The ABC-conjecture for polynomials

Abhishek Parab

1 Introduction

Masser (1985) and Oesterle (1988) made the ABC conjecture about three relatively prime integers which was observed to have important consequences, like the Fermat's last theorem. It has remained unsolved till date (?) and is often regarded as 'the most important unsolved problem in Diophantine analysis'. Since the rings $\mathbb{Z}$ and $K[X]$ share similar properties, it was asked if the corresponding question was true for $K[X]$, where K is a field. The case when $K = \mathbb{R}$ or $\mathbb{C}$ was solved and is known as the Mason-Stothers theorem. In what follows, we shall study the proof of the theorem and its connection to Belyi maps.

Question 1.1 (The "actual" ABC Conjecture) *Let $a, b, c \in \mathbb{N}$ be relatively prime and*

$$a + b = c.$$

Let d denote the product of prime factors of abc. Then, "usually", $c < d$. More precisely, for every $\varepsilon > 0$, there exist at most finitely many $(a, b, c) \in \mathbb{N}^3$ such that

$$c > d^{1+\varepsilon}.$$

Theorem 1.2 (Mason-Stothers theorem) *Let K be an algebraically closed field of characteristic zero. Let $e, f, g \in K[X]$ be relatively prime polynomials satisfying*

$$e(X) + f(X) = g(X).$$

Then,

$$h \leq \deg \operatorname{rad}(efg) - 1$$

where $h = \max\{\deg e, \deg f, \deg g\}$. Moreover, equality occurs precisely when f/g is a Belyi map.

Before understanding Belyi maps, let us go over some basic theory of algebraic curves.

2 A review of algebraic curves

Definition 2.1 *Curve: Projective variety of dimension one.*

Here is some connection between geometry and algebra:

$$\text{Curve} \leftrightsquigarrow \text{field (its function field)}$$
$$\text{Maps between curves} \leftrightsquigarrow \text{field inclusions}$$
$$\phi : C_1 \to C_2 \leftrightsquigarrow \phi^* : K(C_2) \to \phi^*(K(C_1))$$

Definition 2.2 *Non-singular curve: A curve C is nonsingular at a point P if the ring of regular functions around P, viz., $K[C]_P$ is a regular local ring. It is nonsingular if it is nonsingular at every point.*

Let $\phi : C_1 \to C_2$ is a map of nonsingular curves.

Definition 2.3 *Ramification index: The ramification index at a point $P \in C_1$ (denoted by $e_\phi(P)$) is the number* $\mathrm{ord}_P\, \phi^*(t)$ *where $\phi^* : K[C_2]_{\phi(P)} \to K[C_1]_P$ is the map of local rings and t is the uniformizing parameter at $\phi(P)$.*

Definition 2.4 *Degree of ϕ: It is the degree of the field extension $[\phi^*(K(C_1)) : K(C_2)]$.*

Definition 2.5 *Branch point: A point $P \in C_1$ is a ramification point or a branch point if $e_\phi(P) > 1$.*

Theorem 2.6 (Riemann Hurwitz formula) *Let $\phi : C_1 \to C_2$ be a non-constant separable map of smooth curves of genera g_1 and g_2 respectively. Then,*

$$2g_1 - 2 \geq (\deg \phi)(2g_2 - 2) + \sum_{P \in \mathbb{C}_1} e_\phi(P) - 1.$$

Further, equality occurs in fields of characteristic zero.

Definition 2.7 *Belyi map: Let X be a curve. If $\phi : X \to \mathbb{P}^1$ is a map of curves such that*

$$\textit{Branch Locus } (\phi) \subseteq \{0, 1, \infty\}$$

then ϕ is said to be a Belyi map.

Remark Using the Mobius transformations, one may choose any three branch points but its customary to take them to be $\{0, 1, \infty\}$.

Theorem 2.8 (Belyi's theorem, 1979) *Let X be a connected nonsingular curve. Then the following are equivalent:*

1. *X is defined over $\overline{\mathbb{Q}}$,*
2. *There exists a Belyi map $\phi : X \to \mathbb{P}^1_{\mathbb{C}}$.*

Remark The converse (2) $\Rightarrow$ (1) is due to Weil [1956].

3 Proof of ABC for polynomials

Theorem 3.1 (Mason-Stothers) *Let K be an algebraically closed field of characteristic zero. Let $e, f, g \in K[X]$ be relatively prime polynomials and*

$$e(X) + f(X) = g(X).$$

Then,

$$h \leq \mathrm{rad}(efg) - 1$$

where $h = \max\{\deg e, \deg f, \deg g\}$.

Further, equality occurs above precisely when f/g is a Belyi map for $\mathbb{P}^1$ and $f/g(\infty) \in \{0, 1, \infty\}$.

