Journal de Théorie des Nombres de Bordeaux, to appear.

SHARPER ABC-BASED BOUNDS FOR CONGRUENT POLYNOMIALS

DANIEL J. BERNSTEIN

Abstract. Agrawal, Kayal, and Saxena recently introduced a new method of proving that an integer is prime. The speed of the Agrawal-Kayal-Saxena method depends on proven lower bounds for the size of the multiplicative semigroup generated by several polynomials modulo another polynomial h. Voloch pointed out an application of the Stothers-Mason ABC theorem in this context: under mild assumptions, distinct polynomials A, B, C of degree at most $1.2 \deg h - 0.2 \deg \operatorname{rad} ABC$ cannot all be congruent modulo h. This paper presents two improvements in the combinatorial part of Voloch's argument. The first improvement moves the degree bound up to $2 \deg h - \deg \operatorname{rad} ABC$. The second improvement generalizes to $m \geq 3$ polynomials $A_1, \ldots, A_m$ of degree at most $((3m-5)/(3m-7)) \deg h - (6/(3m-7)m) \deg \operatorname{rad} A_1 \cdots A_m$.

1. Introduction

Fix a nonconstant univariate polynomial h over a field k. Assume that the characteristic of k is at least $3 \deg h - 1$. The main theorem of this paper, Theorem 2.3, states that if $m \geq 3$ distinct polynomials $A_1, \ldots, A_m$ are all congruent modulo h and coprime to h then

$$\max\{\deg A_1, \ldots, \deg A_m\} > \frac{3m-5}{3m-7} \deg h - \frac{6}{(3m-7)m} \deg \operatorname{rad} A_1 \cdots A_m.$$

As usual, $\operatorname{rad} X$ means the largest monic squarefree divisor of X, i.e., the product of the monic irreducibles dividing X. If $\deg \operatorname{rad} A_1 \cdots A_m < (m/3) \deg h$ then this bound is better than the obvious bound $\max\{\deg A_1, \ldots, \deg A_m\} > \deg h - 1$.

For example, if distinct polynomials A, B, C are congruent modulo h and coprime to h then $\max\{\deg A, \deg B, \deg C\} > 2 \deg h - \deg \operatorname{rad} ABC$. No better bound is possible in this level of generality: if $h = x^{10} - 1$, $A = x^{20}$, $B = x^{10}$, and $C = 1$ then $\operatorname{rad} ABC = \operatorname{rad} x^{30} = x$ so $2 \deg h - \deg \operatorname{rad} ABC = 19$.

The proof relies on the Stothers-Mason ABC theorem. Analogous bounds in the number-field case follow from the ABC conjecture.

Previous work. Voloch in [3] proved that $\max\{\deg A, \deg B, \deg C\} > 1.2 \deg h - 0.2 \deg \operatorname{rad} ABC$. This paper improves Voloch's result in two ways: first, it is quantitatively stronger, in the interesting case that $\deg \operatorname{rad} ABC < \deg h$; second, it applies to larger values of m.

Date: 2003.10.01. Permanent ID of this document: `1d9e079cee20138de8e119a99044baa3`.

2000 *Mathematics Subject Classification.* Primary 11C08.

The author was supported by the National Science Foundation under grant DMS–0140542, and by the Alfred P. Sloan Foundation. He used the libraries at the Mathematical Sciences Research Institute and the University of California at Berkeley.

Application. Consider the subgroup G of $(k[x]/h)^*$ generated by $\{x-s : s \in S\}$, where $S \subseteq k$ and $0 \notin h(S)$. The Agrawal-Kayal-Saxena primality-proving method requires a lower bound on $\#G$ for groups G of this type, typically with $\#S = \deg h$. The primality-proving method becomes faster as the lower bound on $\#G$ increases, as discussed in [1, Section 7].

