A new proof that 83 is prime

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

Theorem: 83 is prime.

Proof: Define R as the ring $(\mathbf{Z}/83)[i]/(i^2+1)$.

Map R onto a field k.

(There exists a prime p dividing 83, since $83 > 1$.
There exists an irreducible $\varphi \in (\mathbf{Z}/p)[i]$ dividing i^2+1.
Define $k = (\mathbf{Z}/p)[i]/\varphi$.)

Use calculator to see that

$83^2 - 1 = 14 \cdot 492$ in $\mathbf{Z}$

and $(2+i)^{492} = 34 + 16i$ in R.

(Square repeatedly:

$(2+i)^2 = 3 + 4i$ in R;

$(2+i)^3 = 2 + 11i$ in R;

$(2+i)^6 = -34 - 39i$ in R;

$\ldots$;

$(2+i)^{123} = 16 + 18i$ in R;

$(2+i)^{246} = 15 - 5i$ in R;

$(2+i)^{492} = 34 + 16i$ in R.)

Use calculator to see that
$(34+16i)^2-1=-14+9i$
is in R^*, reciprocal $41-27i$;
$(34+16i)^7-1=-2$
is in R^*, reciprocal 41;
and $(34+16i)^{14}=1$ in R.

Thus $(2+i)^{\#R-1}=1$ in R;
$(2+i)^{(\#R-1)/2}-1$ and
$(2+i)^{(\#R-1)/7}-1$ are in R^*;
also, $(2+i)-1$ is in R^*.

Define ζ as the image in k
of $(2+i)^{(\#R-1)/14}$.
Then $\zeta^2 \neq 1$, $\zeta^7 \neq 1$, $\zeta^{14} = 1$,
so ζ has order 14,
and 14 divides $\#k - 1$.

$(2+i)^{\#k-1} = 1$ in k
so $(2+i)^{(\#k-1)/14} = \zeta^\ell$ in k
for some $\ell \in \mathbf{Z}$.

Use calculator to see that

$$(x-1)^{83^2} = (2+i)^{(83^2-1)/14}x - 1$$

in the ring $R[x]/(x^{14} - (2+i))$.

(Square repeatedly:

$(x-1)^2 = x^2 - 2x + 1$,

$(x-1)^3 = x^3 - 3x^2 + 3x - 1$,

$\ldots$,

$(x-1)^{1722} = (-10+40i)x^{13} + \cdots$,

$(x-1)^{3444} = (-39-24i)x^{13} + \cdots$,

$(x-1)^{6888} = (-17+33i)x^{13} + \cdots$,

$(x-1)^{6889} = (34+16i)x - 1$.)

Define $S = k[x]/(x^{14} - (2+i))$.
$(x-1)^{\#R} = \zeta x - 1$ in S.

