $n / p \in S$  och få  $|G| \leq n^{\sqrt{|R|}} - 1$   
– Bevis som förut!
- $d := o_r(n)$
- Visa:  $a \in S$  och  $b \equiv a \pmod{n^d - 1} \Rightarrow b \in S$
- $n^d \equiv 1 \pmod{r} \Rightarrow x^{n^d} \equiv x \pmod{x^r - 1}$   
 $x^r - 1 \mid x^{n^d} - x \mid x^b - x^a \mid g(x^b) - g(x^a) \forall g \in Z[x]$
- Om  $g(x) \in H$  så enligt lemma 1:  
$$g(x)^{n^d} \equiv g(x^{n^d}) \pmod{(p, x^r - 1)}$$

# Förbättring, forts.

$$g(x)^{n^d} \equiv g(x) \pmod{(p, x^r - 1)}, g(x)^{n^d - 1} \equiv 1 \pmod{(p, x^r - 1)}$$

$$g(x)^a \equiv g(x)^b \pmod{(p, x^r - 1)}$$

– då  $n^d - 1 \mid b - a$

- Alltså  $g(x^b) \equiv g(x^a) \equiv g(x)^a \equiv g(x)^b \pmod{(p, x^r - 1)}$
- $a \in S \Rightarrow b \in S$
- Sätt  $b = n / p$  och  $a = np^{\phi(n^d - 1) - 1}$ 
  - $\phi(m) :=$  antal heltal  $< m$  relativt prima med  $m$
- $a \in S$  enligt lemma 1.  $b \equiv a \pmod{n^d - 1}$ 
  - Eulers teorem:  $(c, m) = 1 \Rightarrow c^{\phi(m)} \equiv 1 \pmod{m}$
- så  $b = n / p \in S$ . ♦

# Undre begränsning för $|G|$

- Polynomen  $\prod_{1 \leq a \leq A} (x + a)^{e_a}$  av grad  $< m$  är alla olika i  $G$ . Kan ge bra undre gräns.
- Lenstra gav ett bättre gradtal :  $|R|$

# Lemma 3

- **Antag**  $f(x), g(x) \in \mathcal{Z}[x]$ ,  $f(x) \equiv g(x) \pmod{(p, h(x))}$ ,  
resterna av  $f$  och  $g \in G$ ,  $\text{grad}(f), \text{grad}(g) < |R|$
- **Då gäller**  $f(x) \equiv g(x) \pmod{(p)}$
- **Bevis.**
- Betrakta  $\Delta(y) := f(y) - g(y) \in \mathcal{Z}[y]$  reducerat i  $\mathcal{F}$ .
- Om  $k \in S$  så
- $\Delta(x^k) = f(x^k) - g(x^k) \equiv f(x)^k - g(x)^k \equiv 0 \pmod{(p, h(x))}$
- $\{x^k: k \in R\}$  rötter till  $\Delta(y) \equiv 0 \pmod{(p, h(x))}$
- $x$  har ordning  $r$  i  $\mathcal{F} \Rightarrow$  rötterna olika
- $\Delta$  har  $\geq |R|$  rötter,  $\text{grad}(\Delta) < |R|$ :
- Alla koefficienter i  $\Delta \equiv 0 \pmod{(p, h(x))}$
- Men inga  $x$  i koeff.  $\Rightarrow \Delta(y) \equiv 0 \pmod{p}$  ♦

# Slutkläm bevis AKS

$$B := \lfloor \sqrt{R} \cdot \log n \rfloor$$

- $|R| \geq d = o_r(n) > \log^2 n$  enl. ant.  $\Rightarrow |R| > B$
- $A > B$
- Lemma 3  $\Rightarrow$  Produkterna ger olika element i  $G$  för varje äkta delmängd av  $\{0, 1, 2, \dots, B\}$
- Alltså nu:  $|G| \geq 2^{B+1} - 1 > n^{\sqrt{|R|}} - 1$
- Förut  $|G| \leq n^{\sqrt{|R|}} - 1$
- Motsägelse! ♦

# Annan undre gräns för $|G|$

- **Lemma 3'.**  $|G| \geq \binom{|R|+A}{A+1}$
- **Bevis.** Kombinatoriskt.
- Betrakta alla element i  $H$  med grad  $< |R| < r$ .
- Eftersom  $A < r$  är de olika mod  $p$ .
  - $(a, n) = 1$  för  $a < r$
  - $a < A = \sqrt{r} \cdot \log n < r$  om  $r > \log^2 n$
  - Unik faktorisering i  $\mathbb{Z}[x] / p$ , för vi har Euklides' algoritm
- Enligt lemma 3 är de olika i  $G$ .