This paper shows that $\#G \geq \frac{1}{m-1}\binom{\lfloor((3m-5)/(3m-7))\deg h-(6/(3m-7)m)\#S\rfloor+\#S}{\#S}$ for any $m \geq 3$. Indeed, the binomial coefficient is the number of products of powers of $\{x-s\}$ in $k[x]$ of degree at most $\lfloor((3m-5)/(3m-7))\deg h-(6/(3m-7)m)\#S\rfloor$; m distinct such products cannot all have the same image modulo h.

In particular, if $\#S = \deg h$, then $\#G \geq \frac{1}{3}\binom{\lfloor 2.1\deg h\rfloor}{\deg h} \approx 4.27689^{\deg h}$. Compare this to the bound $\#G \geq \binom{2\deg h-1}{\deg h} \approx 4^{\deg h}$ obtained from a degree bound of $\deg h - 1$. Note that the improvement requires $m > 3$.

Different methods from [3] produce a lower bound around $5.828^{\deg h}$, so the ABC-based techniques in [3] and in this paper have not yet had an impact on the speed of primality proving. However, I suspect that these techniques have not yet reached their limits.

2. Proofs

Theorem 2.1. *Let k be a field. Let h be a positive-degree element of the polynomial ring $k[x]$. Assume that $1, 2, 3, \ldots, 3\deg h - 2$ are invertible in k. Let A, B, C be distinct nonzero elements of $k[x]$. If $\gcd\{A,B,C\} = 1$ and $A \equiv B \equiv C \pmod h$ then $\max\{\deg A, \deg B, \deg C\} > 2\deg h - \deg\operatorname{rad} ABC$.*

Proof. Assume without loss of generality that $\deg A = \max\{\deg A, \deg B, \deg C\}$. The nonzero polynomial $A-B$ is a multiple of h, so $\deg A \geq \deg(A-B) \geq \deg h > 0$; thus $\deg\operatorname{rad} ABC > 0$.

If $\deg A \geq 2\deg h$ then $\deg A > 2\deg h - \deg\operatorname{rad} ABC$; done.

Define $U = (B-C)/h$, $V = (C-A)/h$, and $W = (A-B)/h$. Then $U \neq 0$; $V \neq 0$; $W \neq 0$; U, V, W each have degree at most $\deg A - \deg h$; and $UA + VB + WC = 0$. Define $D = \gcd\{UA, VB, WC\}$.

If $\deg D = \deg UA$ then UA divides VB, WC; so A divides VWA, VWB, VWC; so A divides $\gcd\{VWA, VWB, VWC\} = VW$; but $VW \neq 0$, so $\deg A \leq \deg VW \leq 2(\deg A - \deg h)$; so $\deg A \geq 2\deg h$; done.

Assume from now on that $\deg D < \deg UA$ and that $\deg A \leq 2\deg h - 1$. Then $\deg(UA/D)$ is between 1 and $2\deg A - \deg h \leq 3\deg h - 2$; so the derivative of UA/D is nonzero. Also $UA/D + VB/D + WC/D = 0$, and $\gcd\{UA/D, VB/D, WC/D\} = 1$. By Theorem 3.1 below, $\deg(UA/D) < \deg\operatorname{rad}((UA/D)(VB/D)(WC/D))$.

The proof follows Voloch up to this point. Voloch next observes that D divides $\gcd\{UVWA, UVWB, UVWC\} = UVW\gcd\{A,B,C\} = UVW$. I claim that more is true: $D\operatorname{rad}((UA/D)(VB/D)(WC/D))$ divides $UVW\operatorname{rad} ABC$.

(In other words: If $d = \min\{u+a, v+b, w+c\}$ and $\min\{a,b,c\} = 0$ then $d + [u+v+w+a+b+c > 3d] \leq u+v+w+[a+b+c > 0]$. Proof: Without loss of generality assume $a = 0$. Then $d \leq u \leq u+v+w$. If $d < u+v+w$ then $d + [\cdots] \leq d+1 \leq u+v+w \leq u+v+w+[\cdots]$ as claimed. If $a+b+c > 0$ then $d+[\cdots] \leq u+v+w+1 = u+v+w+[\cdots]$ as claimed. Otherwise $u+v+w+a+b+c = d \leq 3d$ so $d + [u+v+w+a+b+c > 3d] = d \leq u+v+w \leq u+v+w+[\cdots]$ as claimed.)

