THE ABC CONJECTURE AND ITS APPLICATIONS

by

JOSEPH SHEPPARD

B.A., Kansas State University, 2014

A REPORT

submitted in partial fulfillment of the
requirements for the degree

MASTER OF SCIENCE

Department of Mathematics
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2016

Approved by:

Major Professor
Christopher Pinner

Abstract

In 1988, Masser and Oesterlé conjectured that if A, B, C are co-prime integers satisfying

$$A + B = C,$$

then for any $\epsilon > 0$,

$$\max\{|A|, |B|, |C|\} \leq K(\epsilon)\mathrm{Rad}(ABC)^{1+\epsilon},$$

where $\mathrm{Rad}(n)$ denotes the product of the distinct primes dividing n. This is known as the ABC Conjecture. Versions with the ϵ dependence made explicit have also been conjectured. For example in 2004 A. Baker suggested that

$$\max\{|A|, |B|, |C|\} \leq \frac{6}{5}\mathrm{Rad}(ABC)\frac{(\log \mathrm{Rad}(ABC))^{\omega}}{\omega!}$$

where $\omega = \omega(ABC)$, denotes the number of distinct primes dividing A, B, and C. For example this would lead to

$$\max\{|A|, |B|, |C|\} < \ \mathrm{Rad}(ABC)^{\frac{7}{4}}.$$

The ABC Conjecture really is deep. Its truth would have a wide variety of applications to many different aspects in Number Theory, which we will see in this report. These include Fermat's Last Theorem, Wieferich Primes, gaps between primes, Erdős-Woods Conjecture, Roth's Theorem, Mordell's Conjecture/Faltings' Theorem, and Baker's Theorem to name a few. For instance, it could be used to prove Fermat's Last Theorem in only a couple of lines. That is truly fascinating in the world of Number Theory because it took over 300 years before Andrew Wiles came up with a lengthy proof of Fermat's Last Theorem.

We are far from proving this conjecture. The best we can do is Stewart and Yu's 2001 result

$$\max\{\log|A|, \log|B|, \log|C|\} \leq K(\epsilon)\mathrm{Rad}(ABC)^{\frac{1}{3}+\epsilon}. \tag{1}$$

However, a polynomial version was proved by Mason in 1982.

Contents

Acknowledgments

Thank you Dr. Pinner for all the help on my report; setting me on the right path when I had gone astray. Thank you for putting up with me and caring so much; you are truly the “Charming British Number Theorist”. I enjoy our talks and the exchange of civil conversations about the future of America and other daily matters. A true motivator in Number Theory; you were one of the big reasons why I chose Number Theory. If I haven’t said it enough, thank you.

Thank you also to the other committee members, Dr. Cochrane and Dr. Spencer for your help and influence over the years. Dr. Spencer, you were my undergrad adviser and I enjoyed all the stories you shared with me. Thank you Dr. Cochrane for having great patience and guidance over the years. I wouldn’t be the mathematician that I am today without all of your influences Dr. Cochrane, Dr. Pinner, and Dr. Spencer. So I will say it one more time, thank you.

Dedication

This report is dedicated to Number Theory and those who helped me on my path. Thank you family and friends for being there as support along with Dr. Cochrane, Dr. Pinner, and Dr. Spencer as guidance.

Preface
History of the ABC Conjecture

In 1988, Masser [12] and Oesterlé [14] conjectured that if A, B, C are co-prime integers satisfying

$$A + B = C,$$

then for any $\epsilon > 0$,

$$\max\{|A|, |B|, |C|\} \leq K(\epsilon)\text{Rad}(ABC)^{1+\epsilon}$$

where $\text{Rad}(n)$ denotes the product of the distinct primes dividing n. This is known as the ABC Conjecture.

