ON SOME POLYNOMIALS ALLEGEDLY RELATED TO THE ABC CONJECTURE

ALEXANDR BORISOV

1. Introduction

The main goal of this paper is to bring your attention to the following family of polynomials.

Definition 1.1. *For every $a = b + c$, where a, b, c are coprime natural numbers the abc-polynomial*

$$f_{abc}(x) = \frac{bx^a - ax^b + c}{(x-1)^2}.$$

I discovered these polynomials when pursuing a rather naive approach to the Masser-Oesterlé's *abc* conjecture. The following argument describes the idea. It's extremely vague and I would be very happy to hear any comments on how to make it more precise or why it is doomed to fail.

Argument. Although the arithmetic *abc* conjecture is a great mystery, its algebraic counterpart is a rather easy theorem. It looks like it was first noticed by W. W. Stothers (cf [21]). Later on it was generalized and rediscovered independently by several people, including R.C. Mason (cf. [12]) and J. Silverman (cf. [19]). This list might be incomplete and I would appreciate any amendments to it.

Theorem. *Suppose $a + b + c = 0$, where a, b, c are coprime, not all constant, polynomials with coefficients in a field K,* $\mathrm{char}K = 0$. *Suppose $R(x) \in K[x]$ is the product of all irreducible monic polynomials from $K[x]$ that divide abc. Then*

$$\deg R \geq \max(\deg a, \deg b, \deg c) + 1.$$

There are several proofs of this theorem, all involving derivatives or differential forms. I will discuss two of them, probably the easiest ones and then try to translate them into the arithmetical setting.

Date: October 23, 1997.

Proof 1. (Oesterlé, cf. [14], Thm 2) Let's differentiate the equality $a(x)+b(x)+c(x)=0$ with respect to x. Then we get two equalities.

$$\begin{cases} a+b+c=0 \\ a'+b'+c'=0 \end{cases}$$

Together they imply that

$$\begin{vmatrix} a & b \\ a' & b' \end{vmatrix} = \begin{vmatrix} b & c \\ b' & c' \end{vmatrix} = \begin{vmatrix} c & a \\ c' & a' \end{vmatrix}$$

If we denote the above determinant by $D(x)$, then we have the following.

1) If $D(x)=0$, this would imply that $ab'=a'b$, so $a|a'b$, so $a|a'$, so $a'=0$ (because $\deg a' < \deg a$.) Therefore, because $\mathrm{char}K=0$, $a(x)$ is a constant. As the same can be done for b and c and because we assumed that a, b, c are not all constants, we conclude that $D(x)\neq 0$.

2) If, say, $\deg a = \deg b = n \geq m = \deg c$, then

$$\deg D \leq \deg(bc'-cb') \leq n+m-1.$$

3) Suppose $p \in K[x]$ is a monic irreducible divisor of $a(x)$. Suppose k is the biggest integer such that $p^k|a$. Then $p^{k-1}|a'$, so $p^{k-1}|D$. Considering this for all $p|abc$, we get that $\frac{abc}{R}|D$. Therefore

$$n+n+m-\deg R \leq \deg D \leq n+m-1,$$

so $\deg R \geq n+1$, the theorem is proven.

Remark 1.1. One can generalize the above theorem (with some extra condition imposed) and the above proof to $\mathrm{char}K>0$.

Proof 2.(Stothers [21], Mason [12], Silverman [19])

First of all, we may assume that K is algebraically closed. Suppose as before that $\deg a = \deg b = n \geq m = \deg c$. Consider the map $\varphi : P^1 \to P^1$ given by $\frac{a(x)}{c(x)}$. It has degree n. The total number of points in $\varphi^{-1}(\{o,-1,-\infty\})$ is $\deg R$ or $\deg R+1$ (if $m<n$.) Therefore if D is the ramification divisor of φ (i.e. $K_{P^1} = \varphi^* K_{P^1} + D$) then $\deg D \geq 3n - (\deg R + 1)$.

On the other hand, $\deg D = 2(n-1)$ by the Hurwitz theorem. Therefore

$$3n - \deg R - 1 \leq 2n-2,$$

so $\deg R \geq n+1$, the theorem is proven.

Remark 1.2. The above proof can also be generalized to $\mathrm{char}K>0$ with the assumption that φ is separable. Also, the first P^1 can be replaced by any other fixed curve, which means that one can prove a similar result for a, b, c in any finite extension of $K[x]$. (cf. [12].)

What we did above was 100% rigorous, here comes the vague part of the argument.

Both of the above proofs are hard to follow in the arithmetic case. The reason is that there is no such map φ and no non-zero differentiation. This is related to the fact that the set of integers is naturally discrete so they don't have any non-trivial deformations. However, the integers have QUANTUM deformations: for any positive integer a, one denotes $[a]_q = q^{a-1} + \ldots + q + 1$ where q is quantum parameter. Other people call the same thing $q-$expansion. The classical integers are obtained by specializing q to 1.

Let's try therefore to "quantize" the abc conjecture. In order to deal with positive integers we will rewrite $a + b + c = 0$ as $a = b + c$, with a, b, c positive, possibly switching a, b, and c and changing some signs. The equality $a = b + c$ can then be quantized as $[a]_q = [b]_q + [c]_q \cdot q^b$.

Another way to go is $[a]_q = [b]_q \cdot q^c + [c]_q$. They yield basically the same. Unfortunately, the extra q-factor can not be avoided.

Following Proof 1, consider

$$D = \begin{vmatrix} b & a \\ [b]_q & [a]_q \end{vmatrix} = \frac{b(q^a-1) - a(q^b-1)}{q-1} = \frac{bq^a - aq^b + c}{q-1}.$$

Then D is obviously divisible by $q-1$, which is actually something similar to the geometric case, because there we didn't just deform, but actually differentiated. And if we deformed, i.e. considered $a(x+\varepsilon)$ etc., we would have had to divide by ε at some point. So $\frac{D(q)}{q-1}$ corresponds somehow to the determinant in the Proof 1. Note now that this is exactly the abc-polynomial $f_{abc}(q)$.

This abc-polynomial also arises if one tries to follow Proof 2 as a non-trivial factor of the derivative of $\frac{[a]_q}{[c]_q}$:

$$\left(\frac{[a]_q}{[c]_q}\right)' = \frac{q^{c-1}}{[c]_q^2}\left(\frac{bq^a - aq^b + c}{(q-1)^2}\right).$$

So this is how these polynomials appear. The exact comparison with the geometric case is definitely lost at this point. However the abc-polynomials do satisfy some really nice properties.

First of all, it looks like they are always irreducible. This question is naturally invariant under the switch of b and c because $f_{abc}(x)$ is reciprocal to $f_{acb}(x)$. In the case when it is irreducible, it is natural to call the corresponding field the abc-field . It only depends on the triple $a = b + c$ and not on the order of b and c. It has degree $a - 2$ and is

unramified outside of abc, which follows from the direct calculation of the discriminant of $f_{abc}(x)$ (Lemma 2.1.)

Although the author has no knowledge of any previous investigations on abc-polynomials in the general case, the particular case $c = 1$ (or $b = 1$) was studied before. First of all, Schinzel and Nicolas studied the distribution of roots of $f_{n,1,(n-1)}(x) = \frac{x^n - nx + (n-1)}{(x-1)^2}$ in the complex plane and obtained some remarkably precise results on it (cf. [13]).

Also, M. Filaseta conjectured that $f_{(n+1),n,1}(x) = (x^n + x^{n-1} + ... + x + 1)'$ is always irreducible. He proved it for n being prime power (cf. Theorem 3.1). T.Y. Lam conjectured that all the higher derivatives $(x^n + x^{n-1} + ... + x + 1)^{(k)}$ are also irreducible. Using the methods of this paper (with some significant modifications) for any fixed k one can prove the irreducibility for almost all (in the sense of density) n. These results will appear elsewhere in a joint paper with Filaseta and Lam. In this paper we prove that $f_{abc}(x)$ are irreducible for the density one set of coprime triples ($a = b + c$). We also prove the same result for any fixed b. And for "good" b that is if there is a prime p, such that $p||b$, we prove that all but finitely many abc-polynomials are irreducible. To be more precise, it suffices to assume that $c \gg b \ln b$.

I should mention here that the irreducibility results of this paper can be viewed as a part of a more general problem of irreducibility of the kernels of trinomials. It was extensively studied by Schinzel (cf. [16].) From the older results on this topic I should mention that of Selmer (cf. [18]).

The paper is organized as follows. Section 2 contains the results about the distribution of roots of abc-polynomials in usual and $p-$adic complex numbers. The key Section 3 is devoted to the irreducibility results which rely heavily on the results of Section 2. Section 4 contains some miscellaneous remarks and heuristics that I have gathered in the unsuccessful attempt to link the abc-polynomials closer to the abc conjecture from which they originated.

