RÉSUMÉ. Agrawal, Kayal, et Saxena ont récemment introduit une nouvelle méthode pour montrer qu’un entier est premier. La vitesse de cette méthode dépend des minorations prouvées pour la taille du semi-groupe multiplicatif engendré par plusieurs polynômes modulo un autre polynôme $h$. Voloch a trouvé une application du théorème ABC de Stothers et Mason dans ce contexte: sous de petites hypothèses, des polynômes distincts $A, B, C$ de degré au plus $1.2 \deg h - 0.2 \deg \rad{ABC}$ ne peuvent pas être tous congrus modulo $h$. Nous présentons deux améliorations de la partie combinatoire de l’argument de Voloch. La première amélioration augmente $1.2 \deg h - 0.2 \deg \rad{ABC}$ en $2 \deg h - \deg \rad{ABC}$. La deuxième amélioration est une généralisation à $A_1, \ldots, A_m$ de degré au plus $((3m-5)/(3m-7)) \deg h - (6/(3m-7)m) \deg \rad{A_1 \cdots A_m}$, avec $m \geq 3$.

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 $1.2 \deg h - 0.2 \deg \rad{ABC}$ 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 $2 \deg h - \deg \rad{ABC}$. The second improvement generalizes to $m \geq 3$ polynomials $A_1, \ldots, A_m$ of degree at most $((3m-5)/(3m-7)) \deg h - (6/(3m-7)m) \deg \rad{A_1 \cdots A_m}$.
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

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

As usual, \( \text{rad} X \) means the largest monic squarefree divisor of \( X \), i.e., the product of the monic irreducibles dividing \( X \). If \( \deg \text{rad} A_1 \cdots A_m < (m/3) \deg h \) then the bound in Theorem 2.3 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 \( \max\{\deg A, \deg B, \deg C\} > 2 \deg h - \deg \text{rad} ABC \). 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 \( \text{rad} ABC = \text{rad} x^{30} = x \) so \( 2 \deg h - \deg \text{rad} ABC = 19 \).

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 \( \max\{\deg A, \deg B, \deg C\} > 1.2 \deg h - 0.2 \deg \text{rad} ABC \). This paper improves Voloch’s result in two ways:

- This paper is quantitatively stronger, in the interesting case that \( \deg \text{rad} ABC < \deg h \).
- This paper applies to larger values of \( m \).

Application. Inside the unit group \( (k[x]/h)^* \) consider the subgroup \( G \) 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

\[
\#G \geq \frac{1}{m - 1} \left( \left\lfloor \frac{(3m - 5)/(3m - 7)}{\deg h - (6/(3m - 7)m)\#S} \right\rfloor + \#S \right)
\]

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

\[
\left( \frac{(3m - 5)/(3m - 7)}{\deg h - (6/(3m - 7)m)\#S} \right);
\]

\( m \) distinct such products cannot all have the same image modulo \( h \).
In particular, if \( \#S = \deg h \), then
\[
\#G \geq \frac{1}{3} \left( \frac{\deg h}{\deg h} \right)^{2.1} \approx 4.2768^{\deg h}.
\]
Compare this to the bound \( \#G \geq \frac{2^{\deg h - 1}}{\deg h} \approx 4^{\deg h} \) 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
\[
\text{max}\{\deg A, \deg B, \deg C\} > 2 \deg h - \deg \text{rad} \ ABC.
\]

**Proof.** Permute \( A, B, C \) so 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 \( \deg \text{rad} \ ABC > 0 \).

If \( \deg A \geq 2 \deg h \) then \( \deg A > 2 \deg h - \deg \text{rad} \ ABC \); 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 \( U A + V B + W C = 0 \). Define \( D = \gcd\{U A, V B, W C\} \).

If \( \deg D = \deg U A \) then \( U A \) divides \( V B, W C \); so \( A \) divides \( V W A, V W B, V W C \); so \( A \) divides \( \gcd\{V W A, V W B, V W C\} = V W \); but \( V W \neq 0 \), so \( \deg A \leq \deg V W \leq 2(\deg A - \deg h) \); so \( \deg A \geq 2 \deg h \); done.