In 1982, a polynomial version of the ABC Conjecture was proved by Mason [11], resulting in the Mason's Inequality, also known as Mason-Stothers' Theorem. We are still a long way from proving the ABC Conjecture. The best we have are still a logarithm away from proving the ABC Conjecture. For example in 1986, Stewart and Tijdeman [17] first came up with an upper bound

$$\max\{|A|, |B|, |C|\} < \ \exp(K_1\text{Rad}(ABC)^{15})$$

for the ABC Conjecture. This was improved by Stewart and Yu [18] in 1991 to

$$\max\{|A|, |B|, |C|\} < \ \exp(K_2\text{Rad}(ABC)^{\frac{2}{3}+\epsilon})$$

and again in 2001 by Stewart and Yu [19] to

$$\max\{|A|, |B|, |C|\} < \exp(K_3 \mathrm{Rad}(ABC)^{\frac{1}{3}+\epsilon}).$$

People are still actively working on proving the ABC Conjecture. Japanese mathematician Shinichi Mochizuki claims to have proven the ABC Conjecture, but he is in the process of editing his theories. The ABC Conjecture is a very deep result if it holds true. We shall see applications to many different branches of Number Theory

In Chapter 1, we will look at the polynomial version of the ABC Conjecture (Mason's Inequality) proved by Mason in 1982. We will give the proof involving the Wronskian; there is another proof by Silverman [16] (see also Granville and Tucker [9]) using the Riemann-Hurwitz formula. We will see that Mason's Inequality can be used to prove the polynomial version of Fermat's Last Theorem and its variants.

In Chapter 2, we will discuss the ABC Conjecture, effective forms and the current state of knowledge, and see how the ABC Conjecture leads to a simple proof of Fermat's Last Theorem.

In Chapter 3, we present a wide range of other applications of the ABC Conjecture, including Wieferich primes, gaps between primes, the Erdős-Woods Conjecture, Roth's Theorem, Baker's Theorem, and the Mordell Conjecture (Faltings' Theorem).

Chapter 1

ABC Conjecture for Polynomials

In this section we will see Mason's Inequality, the polynomial version of the ABC Conjecture, which can be proved.

1.1 Some Basic Definitions

We are going to define some terms such as the α-order of F, a polynomial with complex coefficients and positive degree, before we head into the Mason Inequality.

Let $F(x) = \sum_{i=0}^{N} a_i x^i$ be a polynomial over $\mathbb{C}$ with $a_N \neq 0$. By the Fundamental Theorem of Algebra, we have

$$F(x) = a_N(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_N),$$

for some complex numbers $\alpha_1, \alpha_2, \cdots \alpha_N$, the roots of the polynomials of F, where $N = \deg F$ is the degree of F.

For $\alpha \in \mathbb{C}$, we define

$$\mathrm{ord}_\alpha(F) = |\{n : 1 \leq n \leq N \text{ and } \alpha_n = \alpha\}|$$

as the number of roots of F, which are equal to α, i.e. if $\text{ord}_\alpha(F) = M$, then we have $(x-\alpha)^M \mid F$, but $(x-\alpha)^{M+1} \nmid F$.

When we sum up the orders we have, as long as F is not the zero polynomial,

$$\sum_{\alpha\in\mathbb{C}} \text{ord}_\alpha(F) = \text{ deg } F.$$

We also define,

$$Z(F) \coloneqq \{\alpha \in \mathbb{C} : F(\alpha) = 0\}$$

for the set of distinct zeros of F. Thus we have,

$$|Z(F)| \leq \text{ deg } F.$$

1.2 Mason's Inequality

Theorem 1.2.1. *Let $A(x)$, $B(x)$, $C(x)$ be polynomials in $\mathbb{C}[x]$ such that:*

(i) $A(x) + B(x) = C(x)$

(ii) $A(x), B(x), C(x)$ *are not all constants*

(iii) $A(x), B(x),$ *and* $C(x)$ *have no common zeroes.*

Then

$$\max\{\deg A, \deg B, \deg C\} \leq |Z(ABC)| - 1.$$

Proof. Assume that (i),(ii), and (iii) hold.

Define the Wronskian

$$\begin{aligned} W(x) &\coloneqq \det \begin{bmatrix} A(x) & B(x) \\ A'(x) & B'(x) \end{bmatrix} \\ &= A(x)B'(x) - B(x)A'(x) \end{aligned}$$

Observe that substituting $C(x) - B(x)$ into $A(x)$ we get,

$$\begin{aligned} W(x) &\coloneqq \det \begin{bmatrix} C(x) - B(x) & B(x) \\ C'(x) - B'(x) & B'(x) \end{bmatrix} \\ &= \det \begin{bmatrix} C(x) & B(x) \\ C'(x) & B'(x) \end{bmatrix} \\ &= C(x)B'(x) - B(x)C'(x). \end{aligned}$$

