Sharper ABC-based bounds for congruent polynomials

Or: Fun with radical combinatorics

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

How to prove that n is prime

Select group scheme G over $\mathbf{Z}/n$.
Typical examples: $(\mathbf{Z}/n)^*$;
$((\mathbf{Z}/n)[x]/(x^2+1))^*$;
an elliptic curve over $\mathbf{Z}/n$.

Prove that $G(\mathbf{Z}/p)$ is large
for all primes p dividing n.
Conclude that p is large.

How to prove that group is large

Old strategy (Pocklington et al.): Identify order-q element of group, for various prime powers q dividing presumed group order.

New strategy (Fellows-Koblitz, Agrawal-Kayal-Saxena, et al.): Combinatorially identify many distinct elements of group.

Typical example

Given $h \in k[x]$, $\deg h = e$,
$S \subseteq k$, $\#S = e$, with
$x - s \in (k[x]/h)^*$ for each $s \in S$.

Consider group $G \subseteq (k[x]/h)^*$
generated by $\{x - s : s \in S\}$.

$\#G \geq 2^e - 1$: products of
proper subsets of $\{x - s\}$
are all distinct modulo h.

Better bounds

$\#G \geq \binom{2e-1}{e} \approx 2^{2e}$:
count polynomials of degree $\leq e-1$.

$\#G \geq \binom{e}{z}\binom{\lfloor e/2 \rfloor}{z}\binom{\lceil e/2 \rceil - 1 + e - z}{e-z}$
$\approx 2^{2.54e}$ with $z \approx 0.29e$:
count rational functions
with numerator degree $\leq \lfloor e/2 \rfloor$
and denominator degree $\leq \lceil e/2 \rceil - 1$.

Lower bound $2^{\alpha e}$ produces
α^4 speedup in AKS algorithm,
α^2 speedup in newer variants.

Applying ABC

Look at polynomials of larger degree.
Use ABC theorem to see that
three such polynomials
cannot be the same modulo h.

Suggested by Voloch.
Further improvements by Bernstein:
$\#G \geq \frac{1}{3}\binom{\lfloor 2.1e \rfloor}{e} \approx 2^{2.096e}$.

Thm: If $h \in k[x]$, $\deg h > 0$,
$1, 2, 3, \ldots, 3 \deg h - 2 \in k^*$,
$a, b, c \in k[x]$, distinct, nonzero,
$\gcd \{a, b, c\} = 1$,
$a \equiv b \equiv c \pmod{h}$
then $\deg \operatorname{rad} abc >$
$2 \deg h - \max \{\deg a, \deg b, \deg c\}$.

Typical example:
$a = x^{20}$, $b = x^{10}$, $c = 1$,
$\operatorname{rad} abc = x$, $h = x^{10} - 1$.

Pf: Assume $\deg a$ largest. Define
$u = \frac{b-c}{h}$, $v = \frac{c-a}{h}$, $w = \frac{a-b}{h}$,
$d = \gcd\{ua, vb, wc\}$.

$\deg a > 0$ so $\deg \operatorname{rad} abc > 0$.
Done unless $\deg a \le 2 \deg h - 1$.

Idea when $d = 1$: $(ua)' \ne 0$
since $1 \le \deg ua \le 3 \deg h - 2$.
$ua + vb + wc = 0$ so
$\deg \operatorname{rad} uvwabc > \deg ua$ so
$\deg uvw + \deg \operatorname{rad} abc > \deg ua$.
Use $\deg vw \le 2(\deg a - \deg h)$.

For arbitrary d:

Done unless $\deg d < \deg ua$.

$(ua/d)' \neq 0$ since

$1 \leq \deg(ua/d) \leq 3 \deg h - 2$.

$ua/d + vb/d + wc/d = 0$ so

$\deg \operatorname{rad}(uvwabc/d^3) > \deg(ua/d)$.

Voloch continuation: d divides

$\gcd \{uvwa, uvwb, uvwc\} = uvw$ so

$2 \deg uvw + \deg \operatorname{rad} abc > \deg ua$.

Bernstein continuation:
$d\,\mathrm{rad}(uvwabc/d^3)$ divides $uvw\,\mathrm{rad}\,abc$.