Thus $\deg UA < \deg(D \operatorname{rad}((UA/D)(VB/D)(WC/D))) \leq \deg(UVW \operatorname{rad} ABC)$. Hence $\deg A < \deg(VW \operatorname{rad} ABC) \leq 2(\deg A - \deg h) + \deg \operatorname{rad} ABC$; i.e., $\deg A > 2\deg h - \deg \operatorname{rad} ABC$ as claimed. □

Theorem 2.2. *Let k be a field. Let h be a positive-degree element of the polynomial ring $k[x]$. Assume that $1, 2, 3, \ldots, 3\deg h - 2$ are invertible in k. Let A, B, C be distinct nonzero elements of $k[x]$. If $\gcd\{A, B, C\}$ is coprime to h and $A \equiv B \equiv C \pmod{h}$ then*

$$\begin{aligned}\max\{&\deg A, \deg B, \deg C\} \\ &> 2\deg h - \deg \operatorname{rad} A - \deg \operatorname{rad} B - \deg \operatorname{rad} C \\ &\quad + \deg \operatorname{rad} \gcd\{A, B\} + \deg \operatorname{rad} \gcd\{A, C\} + \deg \operatorname{rad} \gcd\{B, C\}.\end{aligned}$$

Proof. Write $G = \gcd\{A, B, C\}$. Then G is coprime to h, so $A/G \equiv B/G \equiv C/G \pmod{h}$. By Theorem 2.1,

$$\max\left\{\deg \frac{A}{G}, \deg \frac{B}{G}, \deg \frac{C}{G}\right\} > 2\deg h - \deg \operatorname{rad} \frac{ABC}{GGG} \geq 2\deg h - \deg \operatorname{rad} ABC,$$

so $\max\{\deg A, \deg B, \deg C\} \geq 2\deg h + \deg G - \deg \operatorname{rad} ABC$. But $\deg G \geq \deg \operatorname{rad} G = \deg \operatorname{rad} ABC - \deg \operatorname{rad} A - \deg \operatorname{rad} B - \deg \operatorname{rad} C + \deg \operatorname{rad} \gcd\{A, B\} + \deg \operatorname{rad} \gcd\{A, C\} + \deg \operatorname{rad} \gcd\{B, C\}$ by inclusion-exclusion. □

Theorem 2.3. *Let k be a field. Let h be a positive-degree element of the polynomial ring $k[x]$. Assume that $1, 2, 3, \ldots, 3\deg h - 2$ are invertible in k. Let S be a finite subset of $k[x] - \{0\}$, with $\#S \geq 3$. If each element of S is coprime to h, and all the elements of S are congruent modulo h, then*

$$\max\{\deg A : A \in S\} > \frac{3\#S - 5}{3\#S - 7} \deg h - \frac{6}{(3\#S - 7)\#S} \deg \operatorname{rad} \prod_{A \in S} A.$$

For example, $\max\{\deg A : A \in S\} > 1.4 \deg h - 0.3 \deg \operatorname{rad} \prod_{A \in S} A$ if $\#S = 4$, and $\max\{\deg A : A \in S\} > 1.25 \deg h - 0.15 \deg \operatorname{rad} \prod_{A \in S} A$ if $\#S = 5$.

Proof. Define $d = \max\{\deg A : A \in S\}$ and $e = \deg \operatorname{rad} \prod_{A \in S} A$. By Theorem 2.2,

$$\begin{aligned}d &> 2\deg h - \deg \operatorname{rad} A - \deg \operatorname{rad} B - \deg \operatorname{rad} C \\ &\quad + \deg \operatorname{rad} \gcd\{A, B\} + \deg \operatorname{rad} \gcd\{A, C\} + \deg \operatorname{rad} \gcd\{B, C\}\end{aligned}$$

for any distinct $A, B, C \in S$. Average this inequality over all choices of A, B, C to see that $d > 2\deg h - 3 \operatorname{avg}_A \deg \operatorname{rad} A + 3 \operatorname{avg}_{A \neq B} \deg \operatorname{rad} \gcd\{A, B\}$. On the other hand, $e \geq \#S \operatorname{avg}_A \deg \operatorname{rad} A - \binom{\#S}{2} \operatorname{avg}_{A \neq B} \deg \operatorname{rad} \gcd\{A, B\}$ by inclusion-exclusion, so

$$d + \frac{3}{\#S} e > 2\deg h - \frac{3\#S - 9}{2} \operatorname{avg}_{A \neq B} \deg \operatorname{rad} \gcd\{A, B\}.$$