Notations. Throughout the paper if we write $g(x)|f_{abc}(x)$ we assume that $g \in \mathbb{Z}[x]$ and $\frac{f_{abc}(x)}{g(x)} \in \mathbb{Z}[x]$. All signs " $\gg$ " and " $\ll$ " assume absolute constants unless specified otherwise. The notation $m||n$ means, as usual, that $m|n$ and $\gcd(m, \frac{n}{m}) = 1$.

Acknowledgments. I am taking this opportunity to thank my Penn State adviser Yuri Zarhin for his interest and support of this research in its embryonic stage. I also thank A. Schinzel for the reference to Filaseta and Lam's work. I am especially thankful to M. Filaseta whose numerous helpful comments and interest in this study helped me push it a lot farther than what I originally thought possible. In

particular, Lemma 3.1 for $k > 1$ and the current version of Theorem 3.7 are due to him.

2. Distribution of Roots

First of all, let's calculate the discriminant of the abc-polynomial.

Lemma 2.1. *The discriminant of $f_{abc}(x)$ is equal to $2a^{a-3}b^{a-4}c^{a-4}$.*

Proof. First of all, $f_{abc}(1) = \frac{1}{2} \cdot \big(bx^a - ax^b + c\big)''(1) = \frac{abc}{2}$. Denote by (u, v) the resultant of polynomials u and v. Then the discriminant of $f_{abc}(x)$ is calculated as follows.

$$\frac{1}{b}(f, f') = \frac{1}{b}\Big(\frac{bx^a - ax^b + c}{(x-1)^2}, \frac{abx^{b-1}(x^c-1)(x-1) - 2(bx^a - ax^b + c)}{(x-1)^3}\Big) =$$

$$= \frac{1}{b}\Big(\frac{bx^a - ax^b + c}{(x-1)^2}, \frac{abx^{b-1}(x^c-1)(x-1) - 2(bx^a - ax^b + c)}{(x-1)^2}\Big)\frac{2}{abc} =$$

$$= \frac{1}{b}\Big(\frac{bx^a - ax^b + c}{(x-1)^2}, \frac{abx^{b-1}(x^c-1)}{(x-1)}\Big)\frac{2}{abc} =$$

$$= \frac{2}{a^2c}\Big(\frac{b(x^c-1)x^b - c(x^b-1)}{(x-1)^2}, \frac{(x^c-1)}{(x-1)}\Big)c^{b-1} \cdot (ab)^{a-2} =$$

$$= \frac{2}{ab^2c}c^{b-1} \cdot (ab)^{a-2}\Big(\frac{b(x^c-1)x^b}{(x-1)} - c\frac{(x^b-1)}{(x-1)}, \frac{(x^c-1)}{(x-1)}\Big)\frac{1}{c} =$$

$$= 2a^{a-3}b^{a-4}c^{b-3} \cdot \Big(c\frac{(x^b-1)}{(x-1)}, \frac{(x^c-1)}{(x-1)} =$$

$$= 2a^{a-3}b^{a-4}c^{b-3}c^{c-1} = 2a^{a-3}b^{a-3}c^{a-4}.$$

Remark 2.1. The Mahler measure M of $f_{abc}(x)$ is at most $2a$, which can be shown by applying Mahler's result [10] to the corresponding trinomial. Therefore the Mahler's estimate for the discriminant (cf. [11]) implies that $D(f_{abc}(x)) \leq (a-2)^{a-2} \cdot (2a)^{2a-6}$ which is of about the same magnitude as the exact value, especially if b is about the same as c. This means that the roots are more or less uniformly distributed around the unit circle. In Theorem 2.1 we make it much more precise using the result of P. Erdős and P. Turán. (cf. [5]).

Let's prove now that $f_{abc}(x)$ is the kernel of the corresponding trinomial (i.e. it has no roots on the unit circle.)

Lemma 2.2. *1) If $bx^a - ax^b + c = 0$ and $|x| = 1$, then $x = 1$.*
2) $f_{abc}(1) = \frac{abc}{2}$.

Proof. 1) If $|x| = 1$ then $|bx^a| = b$, $|ax^b| = a$, $|c| = c$. So in order for x to be the root the above three numbers have to lie on the same ray. So x^b and x^a have to be 1. This implies that $x = 1$ because $\gcd(a, b) = 1$.

2) We actually proved it in the beginning of Lemma 2.1.

Remark 2.2. For any $a = b + c$ with $\gcd(a, b, c) = d$ the same argument as above show that $\frac{bx^a - ax^b + c}{(x^d-1)^2}$ is the kernel of the corresponding trinomial. Probably these polynomials also deserve to be studied.

Lemma 2.3. *For $a = b + c$, coprime, $f_{abc}(x)$ has exactly $b - 1$ roots inside and $c - 1$ outside of the unit circle.*

Proof. Instead of $f_{abc}(x)$ it's easier to consider the trinomial $bx^a - ax^b + c$ itself. It has besides the roots of $f_{abc}(x)$ the double root at 1. If we deform c by a very small *negative* real number, $(-\varepsilon)$, then the polynomial $g_\varepsilon(x) = bx^a - ax^b + (c - \varepsilon)$ will have simple roots close to the roots of $f_{abc}(x)$ as well as two simple real roots near 1, one less and one bigger than 1. This follows from the fact that

$$bx^a - ax^b + c - \varepsilon = -\varepsilon + \frac{abc}{2}(x - 1)^2 + O(x - 1)^3$$

when $x \to 1$. As a result, for ε small enough the number of roots of $g_\varepsilon(x)$ inside of the unit circle is exactly one plus the number of roots of $f_{abc}(x)$ in there. Let's notice now that when $|x| = 1$, then

$$|ax^b| = a = b + c > b + c - \varepsilon = |bx^a| + |c - \varepsilon| \geq |bx^a + c - \varepsilon|.$$

So, when x makes one revolution around 0 on the unit circle, ax^b makes b revolutions and so does $g_\varepsilon(x)$.

Therefore, $g_\varepsilon(x)$ has b roots inside of the unit circle, and $f_{abc}(x)$ has $b-1$. The remaining $c-1$ roots of $f_{abc}(x)$ are outside of the unit circle.

Lemma 2.4. *If a is even then $f_{abc}(x)$ has no real roots. If a is odd it has exactly one real root which is always negative.*

Proof. If a is even, then b and c are odd (since a, b, and c are pairwise coprime) and Descartes' Rule of Signs implies that the polynomial $bx^a - ax^b + c$ has at most and, hence, exactly two positive real roots corresponding to the two roots at 1, and no negative real roots. Similarly, if a is odd, then Descartes' Rule of Signs implies that $bx^a - ax^b + c$ has the two positive roots at 1 and no other positive roots and exactly one negative real root. The lemma follows.

The following lemma is a trivial observation that will be needed in Theorem 3.7.

Lemma 2.5. *If $a \geq 4$ then for every root $x = re^{i\varphi}$ of $f_{abc}(x)$ we have $r = |x| < 2$.*

Proof. First of all, if $f_{abc}(x) = 0$ then

$$bx^a - ax^b + c = 0,$$

so

$$x^c = \frac{a}{b} - \frac{c}{bx^b}.$$

If $r > 1$ then

$$r^c \leq \frac{a}{b} + \frac{c}{b} = 1 + \frac{2c}{b}.$$

If $c < b$ then we estimate $r < 1 + \frac{2}{b}$, as

$$\big(1 + \frac{2}{b}\big)^c = 1 + \frac{2c}{b} + R,$$

where the remainder term R is obviously positive. In this case, because $b > \frac{a}{2}$, $r < 1 + \frac{4}{a} \leq 2$.

If $c > b$, then we estimate

$$r \leq \big(1 + \frac{2c}{b}\big)^{\frac{1}{c}} \leq \big(2c + 1\big)^{\frac{1}{c}} < 2$$

because $c \geq 3$ for $a \geq 4$.

Lemma 2.6. *For every $\varepsilon > 0$ there exists some positive constant $A(\varepsilon)$, such that for every $x = re^{i\varphi}$, which is a root of $f_{abc}(x)$, its absolute value r satisfies the inequality $|r - 1| < (1 + \varepsilon) \cdot \frac{2}{a} \ln(2a)$ if $a \geq A(\varepsilon)$.*

Proof. It's clearly enough to prove the upper bound due to the symmetry of the problem. We proceed as in the previous lemma, so we get

$$r \leq \big(1 + \frac{2c}{b}\big)^{\frac{1}{c}}.$$

If $c < b$ the bound is even better than what we need.