(Exponents: If $\min\{a,b,c\}=0$ and $d=\min\{u+a,v+b,w+c\}$ then $d+[u+v+w+a+b+c>3d] \le u+v+w+[a+b+c>0]$.)

So for any d obtain $\deg uvw + \deg\mathrm{rad}\,abc > \deg ua$. ■

Thm: If $h \in k[x]$, $\deg h > 0$,
$1, 2, 3, \ldots, 3\deg h - 2 \in k^*$,
$a, b, c \in k[x]$, distinct, nonzero,
$\gcd\{a, b, c\}$ coprime to h,
$a \equiv b \equiv c \pmod{h}$
then $\max\{\deg a, \deg b, \deg c\} >$
$2\deg h$
$- \deg \operatorname{rad} a - \deg \operatorname{rad} b - \deg \operatorname{rad} c$
$+ \deg \operatorname{rad} \gcd\{a, b\}$
$+ \deg \operatorname{rad} \gcd\{a, c\}$
$+ \deg \operatorname{rad} \gcd\{b, c\}$.

Pf: Divide by gcd; incl-excl. ∎

What about $a_1 \equiv a_2 \equiv a_3 \equiv a_4$?

Sum previous inequality for $\{a_1, a_2, a_3\}$, $\{a_1, a_2, a_4\}$, etc.:

$$
\begin{aligned}
&4 \max\{\deg a_i\} > 8 \deg h \\
&- 3 \deg \operatorname{rad} a_1 - 3 \deg \operatorname{rad} a_2 \\
&- 3 \deg \operatorname{rad} a_3 - 3 \deg \operatorname{rad} a_4 \\
&+ 2 \deg \operatorname{rad} \gcd\{a_1, a_2\} \\
&+ 2 \deg \operatorname{rad} \gcd\{a_1, a_3\} \\
&+ 2 \deg \operatorname{rad} \gcd\{a_1, a_4\} \\
&+ 2 \deg \operatorname{rad} \gcd\{a_2, a_3\} \\
&+ 2 \deg \operatorname{rad} \gcd\{a_2, a_4\} \\
&+ 2 \deg \operatorname{rad} \gcd\{a_3, a_4\}.
\end{aligned}
$$

$$\deg \operatorname{rad} a_1 a_2 a_3 a_4 \geq$$
$$\deg \operatorname{rad} a_1 + \deg \operatorname{rad} a_2$$
$$\deg \operatorname{rad} a_3 + \deg \operatorname{rad} a_4$$
$$- \deg \operatorname{rad} \gcd \{a_1, a_2\}$$
$$- \deg \operatorname{rad} \gcd \{a_1, a_3\}$$
$$- \deg \operatorname{rad} \gcd \{a_1, a_4\}$$
$$- \deg \operatorname{rad} \gcd \{a_2, a_3\}$$
$$- \deg \operatorname{rad} \gcd \{a_2, a_4\}$$
$$- \deg \operatorname{rad} \gcd \{a_3, a_4\}$$

by incl-excl, so

$$3 \deg \operatorname{rad} a_1 a_2 a_3 a_4 + 4 \max \{\deg a_i\}$$
$$> 8 \deg h$$
$$- \deg \operatorname{rad} \gcd \{a_1, a_2\} - \cdots.$$

Use $\deg \operatorname{rad} \gcd \{a_1, a_2\} \le$
$\max \{\deg a_i\} - \deg h$.

$\deg \operatorname{rad} a_1 a_2 a_3 a_4 >$
$(14/3) \deg h - (10/3) \max \{\deg a_i\}$.

In particular, if $\deg h = e$
and $\deg \operatorname{rad} a_1 a_2 a_3 a_4 \le e$,
then $\max \{\deg a_i\} > 1.1e$.

So 4 products of degree $\le \lfloor 1.1e \rfloor$
cannot all be the same modulo h.

$\#G \ge \frac{1}{3} \binom{\lfloor 2.1e \rfloor}{e}$.

More polynomials

Consider distinct $a_1, a_2, \ldots, a_m$, all congruent modulo h.

Average all subsets of 3: max degree $> \frac{3m^2-5m-6}{3m^2-7m} e$.

Challenge: Prove max degree $\geq 2e$ for some moderate m. Would give lower bound $\approx 2^{2.75e}$ for $\#G$.

Don't have to use ABC per se; play with many derivatives directly.