# Hur många sådana produkter?

- Placera  $|R| - 1$  faktorer i facken  $1, x, x - 1, \dots, x - A$ .
- \* \* \* | \* \* | | | \* | | | \* \* \* | \*
- \* faktor,  $|R| - 1$  stycken
- | vägg mellan fack,  $A + 1$  stycken.
- Antal sätt att välja ut  $A + 1$  ställen av  $|R| + A$  möjliga:  $\binom{|R| + A}{A + 1}$

# Slutkläm bevis AKS

- Vi har nu:

$$\begin{aligned}
 |G| &\geq \binom{|R|+A}{A+1} > |R|^{A-1} > R^{\sqrt{r} \cdot \log n - 1} = \\
 &= e^{(\log R) \cdot (\sqrt{r} \cdot \log n - 1)} = n^{(\sqrt{r} - 1 / \log n) \cdot \log R} > \\
 &> n^{\sqrt{r} \cdot (\log R) - 1} > n^{\sqrt{r}} > n^{\sqrt{|R|}}
 \end{aligned}$$

- Vi hade förut:  $|G| \leq n^{\sqrt{|R|}} - 1$
- Motsägelse. Alltså  $n$  primtal. ♦

# Anmärkning

- Om  $A < \sqrt{r} \log n$  så får vi unika element i  $G$ .
- Om å andra sidan

$$|R|^{A-1} > n^{\sqrt{|R|}}$$

$$A > \frac{\sqrt{r} \cdot \log n}{\log r} + 1 > \frac{\sqrt{\phi(r)} \cdot \log n}{\log \phi(r)} + 1 > \frac{\sqrt{|R|} \cdot \log n}{\log |R|} + 1$$

så får vi motsägelse.

- Arbetet minskar med minst en faktor  $\log r$  eller minst  $2 \log \log n$ .
- Förmodligen gäller detta även  $\log^6 n$ -metoden

# Hur stora $r$ ?

- **Lemma 4.** Om  $r \geq 6$ , så finns ett primtal  $r \in [\log^5 n, 2 \cdot \log^5 n]$  för vilket  $o_r(n) > \log^2 n$
- **Bevis.** Antag att  $o_r(n) \leq I := \log^2 n$  för alla primtal  $r$  i intervallet  $[N, 2N]$ ,  $N := \log^5 n$ .

- $$r \mid \prod_{i \leq I} (n^i - 1) \Rightarrow \prod_{\substack{N \leq r \leq 2N \\ r \text{ primtal}}} r \mid \prod_{i \leq I} (n^i - 1)$$

$$2^N \leq \prod_{\substack{N \leq r \leq 2N \\ r \text{ primtal}}} r \leq \prod_{i \leq I} (n^i - 1) < n^{\sum_{i \leq I} i} < n^{I^2} = 2^{\log^5 n}$$

- **Motsägelse.** ♦

# Primaltalssatsen $\pi(x) \approx \frac{x}{\ln x}$

- Legendre, Gauss  $\approx$  1800: Förmodan
- Chebyshev 1850: Konstanter
- Hadamard, de la Vallée-Poussin 1896: Bevis
- Vi kan nöja oss med något enklare

$$\sum_{N \leq r \leq 2N} \ln r = \int_N^{2N} \ln x d\pi(x) = [\ln x \cdot \pi(x)]_N^{2N} - \int_N^{2N} \frac{1}{x} \pi(x) dx \approx N - \frac{N}{\ln N}$$

$$\prod_{N \leq r \leq 2N} r \approx e^N > 2^N$$

# Elementärt

- Räkna primtal i  $\binom{N}{2N}$  ger

$$\frac{1}{8} \leq \frac{\pi(n)}{n / \ln n} \leq 12, n \geq 2$$

$$\prod_{\substack{N \leq r \leq cN \\ r \text{ primtal}}} r > N^{c' \cdot \frac{N}{\ln N}} = 2^{c'' N}$$

- Resultatet räcker för att hitta  $r = O(\log^5 n)$
- Ursprungliga påståendet bevisat med råge ♦

# Sophie Germain-primtal

- SG:  $r$  och  $(r - 1)/2$  båda primtal
- Förmodan: Asymptotiskt  $\frac{Dx}{\log^2 x} \text{ SG} \leq x$ 
  - $D$  konstanten för primtalstvillingar
- Ful motivering:
  - $\Pr(r \text{ primtal}) = 1/\log r$
  - $\Pr((r - 1)/2 \text{ primtal}) = 1/\log r$
  - ”Oberoende händelser”
  - $\Pr(SG) = \frac{D}{\log^2 x}$

