Randomized primality proving in essentially quartic time

D. J. Bernstein

Thanks to:
University of Illinois at Chicago
NSF DMS–0140542
Alfred P. Sloan Foundation
Math Sciences Research Institute
University of California at Berkeley

Thm: If

- $n > 1$;
- e divides $n - 1$;
- $e - 1 \geq c \geq b \geq 0$;
- $\binom{e}{b}\binom{c}{b}\binom{2e-1-c-b}{e-1-c} \geq n^{\lceil\sqrt{e/3}\rceil}$;
- $r^{n-1} = 1$ in $\mathbf{Z}/n$;
- $r^{(n-1)/q} - 1$ is a unit in $\mathbf{Z}/n$ for each prime q dividing e;
- $r - 1$ is a unit in $\mathbf{Z}/n$; and
- $(x-1)^n = r^{(n-1)/e}x - 1$ in the ring $(\mathbf{Z}/n)[x]/(x^e - r)$;

then n is a power of a prime.

$n = 314159265358979323846264338327950288 41$:

840 divides $n - 1$;

$\binom{840}{246}\binom{419}{246}\binom{1014}{420} \geq n^{\left\lceil\sqrt{840/3}\right\rceil}$;

$17^{n-1} = 1$ in $\mathbf{Z}/n$;

$17^{(n-1)/2} - 1$ is a unit in $\mathbf{Z}/n$;

$17^{(n-1)/3} - 1$ is a unit in $\mathbf{Z}/n$;

$17^{(n-1)/5} - 1$ is a unit in $\mathbf{Z}/n$;

$17^{(n-1)/7} - 1$ is a unit in $\mathbf{Z}/n$;

$(x-1)^n = 17^{(n-1)/840}x - 1$

in the ring $(\mathbf{Z}/n)[x]/(x^{840} - 17)$;

so n is a power of a prime.

There is an algorithm that,
given a prime n,
finds (randomly) and
verifies (deterministically)
a proof of primality of n
in time $(\lg n)^{4+o(1)}$.

Algorithm relies on generalization
of thm to extensions of $\mathbf{Z}/n$,
although most n's don't need this.
Also helpful to use $x-2, x-3, \ldots$.

`http://cr.yp.to`
`/papers.html#quartic`

Pf of thm:

Choose prime p dividing n.

Define ζ as image in $\mathbf{F}_p$ of $r^{(n-1)/e}$.
$\zeta^e = 1$, but $\zeta^{e/q} - 1$ is a unit in $\mathbf{F}_p$
for each prime q dividing e, so
ζ has order e, and e divides $p - 1$.

$r^{p-1} = 1$ in $\mathbf{F}_p$ so
$r^{(p-1)/e} = \zeta^\ell$ in $\mathbf{F}_p$ for some $\ell \in \mathbf{Z}$.

Define $S = \mathbf{F}_p[x]/(x^e - r)$.
$(x-1)^n = \zeta x - 1$ in S.

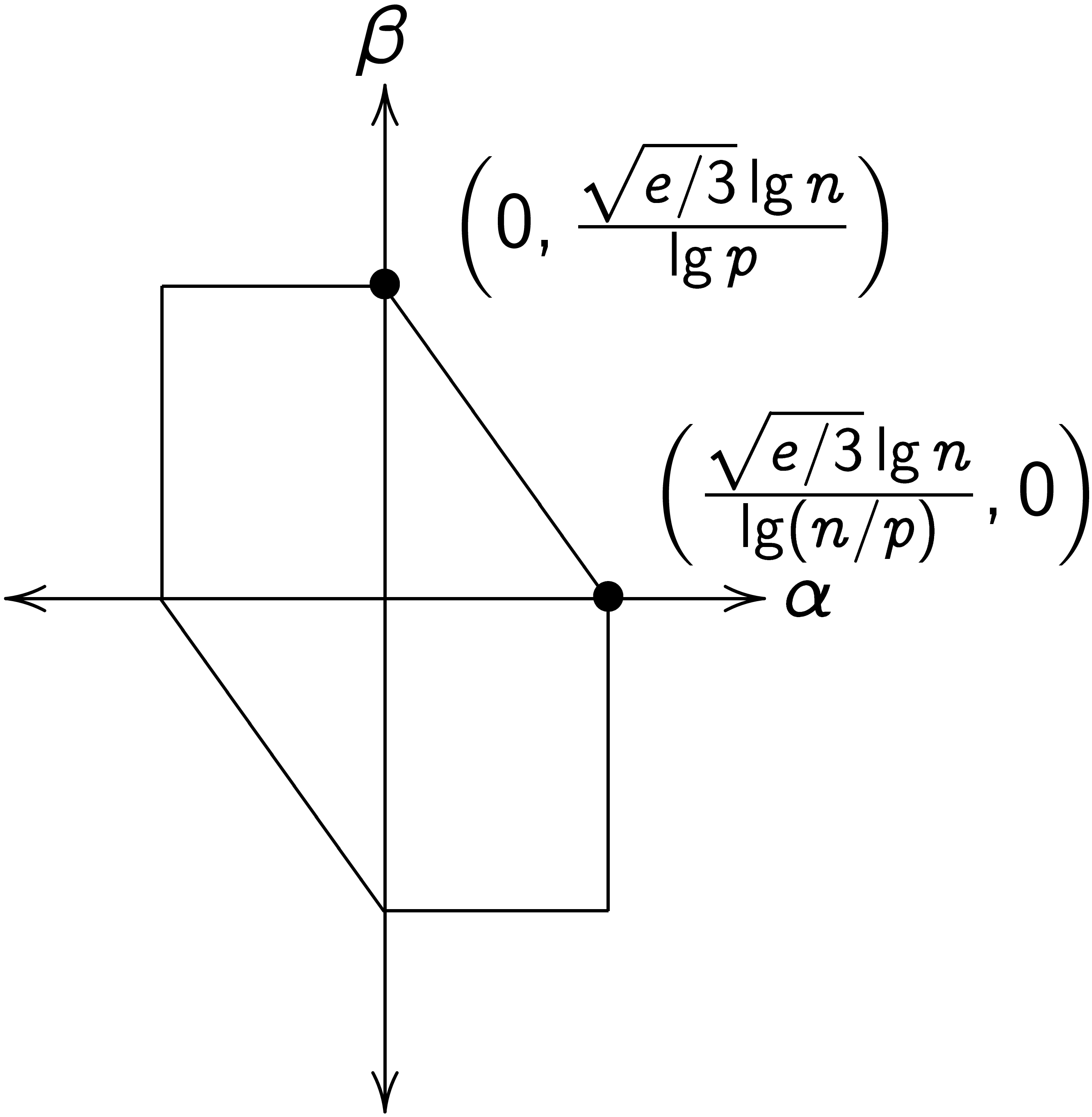
Substitute $\zeta^i x$ for x:
$(\zeta^i x - 1)^n = \zeta^{i+1} x - 1$
in $\mathbf{F}_p[x]/((\zeta^i x)^e - r) = S$.