If $c > b$, $r \leq \big(1 + \frac{2c}{b}\big)^{\frac{1}{c}}$ implies

$$\ln r \leq \frac{1}{c} \ln\big(1 + \frac{2c}{b}\big) \leq \frac{1}{c} \ln(2c + 1).$$

So if $c \gg 1$ ("$\gg$" depends on ε) we have

$$r < 1 + (1 + \frac{\varepsilon}{3}) \cdot \frac{1}{c} \ln(2c + 1) < 1 + (1 + \frac{\varepsilon}{2}) \cdot \frac{1}{c} \ln(2c),$$

So if $a \gg 1$ ("$\gg$" depends on ε) then

$$r < 1 + (1 + \varepsilon) \cdot \frac{2}{a} \ln(2a),$$

which proves the lemma.

The following result is due to P. Erdős and P. Turán.

Theorem. (P. Erdős – P. Turán, [5]) *Suppose the roots of the polynomial* $f(x) = a_n x^n + ... + a_1 x + a_0$ *are denoted by* $x_k = r_k e^{i\varphi_k}$, $k = 1, 2, ..., n$.
For every $0 \le \varphi \le \psi \le 2\pi$ *denote by* $N_f(\varphi, \psi)$ *the number of* x_k *such that* $\varphi \le \varphi_k \le \psi$. *Then*

$$\left|N_f(\varphi,\psi) - \frac{\psi-\varphi}{2\pi}n\right| < 16\sqrt{n \ln \frac{|a_0| + |a_1| + ... + |a_n|}{\sqrt{|a_0 a_n|}}}.$$

Remark 2.3. Instead of the Erdős-Turán theorem one can also use a somewhat similar result of Bilu ([2]), which in the case of $abc-$polynomials gives a little bit worse and ineffective bound.

Now we apply the above theorem to $f_{abc}(x)$.

Theorem 2.1. *In the above notations for any* φ, ψ

$$\left|N_{f_{abc}}(\varphi,\psi) - \frac{\psi-\varphi}{2\pi}n\right| \le 12\sqrt{n \ln(n+1)},$$

where $n = a - 2 = \deg f_{abc}(x)$.

Proof. By the Erdős-Turán theorem applied to $bx^a - ax^b + c$ we have

$$\left|N_{f_{abc}}(\varphi,\psi) - \frac{\psi-\varphi}{2\pi}n\right| \le \left|N_{bx^a - ax^b + c}(\varphi,\psi) - \frac{\psi-\varphi}{2\pi}(n+2)\right| + 2 <$$

$$< 16\sqrt{n \ln \frac{2a}{\sqrt{a-1}}} + 2.$$

One can easily check that, say, for $n \ge 100$

$$16\sqrt{n \ln \frac{2a}{\sqrt{a-1}}} + 2 < 12\sqrt{n \ln(n+1)},$$

when $a = n + 2$. And for $n < 100$ the theorem is true anyway because $12\sqrt{n \ln(n+1)} > n$.

Remark 2.4. In the case $b = 1$ there is a much more precise result of Schinzel and Nicolas (cf. [13]). It would be very interesting to extend it to the general case.

Let's consider now the distribution of roots of $f_{abc}(x)$ in $p-$adic complex fields for $p|abc$. First of all, let's decompose $f_{abc}(x)$ modulo primes that divide either a, b, or c.

Lemma 2.7. *1) For every $p|a$*

$$f_{abc}(x) \equiv b\Big(\frac{x^{a_1}-1}{x-1}\Big)^q \cdot (x-1)^{q-2} \mod p,$$

where $q = p^k$ is the maximum power of p dividing a and $a_1 = \frac{a}{q}$.

2) For every $p|b$

$$f_{abc}(x) \equiv -c\Big(\frac{x^{b_1}-1}{x-1}\Big)^q \cdot (x-1)^{q-2} \mod p,$$

where, similar to above, $q = p^k, \quad b = qb_1, \quad (b_1, p) = 1$.

3) For every $p|c$

$$f_{abc}(x) \equiv bx^b\Big(\frac{x^{c_1}-1}{x-1}\Big)^q \cdot (x-1)^{q-2} \mod p,$$

where $q = p^k, \quad c = qc_1, \quad (c_1, p) = 1$.

Proof. The proofs of all three statements are straightforward. Let's prove just one of them, say (3). The $A \equiv B$ below means that $A - B = p \cdot U(x)$, where $U(x)$ is a rational function with integer coefficients and monic denominator.

$$f_{abc}(x) = \frac{bx^a - ax^b + c}{(x-1)^2} \equiv \frac{bx^a - ax^b}{(x-1)^2} \equiv bx^b \frac{x^c - 1}{(x-1)^2} =$$

$$= bx^b \cdot \frac{x^{c_1 q} - 1}{(x^q - 1)} \cdot \frac{x^q - 1}{(x-1)^2} \equiv bx^b \cdot \Big(\frac{x^{c_1}-1}{x-1}\Big)^q \cdot (x-1)^{q-2}.$$

This proves the desired formula.

Because of the above decomposition, it's very natural to consider the roots in p-adic complex field as coming in clusters around the a_1-th (or b_1-th, c_1-th) roots of unity and 0 (for $p|c$) and "∞" (for $p|b$). The $p-$adic distance between the above roots of unity is obviously equal to 1, so the clusters don't have common roots.

Lemma 2.8. *Suppose $p|a, \quad a = qa_1, \quad (p, a_1) = 1, \quad q = p^k$. Suppose we fix a p-adic complex field with valuation v, $v(p) = 1$. Then for every $\zeta \neq 1, \quad \zeta^{a_1} = 1$, we have exactly p roots x_i of $f_{abc}(x)$ with $v(x_i - \zeta) = \frac{1}{p}$, exactly $p^2 - p$ roots with $v(x_i - \zeta) = \frac{1}{p^2 - p}$, exactly $p^3 - p^2$ roots with $v(x_i - \zeta) = \frac{1}{p^3 - p^2}$, and so on, until exactly $p^k - p^{k-1}$ roots with $v(x_i - \zeta) = \frac{1}{p^k - p^{k-1}}$.*

Proof. The roots of $f_{abc}(x)$ that are inside of the unit ball with the center $\zeta \neq 1$, $\zeta^{a_1} = 1$, are the roots of $bx^a - ax^b + c$, because $v(\zeta - 1) = 0$. Consider the polynomial $g(x) = b(\zeta + x)^a - a(\zeta + x)^b + c$. Its roots are exactly the differences between roots of $f_{abc}(x)$ and ζ.

$$g(x) = (b\zeta^a - a\zeta^b + c) + \sum_{j=1}^{a} x^j \big[b\binom{a}{j}\zeta^{a-j} - a\binom{b}{j}\zeta^{b-j} \big]$$

So

$$g(x) = a(1 - \zeta^b) + \sum_{j=1}^{a} x^j \big[b\binom{a}{j}\zeta^{a-j} - a\binom{b}{j}\zeta^{b-j} \big]$$

So, if $g(x) = u_0 + u_1 x + u_2 x^2 + \cdots + u_a x^a$, then $v(u_0) = k$.

For $1 \leq j \leq a$ if $v(u_j) < k$ or $v\big(\binom{a}{j}\big) < k$ then $v(u_j) = v\big(\binom{a}{j}\big)$

It's a standard and easy to check fact that

$v\big(\binom{a}{j}\big) = v\big(\frac{a}{j}\big)$ for $1 \leq j \leq p^k$.

So, for any $0 \leq n < k$ the least j such that $v(u_j) \leq n$ is $j = p^{k-n}$.

Combined with the Newton Polygon method (cf. N. Koblitz, [9], Chapter 4) this proves the lemma.

Lemma 2.9. *Suppose $p|a$, $a = p^k a_1$, $(a_1, p) = 1$. Then there are exactly $p - 2$ roots x_i of $f_{abc}(x)$ with $v(x_i - 1) = \frac{1}{p-2}$ (no such roots if $p = 2$), also exactly $p^2 - p$ roots with $v(x_i - 1) = \frac{1}{p^2-p}, \ldots$ exactly $p^k - p^{k-1}$ roots with $v(x_i - 1) = \frac{1}{p^k - p^{k-1}}$.*

Proof. Similar to the lemma above, consider

$$g(x) = f_{abc}(1+x) = \frac{b(1+x)^a - a(1+x)^b + c}{x^2} = \sum_{j=2}^{a} x^{j-2} \big[b\binom{a}{j} - a\binom{b}{j} \big]$$

If $g(x) = u_0 + u_1 x + u_2 x^2 + \cdots + u_{a-2} x^{a-2}$, then for $1 \leq j \leq p^k - 2$

$$v(u_j) = v\big(b\binom{a}{j+2}\big) = v(\frac{a}{j+2}),$$

whenever at least one (consequently all) of the above three numbers is less than k.

Notice also that $v(u_0) = k$ if $p \neq 2$ and $v(u_0) = k - 1$ if $p = 2$.

The rest of the proof is absolutely similar to that of the above lemma.