Note that $3\#S - 9 \geq 0$ since $\#S \geq 3$.

One can bound each term $\deg \operatorname{rad} \gcd\{A, B\}$ by the simple observation that $A/\gcd\{A, B\}$ and $B/\gcd\{A, B\}$ are distinct congruent polynomials of degree at most $d - \deg \gcd\{A, B\}$; thus $d - \deg \gcd\{A, B\} \geq \deg h$, so $\deg \operatorname{rad} \gcd\{A, B\} \leq d - \deg h$. Hence

$$d + \frac{3}{\#S} e > 2\deg h - \frac{3\#S - 9}{2}(d - \deg h);$$

i.e., $d > ((3\#S - 5)/(3\#S - 7)) \deg h - (6/(3\#S - 7)\#S)e$. □

3. Appendix: the ABC theorem

Theorem 3.1 is a typical statement of the Stothers-Mason ABC theorem, included in this paper for completeness. The proof given here is due to Noah Snyder; see [2].

Theorem 3.1. *Let k be a field. Let A, B, C be nonzero elements of the polynomial ring $k[x]$ with $A+B+C=0$ and $\gcd\{A,B,C\}=1$. If $\deg A \ge \deg \operatorname{rad} ABC$ then $A'=0$.*

In fact, $A'=B'=C'=0$. As usual, X' means the derivative of X; the relevance of derivatives is that $X/\operatorname{rad} X$ divides X'.

Proof. Note that $\gcd\{A,B\} = \gcd\{A,B,-(A+B)\} = \gcd\{A,B,C\} = 1$. By the same argument, $\gcd\{A,C\}=1$ and $\gcd\{B,C\}=1$.

$C/\operatorname{rad} C$ divides both C and C', so it divides $C'B-CB'$. Similarly, $B/\operatorname{rad} B$ divides $C'B-CB'$. Furthermore, $C' = -(A'+B')$, so $C'B-CB' = -(A'+B')B + (A+B)B' = AB'-A'B$; thus $A/\operatorname{rad} A$ divides $C'B-CB'$.

The ratios $A/\operatorname{rad} A, B/\operatorname{rad} B, C/\operatorname{rad} C$ are pairwise coprime, so their product $ABC/\operatorname{rad} ABC$ divides $C'B-CB'$. But by hypothesis $\deg(ABC/\operatorname{rad} ABC) = \deg ABC - \deg \operatorname{rad} ABC \ge \deg BC > \deg(C'B-CB')$; so $C'B-CB'=0$; so $AB'-A'B=0$; so A divides $A'B$; but A and B are coprime, so A divides A'; but $\deg A > \deg A'$, so $A'=0$. $\square$

References

[1] Daniel J. Bernstein, *Proving primality in essentially quartic random time*. Available from `http://cr.yp.to/papers.html`.

[2] Noah Snyder, *An alternate proof of Mason's theorem*, Elemente der Mathematik **55** (2000), 93–94. ISSN 0013–6018. MR 2001g:11033. Available from `http://www.springerlink.com/openurl.asp?genre=article&issn=0013-6018&volume=55&issue=3&spage=93`.

[3] José Felipe Voloch, *On some subgroups of the multiplicative group of finite rings*. Available from `http://www.ma.utexas.edu/users/voloch/preprint.html`.

Department of Mathematics, Statistics, and Computer Science (M/C 249), The University of Illinois at Chicago, Chicago, IL 60607–7045

E-mail address: `djb@cr.yp.to`