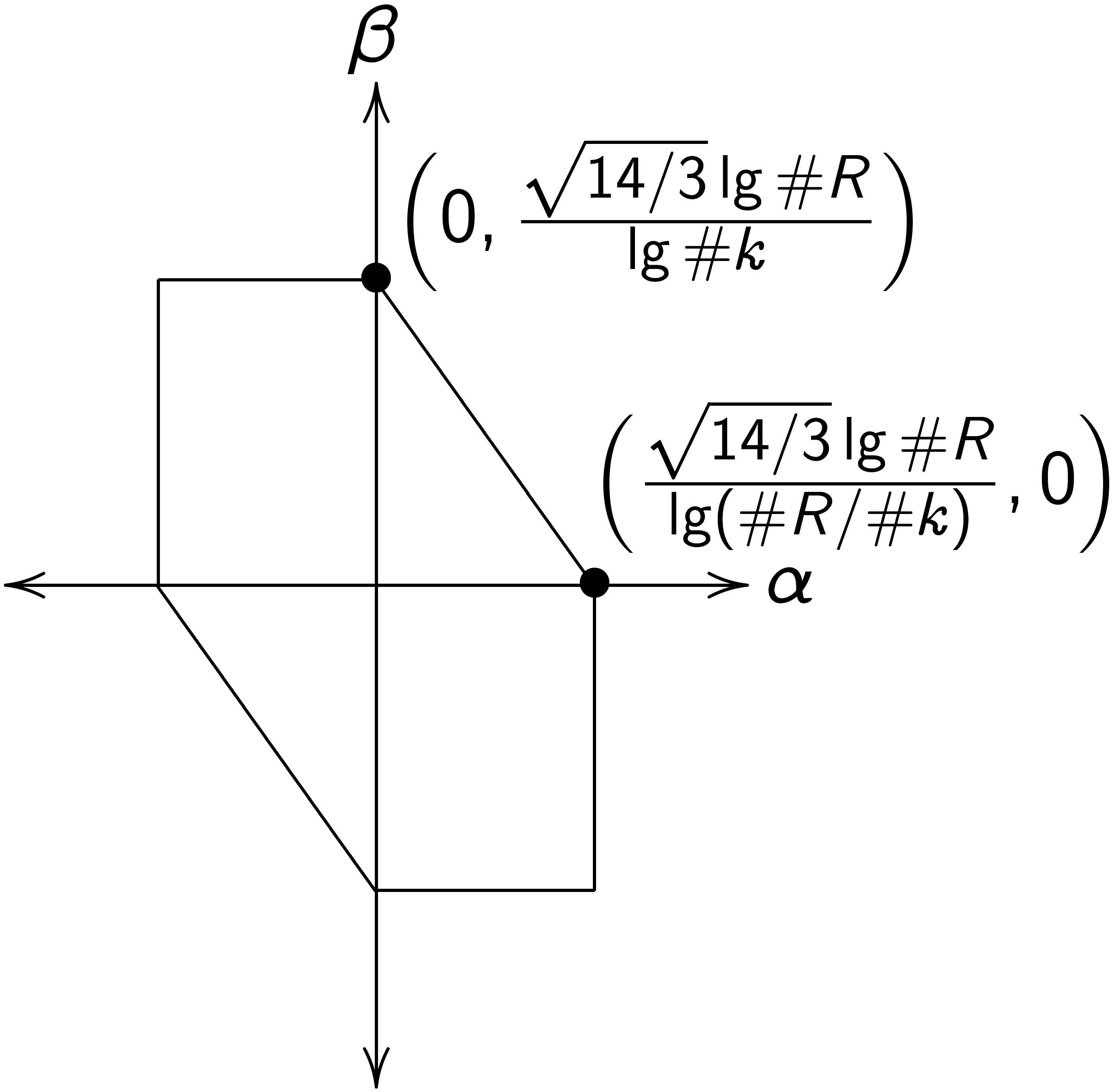
Substitute $\zeta^m x$ for x:
$(\zeta^m x - 1)^{\#R} = \zeta^{m+1} x - 1$
in $k[x]/((\zeta^m x)^{14} - (2+i)) = S$.

$(x-1)^{\#R^m} = \zeta^m x - 1$ in S.

$(x-1)^{\#R^m \#k^j} = \zeta^{m+j\ell} x - 1$ in S.

Define C as the set of $(\alpha, \beta) \in \mathbf{R} \times \mathbf{R}$ such that $|\alpha \lg(\#R/\#k)|$, $|\beta \lg \#k|$, and $|\alpha \lg(\#R/\#k) + \beta \lg \#k|$ are $\le \sqrt{14/3} \lg \#R$.

If $\#k = \#R$ then can skip to end of proof, so assume $\#k < \#R$.



β
$\left(0, \frac{\sqrt{14/3}\,\lg \#R}{\lg \#k}\right)$
$\left(\frac{\sqrt{14/3}\,\lg \#R}{\lg(\#R/\#k)}, 0\right)$
α

C is a closed convex symmetric set of area $3(14/3)\dfrac{(\lg \#R)^2}{(\lg \#\boldsymbol{k})\lg(\#R/\#\boldsymbol{k})}$, which is at least $4 \cdot 14$.

By Minkowski's theorem, C has a nonzero point (α, β) in the determinant-14 lattice $\{(\alpha, \beta) \in \mathbf{Z} \times \mathbf{Z} :$ $\alpha + (\beta - \alpha)\ell \in 14\mathbf{Z}\}$.

Assume wlog that $\alpha \geq 0$.