Lemma 2.10. *Suppose $p|c$, $c = p^k c_1$, $(c_1, p) = 1$. Then there are exactly b roots x_i of $f_{abc}(x)$ such that $v(x_i) = \frac{k}{b}$. The remaining $c - 2$ roots are located in clusters around c_1-th roots of unity, exactly as for $p|a$.*

Proof. When we look for x_i, such that $v(x_i) > 0$ it's enough to consider $g(x) = bx^a - ax^b + c$.

We have $v(c) = k$, $v(a) = 0$, and the first statement follows easily from the Newton Polygon method. The proof of the second one is completely parallel to the two lemmas above and is omitted for brevity.

Lemma 2.11. *Suppose $p|b$, $b = p^k b_1$, $(b_1, p) = 1$. Then there are exactly c roots with $v(x_i) = -\frac{k}{c}$. The remaining $b-2$ roots are located in the same way as for $p|a$.*

Proof. Let's just recall that the roots of f_{abc} are reciprocal to the roots of f_{acb}. Then everything follows from the previous lemma.

Remark 2.5. One can make some more precise statements regarding the distribution of x_i in p-adic complex numbers. For instance, if one looks at the roots not from ζ, but from any $a-$th ($b-$th, $c-$th) root of unity, or one of x_i-s, the picture will be about the same. I don't want to go into the details because I haven't found any applications for it yet.

3. Irreducibility results.

We start with some relatively simple irreducibility results and proceed gradually to the harder and stronger ones.

Theorem 3.1. *Suppose $c = 1$ and $b = p^k$, where p is a prime. Then $f_{abc}(x)$ is irreducible.*

Proof. In p-adic complex plane there is just one root x_i of $f_{abc}(x)$ with $v(x) < 0$. For all the rest $v(x) = 0$. So if $f_{abc}(x) = g_1(x) \cdot g_2(x)$ then one of g_i, say g_1, has the leading coefficient ± 1. But this is impossible as all the roots lie strictly inside of the unit circle (Lemma 2.3).

Remark 3.1. This result is due to M. Filaseta. Together with the first part of the next theorem is probably all that was known about the irreducibility of *abc*-polynomials prior to this paper. It is interesting that I don't know how to generalize it to the arbitrary c because the methods of this paper work well only if a, b, and c are not too far from being square-free.

Theorem 3.2. *For any $a = b + c$, coprime, $f_{abc}(x)$ is irreducible if $a = p$ or $a = 2p$, where p is an odd prime.*

Proof. If $a = p$ then $f_{abc}(1 + x)$ is Eisenstein, so we are left with the case $a = 2p$. In p-adic complex plane, we have p roots x_i of $f_{abc}(x)$ with $v(x_i + 1) = \frac{1}{p}$ and $p - 2$ roots x_i of $f_{abc}(x)$ with $v(x_i - 1) = \frac{1}{p-2}$. If $f(x) = g(x) \cdot h(x)$ then, obviously, one of the polynomials g, h has to

contain all roots from one cluster and one has to contain all roots from another one. This implies that, say, $\deg g = p,\ \deg h = p-2$. But by Lemma 2.4 for even a $f_{abc}(x)$ has no real roots. So $\deg g,\ \deg h$ have to be even, contradiction.

Theorem 3.3. *For any $a = b + c$, coprime, the abc-polynomial is irreducible if $a = pl$, where p and l are distinct primes and the order of p in $(\mathbb{Z}/l\mathbb{Z})^*$ doesn't divide the number N, which is the integer from 1 to l defined by the property $N \equiv -\frac{2}{p} \mod l$.*

Proof. Consider the roots of $f_{abc}(x)$ in p-adic complex field. They come in clusters around l-th roots of unity ζ_l. If $\zeta_l \neq 1$ then there are exactly p roots around it, on equal distance, $v(x_i - \zeta) = \frac{1}{p}$. If $f_{abc}(x) = g(x)h(x),\ g,\ h$ are with integer coefficients, then $v(g(\zeta_l))$ is integer, because p is unramified in $\mathbb{Z}(\zeta_l)$. Therefore if g contains one root from the cluster of ζ_l it contains all of them. The same is true if $\zeta_l = 1$. Therefore, either $\deg g \equiv 0 \mod p,\ \deg h \equiv -2 \mod p$ or the other way around. The same is obviously true for l instead of p.

As $\deg g,\ \deg h$ are both less than $a-2$, we can assume that

$$\deg g \equiv 0 \mod p,\ \deg g \equiv -2 \mod l;$$

$$\deg h \equiv -2 \mod p,\ \deg h \equiv 0 \mod l.$$

This clearly leaves just one choice for $\deg g$: $\deg g = pN$, where N is the number from the statement of this theorem.

Now let's notice that we can actually be a little bit more precise. As $g(x)$ doesn't contain the roots around 1, and contains all or none of the roots from any of the clusters, its reduction modulo p has to be of the form $u(x)^p$, where $u(x)$ is some polynomial dividing $\frac{x^l-1}{x-1}$. But it is an elementary fact from the theory of cyclotomic fields that $\frac{x^l-1}{x-1}$ splits modulo p into the product of prime factors of same degree k, where k is the order of p in $(\mathbb{Z}/l\mathbb{Z})^*$. As $\deg u = N,\ k$ must divide N. But we assumed that it doesn't, so the theorem is proven.

Remark 3.2. It looks like for most pairs (p,l) either (p,l) or (l,p) satisfies that extra condition from the above theorem. However, it is not the case, say, for $p = 5, l = 31$. So the above theorem is not applicable for $a = 155$.

Theorem 3.4. *If $c = 2$, then $f_{abc}(x)$ is irreducible.*

Proof. By Lemma 2.10, in 2-adic field we have b roots x_i of $f_{abc}(x)$ with $v_2(x_i) = \frac{1}{b}$. So $f_{abc}(x)$ is irreducible (actually, Eisenstein).

Theorem 3.5. *If $c = p$, p is odd prime, a is even, then $f_{abc}(x)$ is irreducible.*

Proof. In p-adic complex field we have b roots x_i of $f_{abc}(x)$ with $v_p(x_i) = \frac{1}{b}$ and $p-2$ roots with $v_p(x_i - 1) = \frac{1}{p-2}$. So if $f_{abc}(x) = g(x) \cdot h(x)$ then $\deg g = b$, $\deg h = p-2$ or the other way around. But, as in Theorem 3.2, for even a the degrees of g and h have to be even, contradiction.

Remark 3.3. The above theorems are just the examples of irreducibility results that one can get from knowing the p-adic distribution of roots of $f_{abc}(x)$ for $p|abc$. So far it was just a density zero set of really good triples. The following theorem proves the irreducibility for the positive density set of triples abc.

Theorem 3.6. *If b and c are both square-free and greater than 1, then $f_{abc}(x)$ is irreducible.*

Proof. By the obvious symmetry of the problem, we can assume that $b > c$. Then consider any prime $p|c$. In p-adic complex numbers there are exactly b roots of $f_{abc}(x)$ with $p-$adic valuation $\frac{1}{b}$. If $f(x) = g(x)h(x)$, $\deg g \geq \deg h$, then g has to contain all these roots. As this is true for any $p|c$, h has constant term ± 1. Consider now any prime $p|b$. There are, again, exactly c roots of $f_{abc}(x)$ with p-adic valuation $-\frac{1}{c}$. Either g or h must contain them all. If this is h, then $\deg h \geq c$ which contradicts the equality $\deg g + \deg h = a - 2$ $(< b + c)$. So, it is g again. As this is true for all $p|b$, $h(x)$ is monic. As $h(x)$ only contains roots with 0 p-adic valuations for all $p|bc$, we can apply the argument of the Theorem 3.3 to show that the residue of $\deg h(x)$ modulo any such p is 0 or -2. This implies that

$$bc \Big| \deg h \cdot (\deg h + 2).$$

Therefore $\deg h \cdot (\deg h + 2) \geq bc > c^2$, so $\deg h > c - 2$. But this contradicts to the fact that

$$\deg h(x) = a - 2 - \deg g(x) \leq a - 2 - b = c - 2.$$

Remark 3.4. Unfortunately, the above argument doesn't work in the case $c = 1$ as we have to have at least one prime dividing c to conclude that $\deg g(x) \geq b$.

Before going any further let's prove the following three lemmas.

Lemma 3.1. *As always, we have $a = b + c$, coprime. Suppose $p|a$ (or $p|b$ or $p|c$) and $\zeta \neq 1$ is a nontrivial a_1-th (or b_1-th or c_1-th) root of unity (in the notations of Lemmas 2.8-2.11.) Consider its cluster of roots of $f_{abc}(x)$ in $p-$adic complex numbers. Suppose now that*

$g(x)|f_{abc}(x)$. Then the number of roots of $g(x)$ from the cluster of ζ is always divisible by p.