$(x-1)^{n^i} = \zeta^i x - 1$ in S.

$(x-1)^{n^i p^j} = \zeta^{i+j\ell} x - 1$ in S.

Define C as the set of $(\alpha, \beta) \in \mathbf{R} \times \mathbf{R}$ such that $|\alpha \lg(n/p)|$, $|\beta \lg p|$, and $|\alpha \lg(n/p) + \beta \lg p|$ are $\le \sqrt{e/3} \lg n$.

If $p = n$, done.
Assume $p < n$.


β
$\left(0,\ \frac{\sqrt{e/3}\lg n}{\lg p}\right)$
$\left(\frac{\sqrt{e/3}\lg n}{\lg(n/p)}, 0\right)$
α

C is a closed convex symmetric set of area $3(e/3)\dfrac{(\lg n)^2}{(\lg p)\lg(n/p)}$, which is at least $4e$.

By Minkowski's theorem, C has a nonzero point (α, β) in the determinant-e lattice $\{(\alpha, \beta) \in \mathbf{Z} \times \mathbf{Z} :$ $\alpha + (\beta - \alpha)\ell \in e\mathbf{Z}\}$.

Assume wlog that $\alpha \geq 0$.

If $\beta \geq 0$, define
$u = (n/p)^\alpha p^\beta$ and $v = 1$.

Then u and v are positive integers;
u and v are $\leq n^{\sqrt{e/3}}$; and
$(x-1)^{up^\alpha} = (x-1)^{n^\alpha p^\beta}$
$= \zeta^{\alpha+\beta\ell} x - 1 = \zeta^{\alpha\ell} x - 1$
$= (x-1)^{p^\alpha} = (x-1)^{vp^\alpha}$ in S.

Similar results if $\beta < 0$: define
$u = (n/p)^\alpha$ and $v = p^{-\beta}$.

$x - 1$ is in S^*:

$x^e - r \bmod x - 1$ is in $\mathbf{F}_p^*$.

$(x-1)^{p^e} = x - 1$ in S so

order of $x - 1$ is coprime to p.

$(x-1)^{up^\alpha - vp^\alpha} = 1$ in S^*

so $(x-1)^{u-v} = 1$ in S^*.

Note that $|u - v| < n^{\sqrt{e/3}}$.

If $a_0, a_1, \ldots, a_{e-1} \in \mathbf{Z}$ then $(x-1)^{a_0} \cdots (\zeta^{e-1}x-1)^{a_{e-1}}$ is a power of $x-1$ in S^*.

Consider vectors $(a_0, a_1, \ldots, a_{e-1})$ with $\#\{i : a_i < 0\} = b$, $\sum_i -a_i[a_i < 0] \le c$, $\sum_i a_i[a_i \ge 0] \le e-1-c$.

Number of such vectors a is $\binom{e}{b}\binom{c}{b}\binom{2e-1-c-b}{e-1-c} \ge n^{\lceil \sqrt{e/3} \rceil}$.

Say two such vectors a, b have
$\prod_i(\zeta^i x - 1)^{a_i} = \prod_i(\zeta^i x - 1)^{b_i}$
in S^*.