Similarly we get,

$$\begin{aligned} W(x) &\coloneqq \det \begin{bmatrix} A(x) & C(x) \\ A'(x) & C'(x) \end{bmatrix} \\ &= A(x)C'(x) - C(x)A'(x). \end{aligned}$$

For α, a complex number in $Z(ABC)$, we get

$$\mathrm{ord}_\alpha(A) + \mathrm{ord}_\alpha(B) + \mathrm{ord}_\alpha(C) - 1 \leq \mathrm{ord}_\alpha(W).$$

To see this observe that if $\mathrm{ord}_\alpha(A) = M \geq 1$, then $(x-\alpha)^M \mid A$, $(x-\alpha)^{M-1} \mid A'$, but $(x-\alpha) \nmid B, C$, so we have $(x-\alpha)^{M-1} \mid AC' - CA' = W$. Hence,

$$\mathrm{ord}_\alpha(A) + \mathrm{ord}_\alpha(B) + \mathrm{ord}_\alpha(C) - 1 = M + 0 + 0 - 1 = M - 1 \leq \mathrm{ord}_\alpha(W)$$

Next, summing up this inequality over all the points α in $Z(ABC)$, we get

$$\sum_{\alpha\in Z(ABC)} \operatorname{ord}_\alpha(A) + \sum_{\alpha\in Z(ABC)} \operatorname{ord}_\alpha(B) + \sum_{\alpha\in Z(ABC)} \operatorname{ord}_\alpha(C) - |Z(ABC)| \leq \sum_{\alpha\in Z(ABC)} \operatorname{ord}_\alpha(W),$$

and so, by summing up those orders, we get

$$\deg\, A + \ \deg\, B + \ \deg\, C - |Z(ABC)| \leq \ \deg\, W.$$

Looking at $\deg W$, we see that,

$$\begin{aligned} \deg\, W &= \ \deg\{A(x)B'(x) - B(x)A'(x)\} \\ &\leq \ \deg\, A + \ \deg\, B - 1. \end{aligned}$$

Now we have,

$$\deg\, A + \ \deg\, B + \ \deg\, C - |Z(ABC)| \leq \ \deg\, A + \ \deg\, B - 1.$$

Canceling out the $\deg A$ and $\deg B$ on both sides, we get

$$\deg\, C - |Z(ABC)| \leq -1.$$

Rearranging the inequality we get,

$$\deg\, C \leq |Z(ABC)| - 1.$$

Similarly, with the other representations of $W(x)$, we get

$$\deg\, A \leq |Z(ABC)| - 1$$

and

$$\deg\, B \leq |Z(ABC)| - 1.$$

Combining these inequalities, we have that,

$$\max\{\deg A,\ \deg B,\ \deg C\} \leq |Z(ABC)| - 1.$$

□

Thus we have proved Mason's Inequality.

Observation: We see that Mason's Inequality can be proven by making use of Wronskian polynomials. Mason's Inequality provides a foundation for the ABC Conjecture, but perhaps a generalized version will give us a better understanding.

1.3 Generalized Mason's Inequality

Mason's Inequality can be generalized in different ways that could be useful, let's look at one where we have $N+1$ polynomials.

Theorem 1.3.1. *Suppose $\phi_0(x), \phi_1(x), \cdots \phi_N(x)$ are polynomials in $\mathbb{C}[x]$ such that*

(i) $\phi_0(x) + \phi_1(x) + \cdots + \phi_N(x) = 0$

(ii) $\phi_0(x), \phi_1(x), \cdots, \phi_N(x)$ *span a vector space of dimension N over $\mathbb{C}$,*

(iii) $\phi_0(x), \phi_1(x), \cdots, \phi_N(x)$ *have no common zero in $\mathbb{C}$.*

Then,

$$\max\{\ \mathit{deg}\ \phi_n : 0 \leq n \leq N\} \leq \binom{N}{2}(|Z(\phi_0\phi_1 \cdots \phi_N)| - 1).$$

Proof. Suppose we have $\phi_i(x)$ for $0 \leq i \leq N$ satisfying (i), (ii), and (iii). Reordering as necessary, suppose that $\phi_N(x)$ has the maximum degree.