Proof. We will consider the case $p|a$, because the same proof works in the other two cases as well. Suppose $a = p^k \cdot a_1$. It follows from the proof of Lemma 2.8 that the Newton Polygon for $F(x) = f_{abc}(\zeta + x)$ has k non-horizontal edges of length p and $p^i(p-1)$, $i = 1, 2, ..., k-1$ with the slopes $\frac{1}{p}$ and $\frac{1}{p^i(p-1)}$ correspondingly. Because the corresponding cyclotomic field is unramified at p, the Newton Polygon for $G(x) = g(\zeta + x)$ has only integral vertices. Because $G(x)|F(x)$, all edges of G are edges or parts of edges of F. But there are no integral points inside of the non-horizontal edges of the Newton Polygon for F so the non-horizontal part of the Newton Polygon for G consists of the whole edges of the one for F. Therefore the number of roots of $g(x)$ near ζ is a sum of some numbers from the set $\{p, p^i(p-1) | i = 1, 2, ..., k-1\}$. All of them are divisible by p, which completes the proof of the lemma.

Remark 3.5. One can also formulate and prove a similar result for the cluster of 1. We are not going to do it here because we are not going to use it.

Lemma 3.2. *Suppose $a = b + c$ is a coprime triple and $g(x)|f_{abc}(x)$. Then we have the following.*

1) If $p||b$ (or, more, generally, if $p^k||b$, $\gcd(k, c) = 1$) then $g(x)$ contains all or no roots x_i of $f_{abc}(x)$ with $v_p(x_i) < 0$.

2) If $p^k||b$ and $\deg g(x) < \frac{c}{\gcd(k,c)}$ then $g(x)$ contains no roots x_i with $v_p(x_i) < 0$. As a result, if $\deg g(x) < \frac{c}{\log_2 b}$ then $g(x)$ is monic. (If $b = 1$ we treat $\frac{c}{\log_2 b}$ as $+\infty$, so the above condition is always satisfied).

Proof. If $p^k||b$, $k \geq 1$, then there are c such roots x_i of $f_{abc}(x)$ with $v_p(x_i) = -\frac{k}{c}$. If N of them are the roots of $g(x)$ then $\frac{Nk}{c} \in \mathbb{Z}$. This implies that in (1) N is 0 or c and that in (2) $N = 0$. The second conclusion in (2) is because $\gcd(k, c) \leq k \leq \log_2 b$.

Lemma 3.3. *Suppose $g(x)$ is a polynomial with integral coefficients which divides $f_{abc}(x)$. We denote by A_l the following rational number associated with $g(x)$.*

$$A_l = \sum_{g(x_i)=0} (1 - x_i) x_i^l.$$

a) Suppose $p|a$. Then for every integer $l \geq 0$ we have $p|A_l$ (i.e. $v_p(A_l) > 0$).

b) 1) Suppose $p||b$. Then for every integer l, such that $1 \leq l \leq c-2$, we have $p|A_l$.

2) Suppose $f_{abc}(x) = g(x) \cdot h(x)$, $p||b$ *(or, more generally,* $p^k||b$, $\gcd(k,c) = 1$.*) Then* p *always divides at least one of the two numbers* $A_0(g)$ *and* $A_0(h)$.

c) 1) Suppose $p|c$. *Then for any integer* $l > 0$ *we have* $p|A_l$.

2) Suppose $f_{abc}(x) = g(x) \cdot h(x)$, $p||c$ *(or, more generally,* $p^k||c$, $\gcd(k,b) = 1$.*) Then for each* $l \geq 0$, p *always divides at least one of the two numbers* $A_0(g)$ *and* $A_0(h)$.

Proof. a) By Lemma 3.1 the number of roots of $g(x)$ in every cluster of $\zeta \neq 1$ is divisible by p. Therefore

$$A_l = \sum_{\zeta \neq 1} \sum_{\substack{g(x_i)=0 \\ v_p(x_i-\zeta)>0}} (1-x_i)x_i^l + \sum_{\substack{g(x_i)=0 \\ v_p(x_i-1)>0}} (1-x_i)x_i^l \equiv$$

$$\equiv \sum_{\zeta \neq 1} \#\{x_i : v_p(x_i - \zeta) > 0\} \cdot (1-\zeta)\zeta^l \equiv 0,$$

where "$\alpha \equiv \beta$" means that $v_p(\alpha - \beta) > 0$.

b) 1) By Lemma 3.2 $g(x)$ contains all or no roots x_i with $v_p(x_i) < 0$. If it contains no such roots then as in (a) $v_p(A_l) > 0$. If it contains all such roots then $v_p(A_l(f_{abc}(x)) - A_l(g)) > 0$ because $\frac{f_{abc}(x)}{g(x)}$ contains no such roots. Let's notice now that

$$A_l(f_{abc}(x)) = \sum_{f_{abc}(x_i)=0} (1-x_i)x_i^l = \sum_{bx_i^a - ax_i^b + c = 0} (1-x_i)x_i^l.$$

This last number is equal to 0 for $1 \leq l \leq c-2$ because all the elementary symmetric functions $\sigma_1, ..., \sigma_{c-1}$ are zeroes and so are the sums of the powers $\sum x_i^l$ and $\sum x_i^{l+1}$ for $1 \leq l \leq c-2$.

2) Again, by Lemma 3.2 either $g(x)$ or $h(x)$ contains no roots x_i with $v_p(x_i) < 0$. So either $A_l(g)$ or $A_l(h)$ is divisible by p as in (a).

c) 1) The roots x_i with $v_p(x_i) > 0$ cause no trouble for $l \geq 1$ because $v_p\big((1-x_i)x_i^l\big) > 0$. So we can prove that $p|A_l$ as in (a).

2) Lemma 3.2 applied to $f_{acb}(x)$ and reciprocals of $g(x)$ and $h(x)$ implies that either $g(x)$ or $h(x)$ contains no roots with $v_p(x) > 0$. The rest is as in (a).

Theorem 3.7. *Suppose* $b = 1$ *and* $a \geq 3$ *is square-free. Then* $f_{abc}(x) = f_{a,1,a-1}(x)$ *is irreducible.*

Proof. Suppose $f(x) = g(x) \cdot h(x)$. Consider two numbers, $A = A_0(g)$ and $B = A_0(h)$. Because $b = 1$ they are both integers. By the Lemma 3.3 and because a is square-free they are both divisible by a.

By Lemma 2.5 for every root x_i of $f_{abc}(x)$ $|x_i| < 2$.

Therefore $Re(x_i) < 2$, $Re(1 - x_i) > -1$.

So,

$$A = \sum_{g(x_i)=0} (1 - x_i) > -\deg g > -a$$

and the same for B.

Because

$$A + B = A_0(f_{abc}(x)) = \sum_{bx_i^a - ax_i^b + c = 0} (1 - x_i) = a,$$

the only possibility (up to the switch of g and h) is that $A = a, B = 0$.

Because $b = 1$, for every prime $p|c$ we have just one root of $f_{abc}(x)$ in $p-$adic complex numbers with $v_p(x_i) > 0$. If $g(x)$ doesn't contain it then as in the proof of Lemma 3.3(a) we have $p|A$. Because $A = a$ and $a \equiv 1 \mod p$ we conclude that for every $p|c$ $g(x)$ contains the corresponding root. But this implies that $h(x)$ doesn't contain it, so the constant term of $h(x)$ is ± 1. This is impossible because by Lemma 2.3 all the roots of $f_{abc}(x)$ are outside of the unit circle on the complex plane.

Remark 3.6. The above theorem proves irreducibility for a positive density set of a. I first proved it under the additional assumption that $c = a - 1$ is also square-free). By arguing as in the beginning of the next theorem, one can also prove that $f_{abc}(x)$ is irreducible if $b = 1$ and

$$\left(\prod_{p|a} p\right)^2 \cdot \prod_{p|a-1} p > 9a^2$$

with 9 being a really lazy constant.

One can also prove that the right hand side of the above inequality can be replaced by $C \cdot a \log^2 a$ where C is some small effective constant. This can be done by considering the sums of $x_i - \frac{1}{x_i}$ instead of $1 - x_i$. This will be included in our joint paper with M. Filaseta and T.Y. Lam which is currently in preparation.

The remaining part of this paper is in fact motivated by this joint work. In particular, Theorem 3.10 and its Corollary may be viewed as generalizations of the special case $b = 1$ which was first obtained as part of this joint work.

Remark 3.7. The following theorem is our main result. It proves that $f_{abc}(x)$ is irreducible for the set of coprime triples having density one (which will be justified in Theorem 3.9.)

Theorem 3.8. *We consider all coprime triples $a = b + c$, $b < c$. Then for every $\varepsilon > 0$ if a is big enough, and*

$$(1) \qquad \Big(\prod_{p|a} p\Big)^2 \Big(\prod_{p||b} p\Big)\Big(\prod_{p||c} p\Big) > (4+\varepsilon)a^2 b$$

then $f_{abc}(x)$ is irreducible.

