

# Primality testing in polynomial time

---

Or... a ripped-off talk from D.J. Bernstein's paper at <http://cr.yp.to>

## Primality testing

Given **decimal expansion** of  $n$ , return **Yes** iff  $n$  is prime

- not a factorization problem
- different from the compositeness problem

## What's new?

**Agrawal-Kayal-Saxena (2002)  $PRIMES \in P$**

There exists a deterministic algorithm testing primality of  $i$  in  $p(\log(i))$  computer cycles (i.e., the time needed to run the algorithm is polynomial in the size of its input)

**Deterministic:** No random choices, computations depend on algorithm and input only

**Bernstein (2003)** Simplified algorithm (Lenstra,...), improved exposition (!), speed-ups

## Known before

**Artjuhov (1966)**  $n \in 5 + 8\mathbb{Z}$ , divides none of  $b$ ,  $b^{(n-1)/2} + 1$ ,  $b^{(n-1)/4} + 1$ ,  $b^{(n-1)/4} - 1$ , then  $n$  is composite

**Miller-Oesterlé ('70s)** GRH,  $n$  composite then Artjuhov works for some  $b < O(1)(\log n)^2$ . Hence  $\text{GRH} \implies \text{PRIMES} \in P$

$n$  composite  $\implies 75\%$  of  $b$  give a successful test ( $\text{PRIMES} \in \text{coRP}$ )

**Lucas (1876)**  $\text{PRIMES} \in \text{NP}$

$n - 1 = \prod p_i$ ,  $n \mid a^{n-1} - 1$ ,  $n \nmid a^{(n-1)/p_i} - 1 \implies n$  prime

*"Lucas died as the result of a freak accident at a banquet when a plate was dropped and a piece flew up and cut his cheek. He died of erysipelas a few days later."*

## Known before (cont.)

**Adleman-Pomerance-Rumely 1979**  $(\log n)^{c \log \log \log n}$

**Morain** Elliptic curves (ECP), uses randomness and proves that *PRIMES* is in *RP*

## Actual results

20000-bits numbers in  $10^{14}$  clock cycles with elliptic curves methods

1000-bits number shown to be prime with algorithm based on AKS  
(announced Mar 8 2003)

## Algorithm (to test the primality of $n$ )

- positive integer  $n$  in decimal expansion
- is it a prime power?
- $N := 2n(n - 1)(n^2 - 1) \cdots (n^{4^{\lceil \lg n \rceil}} - 1)$  (where  $\lg n = \log_2 n$ )
- smallest  $r$  prime not dividing  $N$
- $n$  equal to any prime below  $r$ ?
- $n$  divisible by any prime below  $r$ ?
- $(x + b)^n \not\equiv (x^n + b)$  in  $(\mathbb{Z}/n\mathbb{Z})[x]/(x^r - 1)$  for all  $b \in \{1, 2, \dots, r\}$
- last case:  $n$  is prime!

**Why is  $r < p(\lg n)$ ?**

$$\begin{aligned} N &:= 2n(n-1)(n^2-1)\cdots(n^{4\lceil\lg n\rceil^2}-1) \\ &< 2n^{1+(2\lceil\lg n\rceil^2)(4\lceil\lg n\rceil^2+1)} \\ &< n^{8(\lg n)^4+\dots} \\ &< 2^{(8+o(1))(\lg n)^5} \end{aligned}$$

**Chebyshev**

$$\prod_{p_i < 2k} p_i > 2^k \text{ is true for large } k$$

Follows from the Prime Number Theorem

$$\#\{p \text{ prime} \in [1, x]\} \sim x / \ln x$$

So  $r < 2(8 + o(1))(\lg n)^5$

## The last case (Don't panic!)

Suppose we are in the last case, set  $S = \{1, \dots, r\}$  and  $v$  to be the order of  $n$  modulo  $r$ . Notice that  $v > 4\lceil \lg n \rceil^2$ . Set  $h := \Phi_r(x)$ .

- Let  $p|n$ ,  $p$  prime,  $p \neq n$
- If  $d|((r-1)/v)$ , then  $\binom{2r-2}{r} \geq n^{2d\lfloor \sqrt{(r-1)/d} \rfloor}$
- Take  $d := \#((\mathbb{Z}/r\mathbb{Z})^*/\langle n, p \rangle)$ ; lift to integers  $m_1, \dots, m_d$
- Prove  $(x^{m_w} + b)^{n^i p^j} = x^{n^i p^j m_w} + b$  in  $\mathbb{F}_p[x]/(x^r - 1) \quad \forall b \in S$
- $\exists 0 \leq i, j, k, l \leq \lfloor \sqrt{(r-1)/d} \rfloor$ ,  $(i, j) \neq (k, l)$ , so that  
 $t := n^i p^j \equiv n^k p^l =: u \pmod{r}$ . Note:  $|t - u| + 1 \leq n^{2\lfloor \sqrt{(r-1)/d} \rfloor}$

## The last case (Don't panic! cont.)

- $x^t = x^u$  in  $\mathbb{F}_p[x]/(x^r - 1)$ , so  $(x^{m_v} + b)^t = (x^{m_v} + b)^u \forall b \in S, \forall v$
- Define  $G$  in  $\mathbb{F}_p[x]/h$  as the group generated by mult. of  $\{0\} \cup \{x^{m_1} + b : b \in S\} \cup \dots \cup \{x^{m_d} + b : b \in S\}$ . Then  $g^t = g^u \quad \forall g \in G$ .
- $G^d \subset (\mathbb{F}_p[x]/h)^d$  has at least  $1 + \binom{2r-2}{r}$  elements, i.e. all vectors  $(\prod_{b \in S} (x^{m_1} + b)^{e_b}, \dots, \prod_{b \in S} (x^{m_d} + b)^{e_b})$  with  $\sum_b e_b \leq r - 2$
- $\#G^d \geq 1 + \binom{2r-2}{r} > n^{2d \lfloor \sqrt{(r-1)/d} \rfloor} \geq (|t - u| + 1)^d$
- $\#G > |t - u| + 1$  and all  $g \in G$  satisfy  $g^t = g^u \implies t = u$ .
- Contradiction because  $(i, j) \neq (k, l)$ , and  $t := n^i p^j, u := n^k p^l$

**If**  $d \mid ((r - 1)/v)$

- $d \leq (r - 1)/v < (r - 1)/4(\lg n)^2$
- $2d \lfloor \sqrt{(r - 1)/d} \rfloor \leq 2d \sqrt{(r - 1)/d} < \sqrt{4d(r - 1)} \leq (r - 1)/\lg n$
- $n^{2d \lfloor \sqrt{(r-1)/d} \rfloor} \leq 2^{(r-1)}$
- $\binom{2r-2}{r} \geq 2^{(r-1)}$ , because  $r - 1 \geq 2$

## Gaps between primes (Mar 2003)

Again, by the PNT, we should expect gaps between consecutive primes  $p_i$  and  $p_{i+1}$  to be  $\sim \ln p_i$

**Theorem (Goldston and Yildirim)** For any positive integer  $r$ ,

$$\liminf_{n \rightarrow \infty} \frac{p_{n+r} - p_n}{\ln p_n} = 0$$

Catch phrase:

*”There exist gaps between primes arbitrarily smaller than their expected size”*

Applications:

- twin primes (?)
- arbitrarily large gaps between primes (\$10,000 Erdős problem)
- April fools’ joke that no one reads