Then $A = B$ in S where
$A = \prod(\zeta^i x - 1)^{a_i[a_i \geq 0] - b_i[b_i < 0]}$,
$B = \prod(\zeta^i x - 1)^{b_i[b_i \geq 0] - a_i[a_i < 0]}$.

$\deg A$, $\deg B$ are at most $e - 1$
so $A = B$ in $\mathbf{F}_p[x]$.
$x - 1, \zeta x - 1, \ldots, \zeta^{e-1} x - 1$
are coprime in $\mathbf{F}_p[x]$ so $a = b$.

So there are $> |u - v|$
powers of $x - 1$ in S^*.

Thus $u = v$, i.e., $n^\alpha = p^{\alpha-\beta}$.
If $\alpha = 0$ then $\beta = 0$, contradiction.
Thus n is a power of p.

Q.E.D.

History: proving compositeness

Displaying a factorization:
proof for every composite n;
verify in time $(\lg n)^{1+o(1)}$;
often very hard to find.

Fermat base 2 ("2-prp"):
proof for nearly every composite n;
find+verify in time $(\lg n)^{2+o(1)}$.

1966 Artjuhov (“sprp”), 1976 Rabin, 1980 Monier, 1982 Atkin-Larson: proof for every composite n; verify in time $(\lg n)^{2+o(1)}$; find in random time $(\lg n)^{2+o(1)}$.

Recognize failure of this algorithm as *guaranteeing* that n is prime. What if we want *proof*?

Conjecturally certifying primality

1976 Miller, with 1979 Oesterlé: conjectured cert for every prime n; find+verify in time $(\lg n)^{4+o(1)}$.

1995 Lukes-Patterson-Williams (or using idea of 1982 Yao): conjectured cert for every prime n; find+verify in time $(\lg n)^{3+o(1)}$.

1980 Baillie et al.: shakily conjectured cert for every prime n; find+verify in time $(\lg n)^{2+o(1)}$.

Proving primality

1876 Lucas: proof for every prime n;
verify in time at most $(\lg n)^{3+o(1)}$
(with Lehmer improvements),
conjectured $(\lg n)^{2+o(1)}$;
conjecturally can find
for infinitely many primes n
in time $(\lg n)^{O(1)}$,
but often very hard to find.

1914 Pocklington, 1975 Morrison, 1975 Brillhart-Lehmer-Selfridge: similar, but findable for more n's.

1979 Adleman-Pomerance-Rumely: proof for every prime n; find+verify in time $(\lg n)^{O(\lg \lg \lg n)}$.

1989 Pintz-Steiger-Szemerédi: proof for infinitely many primes n; verify in time $(\lg n)^{O(1)}$; find in time $(\lg n)^{O(1)}$.

1986 Goldwasser-Kilian, using
1985 Schoof: conjecturally,
proof for every prime n;
verify in time $(\lg n)^{3+o(1)}$;
conjecturally,
find in random time $(\lg n)^{O(1)}$.

1992 Adleman-Huang ("HECPP"):
proof for every prime n;
verify in time $(\lg n)^{O(1)}$;
find in random time $(\lg n)^{O(1)}$.

1993 Atkin-Morain: conjecturally,
proof for every prime n;
verify in time $(\lg n)^{3+o(1)}$;
conjecturally,
find in random time $(\lg n)^{5+o(1)}$.

Current ECPP: conjecturally,
proof for every prime n;
verify in time $(\lg n)^{3+o(1)}$;
conjecturally,
find in random time $(\lg n)^{4+o(1)}$.

2002.08 Agrawal-Kayal-Saxena:
proof for every prime n;
find+verify in time $(\lg n)^{O(1)}$,
conjectured $(\lg n)^{6+o(1)}$.

Introduced basic ideas of thm.

2003.03 Lenstra-Pomerance:
proof for every prime n;
find+verify in time $(\lg n)^{6+o(1)}$.

2002.11 Berrizbeitia:
proof for every prime n;
verify in time $(\lg n)^{4+o(1)}$ if
$\text{ord}_2(n^2 - 1) \geq (2 + o(1)) \lg \lg n$;
find in random time $(\lg n)^{2+o(1)}$.

Introduced idea of
using Kummer extensions,
twisting by powers of ζ.

2003.01 Cheng:
proof for every prime n;
verify in time $(\lg n)^{4+o(1)}$ if
$n-1$ has prime divisor $e \approx (\lg n)^2$;
find in random time $(\lg n)^{2+o(1)}$.

2003.01 Bernstein:
proof for every prime n;
verify in time $(\lg n)^{4+o(1)}$;
find in random time $(\lg n)^{2+o(1)}$.

Many constant-factor speedups:
parameter choice by Bernstein;
negative powers by Voloch,
with optimization by Vaaler;
n/p by Lenstra;
Minkowski by Lenstra.

Casual implementation using
Granlund et al.'s GMP 4.1.2:
primality proof for $2^{1024}+643$
in $\approx 3.8\cdot 10^{13}$ PIII cycles.

Serious implementation will still be an order of magnitude slower than current ECPP.

But within striking distance!