Proof. We will assume in the proof that $\varepsilon < 1$.

Suppose $f_{abc}(x) = g(x) \cdot h(x)$. Consider $A = A_0(g)$ and $B = A_0(h)$ (in the notations of Lemma 3.3). Then if the leading coefficient of $g(x)$ is b_1 and the leading coefficient of $h(x)$ is b_2 then $b_1 \cdot b_2 = b$ and A and B are rational numbers with the denominators dividing b_1 and b_2 correspondingly. Also, by Lemma 3.3 if $p|a$ then $p|A$ and $p|B$ and if $p||b$ or $p||c$ then p divides at least one of the numbers A, B. Therefore, $b \cdot A \cdot B \in \mathbb{Z}$ and it is divisible by $\Big(\prod\limits_{p|a} p\Big)^2 \Big(\prod\limits_{p||b} p\Big)\Big(\prod\limits_{p||c} p\Big)$. On the other hand, by Lemma 2.6 if $a \gg 1$ then

$$|A| \le \deg(g) \cdot (1 + \max(|x_i|)) \le (2 + \frac{\varepsilon}{5}) \cdot \deg(g).$$

The same is true for h. Because $\deg(g)$ and $\deg(h)$ are both less than a,

$$b \cdot A \cdot B < (2 + \frac{\varepsilon}{5})^2 \cdot a^2 b < (4+\varepsilon) \cdot a^2 b$$

The condition (1) now implies that $AB = 0$. We may and will assume that $A = 0$. To complete the proof of the theorem we first prove the following proposition which says that if $A = 0$ then $\deg(g)$ is small.

Proposition 3.1. *In the above notation if $A = 0$ then for $a \gg 1$*

$$\deg(g) < 28\sqrt{a \ln a}.$$

Proof. The basic idea is that the roots x_i of $f_{abc}(x)$ are somewhat uniformly distributed around the unit circle so $Re(1 - x_i)$ is almost always positive and when it is negative it's rather small in absolute value. To be more precise, Lemma 2.6 implies that for a big enough $r_i < 1 + \frac{3 \ln a}{a}$, where $x_i = r_i \cdot e^{\varphi_i}$, $-\pi < \varphi_i \le \pi$.

Therefore $Re(1 - x_i) > -\frac{3 \ln a}{a}$.

Also, it follows from this that if $|\varphi_i| > \frac{4\sqrt{\ln a}}{\sqrt{a}}$ then for $a \gg 1$ $\cos \varphi_i < (1 - \frac{7 \ln a}{a})$. In this case

$$Re(1 - x_i) = 1 - r_i \cos \varphi_i > 1 - (1 + \frac{3 \ln a}{a})(1 - \frac{7 \ln a}{a}).$$

This is greater than $\frac{3 \ln a}{a}$ for $a \gg 1$.

By the Theorem 2.1 the number of roots of $f_{abc}(x)$ with $|\varphi_i| \leq \frac{4\sqrt{\ln a}}{\sqrt{a}}$ is bounded by

$$\frac{8\sqrt{\ln a}}{2\pi\sqrt{a}}n + 12\sqrt{n\ln(n+1)} < 14\sqrt{a\ln a}.$$

So if $\deg g(x) \geq 28\sqrt{a\ln a}$ then for more than half of the roots of $g(x)$ we have $|\varphi_i| > \frac{4\sqrt{\ln a}}{\sqrt{a}}$ and by the above calculations $A = Re(A)$ is positive. Because we assumed that $A = 0$, the proposition is proven.

Let's now continue to prove the theorem. Because of the above proposition, $f_{abc}(x)$ is divisible by a polynomial $g(x)$ of degree less than $28\sqrt{a\ln a}$. By taking an irreducible divisor of $g(x)$ we may and will assume that this $g(x)$ is irreducible. By doing this we may loose the $A = 0$ condition but we don't care about it anymore.

There are at least two different ways to prove that this is impossible. One is to use some results on Lehmer's conjecture as in Theorem 3.11. Instead of doing this let me propose a self-contained proof using Lemmas 3.2 and 3.3 above.

By Lemma 3.2 $g(x)$ is monic, because for $a \gg 1$

$$\deg(g) \leq \frac{a}{3\log_2 a} < \frac{c}{\log_2 b}.$$

Consider $A_l = A_l(g)$ as in Lemma 3.3 for $l = 1, 2, ..., \deg(g)$. Because $g(x)$ is monic, A_l is an integer for every l. Also, for every l as above Lemma 3.3 implies that A_l is divisible by $\big(\prod_{p|a} p\big)$ and by $\big(\prod_{p|c} p\big)$. It is also divisible by $\big(\prod_{p||b} p\big)$ because $\deg(g) + 1 < \frac{a}{3} \leq c - 2$ for $a \gg 1$.

The condition (1) implies that

$$\big(\prod_{p|a} p\big)\big(\prod_{p||b} p\big)\big(\prod_{p|c} p\big) > \sqrt{(4+\varepsilon)a^2 b} > 2a.$$

On the other hand,

$$A_l \leq \deg(g)\cdot\big(\max(r^{l+1}) + \max(r^l)\big) \leq$$

$$\leq 2\deg(g)\cdot(1+\frac{2c}{b})^{\frac{l+1}{c}} \leq 56\sqrt{a\ln a}(1+2a)^{M\frac{\ln a}{\sqrt{a}}},$$

where M is some constant. The second inequality here comes from the estimate in the proof of Lemma 2.5.

Because

$$\ln(1+2a)^{M\frac{\ln a}{\sqrt{a}}} = M\cdot\frac{\ln a\cdot\ln(1+2a)}{\sqrt{a}} \ll 1,$$

we have that

$$A_l \ll \sqrt{a} \ln a.$$

This implies that for $a \gg 1$ all $A_l = 0$ for those l which we are interested in now. But this means that if x is the (abstract) root of $g(x)$ and $K = \mathbb{Q}[x]$ we have $Tr\big((1-x)\cdot x^l\big) = 0$ for all $l = 1, 2, ..., \deg(g)$. This implies that $(1-x)$ is in the kernel of the trace form of K because x^l, $l = 1, 2, ..., \deg(g)$ form a $\mathbb{Q}-$basis of K. Because this form is always non-degenerate (cf., e.g. [1]), $1 - x = 0$, $x = 1$. As this is clearly impossible, the theorem is proven.

Remark 3.8. The constant $(4+\varepsilon)$ in the above theorem can be improved to $(2+\varepsilon)$ by noticing that $\deg(g) + \deg(h) = a - 2$ and that A and B cannot be too negative as a corollary of Theorem 2.1. One can also make the $a \gg 1$ condition above explicit, for any fixed ε, but I am not sure that it's worth the work and it would probably hide the basic ideas of the proof.

Theorem 3.9. *The number of coprime triples $a = b + c$, $b < c$, with $a \leq A$ which satisfy*

$$\Big(\prod_{p|a} p\Big)^2 \Big(\prod_{p||b} p\Big)\Big(\prod_{p||c} p\Big) \ll a^2 b \tag{2}$$

is bounded by $C \cdot A^{\frac{20}{11}} \ln A$ where C is some constant independent of A.

Proof. Let's decompose $a = a_1 \cdot a_2^2$, where a_1 is square-free. Then $\prod_{p|a} p \geq a_1$. Also, we can decompose (not uniquely) $b = b_1 \cdot b_2^2 \cdot b_3^3$ and $c = c_1 \cdot c_2^2 \cdot c_3^3$, where $b_1 = \prod_{p||b} p$ and $c_1 = \prod_{p||c} p$. Then

$$a^2 bc = a_1^2 \cdot a_2^4 \cdot b_1 \cdot b_2^2 \cdot b_3^3 \cdot c_1 \cdot c_2^2 \cdot c_3^3$$

and because by (2) $a_1^2 b_1 c_1 \ll a^2 b$, we get

$$a_2^4 \cdot b_2^2 \cdot b_3^3 \cdot c_2^2 \cdot c_3^3 \gg c \gg a.$$

It follows that either $a_2 b_2 \gg a^{2/11}$, $a_2 c_2 \gg a^{2/11}$, or $b_3 c_3 \gg a^{1/11}$. The argument for the first two of these situations is similar, so we only give here the argument when $a_2 b_2 \gg a^{2/11}$ and $b_3 c_3 \gg a^{1/11}$. Suppose first that $a_2 b_2 \gg a^{2/11}$. Then the number of triples (a, b, c) with $a = b + c$ is bounded by

$$\sum_{1 \leq a_2 \leq A^{1/2}} \#\{a \in [1, A] : a_2^2 | a\} \sum_{1 \leq b_2 \leq A^{1/2}} \#\{b \in [1, A] : b_2^2 | b, b \ll (a_2 b_2)^{11/2}\} \ll$$

$$\ll \sum_{1\le a_2\le A^{1/2}} \frac{A}{a_2^2}\Bigg(\sum_{1\le b_2\le A^{2/11}/a_2} \frac{(a_2b_2)^{11/2}}{b_2^2} + \sum_{A^{2/11}/a_2<b_2\le A^{1/2}} \frac{A}{b_2^2}\Bigg) \ll$$

$$\ll \sum_{1\le a_2\le A^{1/2}} \frac{A}{a_2^2}\times A^{1-(2/11)}a_2 \ll \sum_{1\le a_2\le A^{1/2}} \frac{A^{2-(2/11)}}{a_2} \ll A^{20/11}\ln A.$$