Proof Set $\phi = f/g$. Then $\deg \phi = [K(X) : K(f/g)] = h$. Since at least two of e, f, g must have the same degree, we may assume that $\deg e = \deg f = h$. Depending on whether $\deg g = h$ or $\deg g < h$, we have the two cases viz., $\phi(\infty) \neq \infty$ and $\phi(\infty) = \infty$ respectively.

We apply the Riemann-Hurwitz formula for $\phi = f/g : \mathbb{P}^1 \to \mathbb{P}^1$:

$$2g_1 - 2 \geq (\deg \phi)(2g_2 - 2) + \sum_{P \in \mathbb{C}_1} e_\phi(P) - 1.$$

Since equality holds over characteristic zero and the genus of $\mathbb{P}^1$ is zero, this simplifies to

$$-2 = -2h + \sum_{x\in\mathbb{P}^1}(e_\phi(x) - 1).$$

The last sum is finite because all but finitely many points are unramified so $e_\phi(x) = 1$ for almost all $x \in \mathbb{P}^1$. We split this sum as R_0, R_1, R_∞, R where

$$R_0 = \sum_{x \mapsto 0}\left(e_\phi(x) - 1\right),$$

and similarly R_1, R_∞. R would then be the sum over the remaining points of $\mathbb{P}^1$.

$$R_1 = \sum_{x\mapsto 1}\left(e_\phi(x) - 1\right) = \sum_{x\mapsto 1} e_\phi(x) - |\phi^{-1}(1)|.$$

Notice that $\phi(x) = 1$ precisely when $\dfrac{f(x)}{g(x)} = 1$, i.e., when $e(x) = 0$. Thus points $x \in \mathbb{P}^1$ with $\phi(x) = 1$ correspond to roots of $e(x)$. That gives

$$\begin{aligned}R_1 &= \deg e - \deg \operatorname{rad}(e)\\ &= h - \deg \operatorname{rad}(e).\end{aligned}$$

Similarly, if $\phi(x) = 0$ then either $f(x) = 0$ or $g(x) = \infty$. The latter corresponds to $x = \infty$. But

$$\phi(\infty) = \begin{cases}\infty & \text{if } \deg g < h\\ \text{unit} & \text{if } \deg g = h,\end{cases}$$

so that possibility can be ruled out. Thus,

$$\begin{aligned}R_0 &= \sum_{x \mapsto 0}\left(e_\phi(x) - 1\right)\\ &= \sum_{x \mapsto 0} e_\phi(x) - |\phi^{-1}(0)|\\ &= \deg f - \deg \operatorname{rad}(f)\\ &= h - \deg \operatorname{rad}(f).\end{aligned}$$

Finally, if $\phi(x) = \infty$ then either $g = 0$ or $x = \infty$. If $\deg g = h$ then $\phi(\infty) \neq \infty$ so

$$\begin{aligned}R_\infty &= \deg g - \deg \operatorname{rad} g\\ &= h - \deg \operatorname{rad} g.\end{aligned}$$

If $\deg g < h$ then $\phi(\infty) = \infty$ so we have

$$\begin{aligned}R_\infty &= \deg g - (\deg \operatorname{rad}(g) + 1)\\ &= h - \deg \operatorname{rad}(g) - 1.\end{aligned}$$

The extra contribution of 1 comes from $x = \infty$ viz., $\phi^{-1}(\infty) = \deg \operatorname{rad}(g) + 1$.

Substituting these expressions in the Riemann-Hurwitz formula gives

$$-2 = \begin{cases}h - \deg \operatorname{rad}(e) - \deg \operatorname{rad}(f) - \deg \operatorname{rad}(g) + R & \text{if } \deg g = h\\ h - \deg \operatorname{rad}(e) - \deg \operatorname{rad}(f) - \deg \operatorname{rad}(g) + R - 1 & \text{if } \deg g < h.\end{cases}$$

But e, f, g were assumed to be coprime so $\operatorname{rad}(efg) = \operatorname{rad}(e).\operatorname{rad}(f).\operatorname{rad}(g)$. This gives

$$R = \begin{cases}h - \deg \operatorname{rad}(efg) - 2 & \text{if } \deg g = h\\ h - \deg \operatorname{rad}(efg) - 1 & \text{if } \deg g < h.\end{cases}$$

In either of the cases, using $R \geq 0$ gives

$$h \geq \deg \operatorname{rad}(efg) + 1$$

as required. Further, equality occurs precisely when $\deg g < h$ and $R = 0$. Now $\deg g < h$ means that $\phi(\infty) = \infty$ and $R = 0$ means that ϕ is a Belyi map, as required. This ends the proof. ∎