# Förväntat antal faktorer

- Förväntat antal faktorer i  $n$ :  $\omega(n)$
- $\Pr(p \mid n) = 1/p$
- $E(\text{antalet faktorer}) = \sum_{p \leq n} \frac{1}{p} \approx \log \log n$
- **Bevis:** Elementärt eller med hjälp av primtalssatsen

$$\sum_{p \leq n} \frac{1}{p} = \int_2^n \frac{1}{x} d\pi(x) = \left[ \frac{\pi(x)}{x} \right]_2^n + \int_2^n \frac{\pi(x)}{x^2} dx$$
$$\approx \frac{1}{\log n} + \int_2^n \frac{dx}{x \log x} \approx \log \log n$$

# Förväntad största faktor

- $n = P_s(n) \cdot P_{s-1}(n) \cdot \dots \cdot P_2(n) \cdot P(n); \quad P_s(n) \leq P_{s-1}(n) \leq \dots \leq P_2(n) \leq P(n)$
- $s = \log \log n$

$$s - 1 \approx \log \log \frac{n}{P(n)} = \log(\log n - \log P(n)) =$$

$$= \log \log n + \log \left( 1 - \frac{\log P(n)}{\log n} \right) = s + \log \left( 1 - \frac{\log P(n)}{\log n} \right)$$

$$\log \left( 1 - \frac{\log P(n)}{\log n} \right) = -1$$

$$1 - \frac{\log P(n)}{\log n} = \frac{1}{e}$$

$$\log P(n) = \left( 1 - \frac{1}{e} \right) \cdot \log n$$

$$P(n) \approx n^{0.632}$$

# Förmodan om stora faktorer

För varje  $\theta$  i intervallet  $0 < \theta < 1/2$  finns ett  $c = c(\theta) > 0$  sådant att det finns åtminstone  $2cR/\log R$  stycken primtal  $r$  i  $[R, 2R]$  för vilka  $R - 1$  har en primfaktor  $q > r^{1/2+\theta}$ , förutsatt att  $R$  är tillräckligt stort.

Sant för  $\theta < 0,11$  (svårt)

Sant för  $\theta < 0,167$  (svårare, Fouvry)

Sant för  $\theta < 0,1683$  (svårast)

# Många $r$ med stort $o_r(n)$

**Lemma 5.** Antag förmodan sann för något  $\theta$ ,  $0 < \theta < 1/2$ . Antag  $n$  tillräckligt stort och att  $c(\theta)R^{2\theta} \geq \log n$ . Då finns minst  $c(\theta)R / \log R$  primtal  $r$  i  $[R, 2R]$  för vilka  $o_r(n) > r^{1/2+\theta}$ .

# Bevis

- Låt  $r \in [R, 2R]$ ,  $q \mid r$ ,  $q > r^{1/2+\theta}$  och  $o_r(n) < r^{1/2+\theta}$
- Det finns  $N$  sådana tal. För dessa  $r$  gäller:
- $o_r(n) \mid (r - 1) / q$
- $o_r(n) < r / q \leq r^{1/2-\theta} \leq (2R)^{1/2-\theta}$

$$r \mid \prod_{m \leq (2R)^{1/2-\theta}} (n^m - 1) \Rightarrow \prod_r r \mid \prod_{m \leq (2R)^{1/2-\theta}} (n^m - 1)$$

$$R^N < \prod_{m \leq (2R)^{1/2-\theta}} n^m = n^{\sum_{m \leq (2R)^{1/2-\theta}} m} < n^{R^{1-2\theta}}$$

$$N < R^{1-2\theta} \cdot (\log n) / \log R \leq c(\theta) R / \log R$$

- Minst hälften av talen blir bra!

# Korrolarium 6.

- Antag förmodan sann för något  $\theta$ ,  $0 < \theta < 1/2$ .
- Sätt  $\rho(\theta) := \max\left[\frac{1}{2\theta}, \frac{4}{1+2\theta}\right]$
- Då finns  $c'(\theta)$ ; om  $n$  tillräckligt stort, så finns primtal  $r < c'(\theta) (\log n)^{\rho(\theta)}$  för vilket  $o_r(n) > \log^2 n$ .