If $\beta \geq 0$, define
$u = (\#R/\#k)^\alpha \#k^\beta$ and $v = 1$.

Then u and v are positive integers;
u and v are $\leq \#R^{\sqrt{14/3}}$; and
$(x-1)^{u\#k^\alpha} = (x-1)^{\#R^\alpha \#k^\beta}$
$= \zeta^{\alpha+\beta\ell} x - 1 = \zeta^{\alpha\ell} x - 1$
$= (x-1)^{\#k^\alpha} = (x-1)^{v\#k^\alpha}$ in S.

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

$x-1$ is in S^*:
$x^{14}-(2+i)$ mod $x-1$ is
$1-(2+i)$, which is in k^*.

$(x-1)^{\#k^{14}} = x-1$ in S so
order of $x-1$ is coprime to $\#k$.
$(x-1)^{u\#k^\alpha - v\#k^\alpha} = 1$ in S^*
so $(x-1)^{u-v} = 1$ in S^*.

Note that $|u-v| < (83^2)^{\sqrt{14/3}}$.
Use calculator to see that
$(83^2)^{\sqrt{14/3}} < (83^2)^{\sqrt{169/36}}$
$= 83^{13/3} < 210000000$.

If $a_0, a_1, \ldots, a_{13} \in \mathbf{Z}$ then
$(x-1)^{a_0} \cdots (\zeta^{13} x - 1)^{a_{13}}$
is a power of $x-1$ in S^*.

Consider vectors $(a_0, a_1, \ldots, a_{13})$
with $\#\{m : a_m < 0\} = 4$,
$\sum_m -a_m[a_m < 0] \le 6$,
$\sum_m a_m[a_m \ge 0] \le 7$.

Number of such vectors a is
$\binom{14}{4}\binom{6}{4}\binom{17}{7}$; use calculator to see
that $\binom{14}{4}\binom{6}{4}\binom{17}{7} = 292011720$.

Say two such vectors a, b have
$\prod_m (\zeta^m x - 1)^{a_m} = \prod_m (\zeta^m x - 1)^{b_m}$
in S^*.

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

deg A, deg B are at most $6 + 7 < 14$
so $A = B$ in $k[x]$.
$x - 1, \zeta x - 1, \ldots, \zeta^{13} x - 1$
are coprime in $k[x]$ so $a = b$.

So there are ≥ 292011720 powers of $x - 1$ in S^*.

Thus $u = v$, i.e., $\#R^\alpha = \#k^{\alpha-\beta}$.
If $\alpha = 0$ then $\beta = 0$, contradiction.
Thus 83 is a power of a prime.

Use calculator to see that
83 is not a square, cube, etc.
Thus 83 is prime.

Q.E.D.

This is a really stupid way to prove that 83 is prime.

But it scales really well!

Any prime n has
a similar proof of primality.
Verify in time $(\lg n)^{4+o(1)}$.
Find in expected time $(\lg n)^{2+o(1)}$;
GRH guarantees time $(\lg n)^{2+o(1)}$.

Proving primality of
$n = 314159265358979323846264338327950288 41$:

Use $R = \mathbf{Z}/n$. Check that

- 840 divides $n - 1$;
- $17^{(n-1)/840}$ is a primitive 840th root of 1 in R;
- $(x - 1)^n = 17^{(n-1)/840}x - 1$ in $R[x]/(x^{840} - 17)$; and
- $\binom{840}{246}\binom{419}{246}\binom{1014}{420} \ge n^{\lceil\sqrt{840/3}\rceil}$.

Basic ideas introduced August 2002 by Agrawal-Kayal-Saxena.

Kummer and twists introduced November 2002 by Berrizbeitia: verify in time $(\lg n)^{4+o(1)}$ if $n \pm 1$ has large power of 2.

Generalized to any n January 2003 by Bernstein, analogously to 1985 Lenstra.

Constant-factor speedups:
parameter choice by Bernstein;
negative powers by Voloch,
with optimization by Vaaler;
$\#R/\#k$ by Lenstra;
Minkowski by Lenstra.

Can we achieve $(\lg n)^{3+o(1)}$?
Want to prove that there are
many more powers of $x - 1$ in S^*.