Assume from now on that \( \deg D < \deg U A \) and that \( \deg A \leq 2 \deg h - 1 \). Then \( \deg(U A / D) \) is between 1 and \( 2 \deg A - \deg h \leq 3 \deg h - 2 \); so the derivative of \( U A / D \) is nonzero. Also \( U A / D + V B / D + W C / D = 0 \), and \( \gcd\{U A / D, V B / D, W C / D\} = 1 \). By Theorem 3.1 below, \( \deg(U A / D) < \deg \text{rad}(U A / D)(V B / D)(W C / D) = \deg \text{rad}(U V W A B C / D^3) \).

The proof follows Voloch up to this point. Voloch next observes that \( D \) divides \( \gcd\{U V W A, U V W B, U V W C\} = U V W \gcd\{A, B, C\} = U V W \). I claim that more is true: \( D \gcd(U V W A B C / D^3) \) divides \( U V W \gcd A B C \).

(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 \( d \leq u + v + w \). 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 \( d + [\cdots] \leq u + v + w + 1 \leq u + v + w + [\cdots] \) as claimed. Otherwise \( u + v + w + a + b + c \leq d \leq 3d \) so \( d + [u + v + w + a + b + c > 3d] \leq u + v + w \leq u + v + w + [\cdots] \) as claimed.)

Thus \( \deg U A < \deg(D \gcd(U V W A B C / D^3)) \leq \deg(U V W \gcd A B C) \). Hence \( \deg A < \deg(U V W \gcd A B C) \leq 2(\deg A - \deg h) + \deg \text{rad} \ ABC \); i.e., \( \deg A > 2 \deg h - \deg \text{rad} \ ABC \) 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

$$\max\{\deg A, \deg B, \deg C\}$$

$$> 2 \deg h - \deg \rad A - \deg \rad B - \deg \rad C$$

$$+ \deg \rad \gcd\{A, B\} + \deg \rad \gcd\{A, C\} + \deg \rad \gcd\{B, C\}.$$

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,

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

$$\geq 2 \deg h - \deg \rad ABC.$$  

Furthermore, $\deg G \geq \deg \rad G = \deg \rad \frac{ABC}{A - \deg \rad B - \deg \rad C + \deg \rad \gcd\{A, B\} + \deg \rad \gcd\{A, C\} + \deg \rad \gcd\{B, C\}$ by inclusion-exclusion. Add. \qed

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

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

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

Proof. Define $d = \max\{\deg A : A \in S\}$ and $e = \deg \rad \prod_{A \in S} A$. Then

$$d > 2 \deg h - \deg \rad A - \deg \rad B - \deg \rad C$$

$$+ \deg \rad \gcd\{A, B\} + \deg \rad \gcd\{A, C\} + \deg \rad \gcd\{B, C\}$$

for any distinct $A, B, C \in S$ by Theorem 2.2. Average this inequality over all choices of $A, B, C$ to see that $d > 2 \deg h - 3 \avg_A \deg \rad A + 3 \avg_{A \neq B} \deg \rad \gcd\{A, B\}$. On the other hand, $e \geq \#S \avg_A \deg \rad A - \left(\frac{\#S}{2}\right) \avg_{A \neq B} \deg \rad \gcd\{A, B\}$ by inclusion-exclusion, so

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

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

One can bound each term $\deg \rad \gcd\{A, B\}$ 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 
\[
\deg \rad \gcd\{A, B\} \leq d - \deg h.
\]
Hence
\[
d + \frac{3}{S}e > 2 \deg h - \frac{3 \#S - 9}{2} (d - \deg h);
\]
i.e., \( d > \frac{((3 \#S - 5)/(3 \#S - 7)) \deg h - (6/(3 \#S - 7) \#S)e}{} \).

\[
\Box
\]

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 \( \deg A \geq \deg \rad ABC \) then \( A' = 0 \).

In fact, \( A' = B' = C' = 0 \). As usual, \( X' \) means the derivative of \( X \); the relevance of derivatives is that \( X/\rad X \) 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 \( \gcd\{B, C\} = 1 \).

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

The ratios \( A/\rad A, B/\rad B, C/\rad C \) are pairwise coprime, so their product \( ABC/\rad ABC \) divides \( C' B - C B' \). But by hypothesis

\[
\deg \frac{ABC}{\rad ABC} = \deg ABC - \deg \rad ABC \geq \deg BC > \deg(C' B - C B');
\]
so \( C' B - C B' = 0 \); 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 \( A' = 0 \). \( \Box \)

**References**