# Bevis

- Vi krävde förut:  $\frac{\log n}{R^{2\theta}} < c(\theta)$

$$R^{2\theta} > \frac{\log n}{c(\theta)}$$

$$R > c'(\theta) \cdot (\log n)^{1/2\theta}$$

- Vi kräver nu:

$$o_r(n) > r^{1/2+\theta} > R^{1/2+\theta} > \log^2 n$$

$$R > (\log n)^{2/(1/2+\theta)} = (\log n)^{4/(1+2\theta)}$$

- Det finns  $r < 2R$

# Sophie Germain-tal

- $r$  och  $q = (r - 1) / 2$  båda primtal
- $o_r(n) = 1, 2, q, 2q = r - 1$
- $o_r(n) < q \Leftrightarrow o_r(n) = 1$  eller  $2 \Rightarrow r \mid n^2 - 1$
- Sant för högst  $2 \log n$  tal
- I  $[R, 2R]$  finns  $O\left(\frac{R}{\log^2 R}\right)$  SG-tal
- De flesta har  $o_r(n) > R / 2 > \log^2 n$
- Det finns primtal med  $o_r(n) > \log^2 n$  som är  $> 4 \log^2 n$

# Sifferexempel AKS

	$\theta$	$1 / 2\theta$	$4 / (1 + 2\theta)$	$\rho(\theta)$	$1,5 \cdot \rho + 3$
Visat i dag				5	10,5
Bevisat i art.	0.11	50 / 11	4 / 1,22	50 / 11	9 9/11
Riesel ?	0,132	3,78	3,16	3,78	8,68
Fouvry	1/6	3	3	3	7,5
Sophie Germain	1			2	6

# Nästankroppar, definition:

- Givet heltal  $n$ , moniskt  $f(x) \in \mathbb{Z}[x]$ ,  $\text{grad}(f) = d \geq 1$ .  $\mathbb{Z}[x] / (n, f(x))$  är en *nästankropp* med parametrar  $(e, v(x))$  om
  - $e \mid n^d - 1$
  - $v(x)^{n^d - 1} \equiv 1 \pmod{(n, f(x))}$
  - $v(x)^{(n^d - 1)/q} - 1$  är en enhet i  $\mathbb{Z}[x] / (n, f(x))$  för alla primtal  $q \mid e$

# Nytt kriterium (Bernstein)

- Givet  $n \geq 2$ . Antag att
  - $\mathbb{Z}[x] / (n, f(x))$  är en *nästankropp* med parametrar  $(e, v(x))$ ,  $e > (2d \log n)^2$ .
  - Då är  $n$  primtal då och endast då
    - $n$  inte är en jämn potens
    - $(t-1)^{n^d} \equiv t^{n^d} - 1 \pmod{(n, f(x), t^e - v(x))}$  i  $\mathbb{Z}[x, t]$

# Probabilistisk

- Beviset som förut (tror jag)
- Om  $n$  primtal går det oftast snabbt att hitta nästankropp
- Testet går på  $\tilde{O}(\log^4 n)$
- Kombinera med Miller - Rabin

# Pseudokroppar, definition:

- Givet heltal  $n$ , moniskt  $f(x) \in \mathbb{Z}[x]$ ,  $\text{grad}(f) = d \geq 1$ .  $\mathbb{Z}[x]/(n, f(x))$  är en *pseudokropp* om
- $f(x^n) \equiv 0 \pmod{(n, f(x))}$
- $x^{n^d} - x \equiv 0 \pmod{(n, f(x))}$
- $x^{n^{d/q}} - x$  är en enhet i  $\mathbb{Z}[x] / (n, f(x))$  för alla primtal  $q \mid d$

# Lenstra och Pomerance

- Givet  $n \geq 2$ . Givet moniskt  $f(x) \in \mathbb{Z}[x]$ ,  $\text{grad}(f) = d$ ,  $d \in (\log^2 n, n)$  så att
  - $\mathbb{Z}[x] / (n, f(x))$  är en pseudokropp.
  - Då är  $n$  primtal då och endast då
    - $n$  inte är en jämn potens
    - $n$  inte har någon primfaktor  $\leq d$
    - $(x + a)^n \equiv x^n + a \pmod{(n, f(x))}$  för varje heltal  $a$ ,  $1 \leq a \leq A := \sqrt{d} \cdot \log n$

# Kommentarer

- $d \approx r, f(x) \approx x^r - 1$
- Bevis som förut
- Beräkningar som förut
- $\tilde{O}(\log^6 n)$
- Djupa bevis för att hitta  $f$