For $b_3c_3 \gg a^{1/11}$ the number of triples (a,b,c) with $a=b+c$ is bounded by

$$\sum_{1\le b_3\le A^{1/3}} \#\{b\in[1,A] : b_3^3|b\} \sum_{1\le c_3\le A^{1/3}} \#\{c\in[1,A] : c_3^3|c, c\ll (b_3c_3)^{11}\} \ll$$

$$\ll \sum_{1\le b_3\le A^{1/3}} \frac{A}{b_3^3}\Bigg(\sum_{1\le c_3\le A^{1/11}/b_3} \frac{(b_3c_3)^{11}}{b_3^3} + \sum_{A^{1/11}/b_3<c_3\le A^{1/3}} \frac{A}{b_3^3}\Bigg) \ll$$

$$\ll \sum_{1\le b_3\le A^{1/3}} \frac{A}{b_3^3}\times A^{1-(2/11)}b_3^2 \ll \sum_{1\le b_3\le A^{1/3}} \frac{A^{2-(2/11)}}{b_3} \ll A^{20/11}\ln A.$$

Combining the above, we get that the number of coprime triples (a,b,c) as in the theorem is $O(A^{20/11}\ln A)$.

Corollary 3.1. *The set of coprime triples where $f_{abc}(x)$ is reducible has density zero in the set of all coprime triples.*

Proof. It follows from Theorems 3.8 and 3.9 and the well-known fact that the number of coprime pairs (a,b) where $a>b$ with $a\le A$ is asymptotically equivalent to $\frac{6}{\pi}\cdot\frac{A^2}{2}$. According to Donald Knuth (cf. [8], p. 324) this fact is due to L. Dirichlet.

Now let's consider what happens if one fixes b. When $b=2$ then $f_{abc}(x)$ is always irreducible by Theorem 3.4. Also, Theorem 3.5 gives a partial result for b being an odd prime. The following theorem (with the corollary after it) shows that for any fixed b the abc-polynomial is irreducible for the set of a's having density one. Please note that in the following theorem and its corollary some of the implied constants in " $\gg$ " and " $\ll$ " depend on b.

Theorem 3.10. *If b is fixed, then the number of coprime triples $a=b+c$ with $a<A$ and*

$$(\prod_{p|a} p)^2(\prod_{p||c} p) \ll a^2 \tag{3}$$

is at most $C(b)\cdot A^{\frac{13}{15}}$, where $C(b)$ is some constant depending on b.

Proof. As in Theorem 3.9, let's decompose $a = a_1 a_2^2$ and $c = c_1 c_2^2 c_3^3$. Because $a^2 c = a_1^2 a_2^4 c_1 c_2^2 c_3^3$ and (3) implies that $a_1^2 c_1 \ll a^2$, we get

$$a_2^4 c_2^2 c_3^3 \gg c \gg a.$$

It follows that either $a_2 \gg a^{\frac{2}{15}}$, $c_2 \gg a^{\frac{2}{15}}$, or $c_3 \gg a^{\frac{1}{15}}$. The argument for the first two of these situations is similar so we only give here the argument when $a_2 \gg a^{\frac{2}{15}}$ and $c_3 \gg a^{\frac{1}{15}}$. Suppose first that $a_2 \gg a^{\frac{2}{15}}$. Then the number of triples (a,b,c) with $a = b + c$ is bounded by

$$\sum_{1 \le a_2 \le A} \#\{a : (a_2^2 | a, a \ll a_2^{\frac{15}{2}}, a \le A)\} \ll$$

$$\ll \sum_{1 \le a_2 \le A^{\frac{2}{15}}} (\frac{a_2^{\frac{15}{2}}}{a_2^2}) + \sum_{A^{\frac{2}{15}} \le a_2 \le A} (\frac{A}{a_2^2}) \ll A^{\frac{13}{15}}$$

For $c_3 \gg a^{\frac{1}{15}}$ the number of triples (a,b,c) with $a = b + c$ is bounded by

$$\sum_{1 \le c_3 \le A} \#\{c : (c_3^3 | c, c \ll c_3^{\frac{1}{5}}, c \le A)\} \ll$$

$$\ll \sum_{1 \le c_3 \le A^{\frac{1}{15}}} c_3^{12} + \sum_{A^{\frac{1}{15}} \le c_3 \le A} (\frac{A}{c_3^3}) \ll A^{\frac{13}{15}}$$

Combining together all the estimates, the theorem is proven.

Corollary 3.2. *For any fixed b $f_{abc}(x)$ is irreducible for a set of natural numbers a coprime to b having density one.*

Proof. It follows from Theorems 3.8 and 3.10 and a trivial observation that $\#\{a : a < A, \gcd(a,b) = 1\} \gg A$.

If b is good in the sense that there is a prime p which divides it in exactly the first power, then the following theorem proves that all but finitely many abc-polynomials are irreducible. It also provides a rather small bound for the possible exceptions. I should also mention that almost all (in the sense of density) b's are good in the above sense.

Theorem 3.11. *Suppose p is a prime, $p||b$. Suppose also that $c \ge b \cdot \max(\kappa, \log_2 b)$, where $\kappa = 11.21685874...$ is such that $\beta^\kappa = 1 + 2\kappa$, where $\beta^3 - \beta - 1 = 0$. Then $f_{abc}(x)$ is irreducible.*

Proof. Suppose $f_{abc}(x) = g(x) \cdot h(x)$. Then as in Lemma 3.2 one of the polynomials $g(x)$, $h(x)$ contains none of c roots x_i of $f_{abc}(x)$ with $v_p(x_i) < 0$. We may assume this is $g(x)$. Then $\deg g(x) \le b - 2$.

Now for every other prime $l|b$ $g(x)$ also contains no roots x_i with $v_l(x_i) < 0$ because by our assumption $\deg g \leq b-2 < b < \frac{c}{\log_2 b}$. Therefore $g(x)$ is a monic polynomial. If its constant term is not ± 1 then at least one of its roots has absolute value of at least $2^{\frac{1}{d}}$, where $d = \deg(g)$. If its constant term is ± 1 one can still conclude that one of its roots has absolute value of at least $\beta^{\frac{1}{d}}$, with β as above by applying the Smyth's result on the Lehmer's conjecture (cf. [20]). To apply this result we just need to check that $g(x)$ is not reciprocal. (As far as I know for the reciprocal polynomials the Lehmer's conjecture is not yet proven although there are some (just a little bit) weaker bounds (cf. [4], [15])). If $g(x)$ was reciprocal this would have meant that for some $x \neq 1$ both $bx^a - ax^b + c$ and $cx^a - ax^c + b$ are equal to zero. Therefore

$$a(x^b-1)(x^c-1) = (bx^a - ax^b + c) + (cx^a - ax^c + b) = 0$$

Therefore $|x| = 1$ which is impossible by Lemma 2.2.

As a result, we get a root x of $g(x)$ and therefore of $f_{abc}(x)$ with $|x| \geq \beta^{\frac{1}{d}} > \beta^{\frac{1}{b}}$ But by the estimate in the proof of Lemma 2.5

$$|x| \leq \left(1 + \frac{2c}{b}\right)^{\frac{1}{c}}.$$

Combining the above, we get that

$$\beta^{\frac{c}{b}} < \left(1 + \frac{2c}{b}\right).$$

Therefore for κ as in the theorem $\frac{c}{b} < \kappa$. The theorem follows.

4. Miscellaneous and Heuristics

First of all, combining the results of Chapter 3 one can easily check that $f_{abc}(x)$ is always irreducible for all $a \leq 24$ except of $f_{9,5,4}$ (and $f_{9,4,5}$, of course) and $f_{16,15,1}$. Let us prove separately their irreducibility.

Theorem 4.1. *The polynomial $f_{9,5,4}(x)$ is irreducible.*

Proof. Suppose $f_{9,5,4}(x) = g(x) \cdot h(x)$. In 5−adic complex field we have 4 roots x_i of $f_{9,5,4}$ with $v_5(x_i) = -\frac{1}{4}$ and 3 roots with $v_5(x_i - 1) = \frac{1}{3}$. So, $\deg g = 3$ or $\deg g = 4$. On the other hand, in 2-adic complex field we have 5 roots of $f_{9,5,4}$ with $v_2(x_i) = \frac{2}{5}$ and 2 roots with $v_2(x_i - 1) = \frac{1}{2}$. This implies that $\deg g = 5$ or $\deg g = 2$, contradiction.

Theorem 4.2. *The polynomial $f_{16,15,1}(x)$ is irreducible.*

Proof. Suppose $f_{16,15,1}(x) = g(x) \cdot h(x)$. Then in 3-adic complex field we have 1 root x_i with $v_3(x_i) = -1$, 1 root with $v_3(x_i - 1) = 1$ and 3 roots around each of nontrivial fifth roots of unity, ζ, with $v_3(x_i - \zeta) = \frac{1}{3}$. If g contains one of the last 12 roots, it contains all its

cluster and also all other 9 roots because $\frac{x^5-1}{x-1}$ is irreducible in $\mathbb{Z}_3[x]$. So, if $\deg g \geq \deg h$, then $\deg h \leq 2$. Because 16 is even, by Lemma 2.4 $\deg h = 2$, g doesn't contain the root with $v_3(x_i) = -1$.

The same argument in 5-adic complex field shows that g doesn't contain the root with $v_5(x_i) = -1$, because, again, $\frac{x^3-1}{x-1}$ is irreducible in $\mathbb{Z}_5[x]$. But this implies that the roots of $g(x)$ are units which is impossible as all x_i are inside of the the unit circle in $\mathbb{C}$.

One can also check the irreducibility conjecture numerically for the triples up to a couple of hundreds using the general irreducibility test of Maple. One can definitely try to do more in our particular case because, e.g. one can get tough restrictions on the degree of any divisor polynomial as in the proofs of Theorems 3.6 and 3.11.

This is more or less all I know about the irreducibility of $f_{abc}(x)$. I don't know if it's related in any way to the *abc* conjecture. It is however an experimental fact that it takes longer for a computer to verify the irreducibility when the triple a, b, c is kind of marginal in the sense of *abc* conjecture. (e.g. $169 = 144 + 25$) It's also true that the results of Chapter 3 are mostly about the triples that are not interesting from the point of view of *abc* conjecture. But this may be just the nature of the methods we used there and not of the problem itself.

Let's now discuss a little the hypothetical approaches to the *abc* conjecture using the *abc*-polynomials. The first idea would be to try something similar to the geometric case, i.e. to construct a second polynomial, $g_{abc}(x)$, such that (f, g) is globally bounded but locally big. By this I mean that it has to be on the one hand divisible by a (big) power of any p dividing abc and, on the other hand, be bounded by some inequalities on the complex plane. I tried to cook up such $g(x)$ without any success. Of course, it most probably doesn't exist, because it's extremely unlikely that the conjecture as deep as *abc* could be proven by such primitive methods. But maybe some weaker results could be obtained. Technically, the main problem is to capture the rather subtle dependence of the distribution of the roots of $f_{abc}(x)$ inside the clusters upon k (in the notation of Lemmas 2.8-2.11) without making the degree or coefficients of $g(x)$ too large.

Three other things one can try are the following.

1) One can try to study Arakelov geometry of some curves related to $f_{abc}(x)$, e.g. hyperelliptic curve over $\mathbb{Q}$ $y^2 = f_{abc}(x)$ and elliptic curve over the *abc*-field $y^2 = x(x-1)(x-\lambda)$, where $f_{abc}(\lambda) = 0$. As far as hyperelliptic curves are concerned there is a recent result of I. Kausz (cf. [7]) on ω^2 of semistable hyperelliptic curves. I should note however

that $y^2 = f_{abc}(x)$ is not a semistable model and it actually has pretty bad singularities over $p|abc$. Also, its genus depends on a and Kausz's estimates "at infinity" depend heavily on the genus as they involve a choice of a metric on the relative dualizing sheaf of the "universal stable curve" of given genus.

2) Modulo the irreducibility conjecture, one can try to investigate some invariants of abc-fields , like Galois group, regulator, or ζ–function. One thing which is quite obvious is that there are lots of $abc-$units hanging around. (By $abc-$units I mean elements of the abc-field which have zero valuations for all primes not dividing abc.) Namely, x, $x^a - 1$, $x^b - 1$, $x^c - 1$ and all divisors of the last three polynomials evaluated at the root of abc-polynomial are $abc-$units. For instance, we have a lot of solutions of the equation $x + y = 1$ in $abc-$units. The theory of $S-$units and $S-$unit equations is well developed (cf., e.g. [3], [6], [17]). I don't know, however, if it is better to apply the theory to the roots of $f_{abc}(x)$ instead of just to $\frac{b}{a} + \frac{c}{a} = 1$.

3) One can look at the mutual position of the abc-field and some cyclotomic fields. One can check, for instance, that if K_{abc} is the decomposition field of the abc-polynomial (which one can call the big $abc-$field) then $K_{abc}[\zeta_{\frac{abc}{R}}]$ is unramified over K_{abc}, where R is the product of all primes dividing abc. I don't know however if this is of any interest because K_{abc} is very big.

Finally, I personally would be interested to see an extensive computer investigation of the invariants of abc-fields .

References

[1] *Algebraic number theory. Proceedings of the instructional conference held at the University of Sussex, Brighton, September 1–176, 1965.* Edited by J.W.S. Cassels and A. Frohlich. Reprint of the 1967 original. Academic Press, Inc, London-New York, 1986.

[2] Yu. F. Belotserkovskii, *Uniform distribution of algebraic numbers near the unit circle,* Vestsi Akademii Navuk BSSR, Ser. Fiz-Mat. Navuk 1988, no 1, 49-52 (in Russian).

[3] F. Beukers, H. P. Schlickewei, *The equation $x + y = 1$ in finitely generated groups.* Acta Arith. **78** (1996), no. 2, 189-199.

[4] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial,* Acta Arith. 34 (1979), 391-401.

[5] P. Erdős, P. Turán, *On the distribution of roots of polynomials,* Ann. of Math. **51** (1950), 105–119.

[6] J.-H. Evertse, K. Győry, C.L. Stewart, R. Tijdeman, *S-unit equations and their applications,* New advances in transcendence theory (Durham, 1986), 110-174, Cambridge Univ. Press, Cambridge - New York, 1988.

[7] I. Kausz, *A discriminant and an upper bound for ω^2 for hyperelliptic arithmetic surfaces.* IHES preprint, 1996

[8] D. Knuth, *The Art of Computer Programming.* Vol. 2, 2nd edition, 1981.
[9] Neal Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions.* Second Edition. Graduate Texts in Math. **58**, Springer-Verlag, New York - Berlin, 1984.
[10] K. Mahler, *An application of Jensen's formula to polynomials,* Mathematika **7** (1960), 98-100.
[11] K. Mahler, *An inequality for the discriminant of a polynomial,* Michigan Math. J. **11** (1964), 257-262.
[12] R. C. Mason, *Diophantine equations over function fields.* London Math. Soc. Lecture Notes Series, **96** Cambridge University Press, Cambridge - New York, 1984.
[13] J.-L. Nicolas, A. Schinzel, *Localisation des zéros de polynômes intervenant en théorie du signal*, Lecture Notes in Math **1415**, Springer, Berlin-New York, 1990.
[14] J. Oesterlé *Nouvelles approches du "théorème" de Fermat,* Séminaire Bourbaki, Vol 1987/88. Astérisque No. 161-162 (1988), Exp. 694, 165-186 (1989).
[15] U. Rausch, *On a theorem of Dobrowolski about the product of conjugate numbers,* Colloquium Mathematicum **50** (1985), 137-142.
[16] A. Schinzel, *Reducibility of lacunary polynomials. IX,* New advances in transcendence theory. (Durham, 1986), 313-336, Cambridge Univ. Press, Cambridge - New York, 1988.
[17] Wolfgang M. Schmidt, *Diophantine approximations and Diophantine equations,* Lecture Notes in Mathematics, **1467**. Springer-Verlag, Berlin, 1991.
[18] E. Selmer, *On the irreducibility of certain trinomials,* Math. Scand. **4** (1956), 287 -302.
[19] Joseph H. Silverman, *The S-unit equation over function fields.* Math. Proc. Cambridge Philos. Soc. **95** (1984), no. 1, 3-4.
[20] C.J. Smyth, *On the product of conjugates outside of the unit circle of an algebraic integer,* Bull. London Math. Soc. **3** (1971), 169-175.
[21] W.W. Stothers, *Polynomial identities and Hauptmoduln,* Quart. J. Math. Oxford Ser. (2) **32** (19810, no. 127, 349-370.

Department of Mathematics, The Pennsylvania State University, State College, PA 16802, USA
E-mail address: borisov@math.psu.edu