Say we have,

$$\phi_0(x) + \phi_1(x) + \cdots \phi_{N-1}(x) + \phi_N(x) = 0.$$

Looking at the Wronskian, we get,

$$W(x) = det \begin{bmatrix} \phi_0(x) & \phi_1(x) & \cdots & \phi_{N-1}(x) \\ \phi_0^{(1)}(x) & \phi_1^{(1)}(x) & \cdots & \phi_{N-1}^{(1)}(x) \\ \vdots & \ddots & \cdots & \\ \phi_0^{(N-1)}(x) & \phi_1^{(N-1)}(x) & \cdots & \phi_{N-1}^{(N-1)}(x) \end{bmatrix} \tag{1.1}$$

$$= \sum_{\sigma \in S_N} (-1)^{sgn(\sigma)} \phi_{\sigma(0)}^{(0)} \phi_{\sigma(1)}^{(1)} \cdots \phi_{\sigma(N-1)}^{(N-1)}, \tag{1.2}$$

where S_N is the set of permutations of the numbers 0 to $N-1$ and $sgn(\sigma)$ is ± 1 depending on whether the permutation σ is even or odd.

Let,

$$\begin{gathered} \deg\ \phi_0(x) = k_0 \\ \deg\ \phi_1(x) = k_1 \\ \vdots \\ \deg\ \phi_{N-1}(x) = k_{N-1} \\ \deg\ \phi_N(x) = k_N. \end{gathered}$$

Let α be a zero of the product $\phi_0 \cdots \phi_N$. By assumption (iii), we know that α is not a zero for some ϕ_i. Suppose without loss of generality that $\text{ord}_\alpha(\phi_N(x)) = 0$, if not, then will write

$$\phi_i = -\sum_{j \neq i} \phi_j \tag{1.3}$$

and substituting for the ith column in (1.1), we get an expansion, (1.2), with the ϕ_i replaced by ϕ_N. From (1.2)

$$\text{ord}_\alpha(W) \geq \min_{\sigma \in S_N} \{\text{ord}_\alpha(\phi_{\sigma(0)}^{(0)}(x)) + \text{ord}_\alpha(\phi_{\sigma(1)}^{(1)}(x)) + \cdots + \text{ord}_\alpha(\phi_{\sigma(N-1)}^{(N-1)}(x))\} =: R(\alpha).$$

Plainly,

$$
\begin{aligned}
R(\alpha) &\geq \min_{\sigma\in S_N}\{\mathrm{ord}_\alpha\,\phi_{\sigma(0)}(x) + (\mathrm{ord}_\alpha\,\phi_{\sigma(1)}(x)-1)+\cdots+(\mathrm{ord}_\alpha\,\phi_{\sigma(N-1)}(x)-(N-1))\}\\
&= \mathrm{ord}_\alpha(\phi_0(x)) + \mathrm{ord}_\alpha(\phi_1(x)) + \cdots + \mathrm{ord}_\alpha(\phi_{N-1}(x)) - 1 - 2 - \cdots - (N-1)\\
&= \mathrm{ord}_\alpha(\phi_0(x)) + \mathrm{ord}_\alpha(\phi_1(x)) + \cdots + \mathrm{ord}_\alpha(\phi_{N-1}(x)) + \mathrm{ord}_\alpha(\phi_N(x)) - \binom{N}{2}.
\end{aligned}
$$

Hence, summing over the α in $Z(\phi_0\phi_1\cdots\phi_N)$

$$
\begin{aligned}
\sum_{\alpha\in Z(\phi_0\cdots\phi_N)} \mathrm{ord}_\alpha(W) &\geq \sum_{\alpha\in Z(\phi_0\cdots\phi_N)} \mathrm{ord}_\alpha(\phi_0(x)) + \cdots + \sum_{\alpha\in Z(\phi_0\cdots\phi_N)} \mathrm{ord}_\alpha(\phi_N(x)) - \sum_{\alpha\in Z(\phi_0\cdots\phi_N)} \binom{N}{2}\\
&= k_0 + k_1 + \cdots + k_{N-1} + k_N - \binom{N}{2}|Z(\phi_0\phi_1\cdots\phi_N)|.
\end{aligned}
$$

By (ii) $W(x)$ is not the identically 0 polynomial. Hence by (1.2) then,

$$
\begin{aligned}
\sum_{\alpha\in Z(\phi_0\cdots\phi_N)} \mathrm{ord}_\alpha(W) &\leq \deg W\\
&\leq \max_{\sigma\in S_N}\{\deg\,\phi_{\sigma_{(0)}}(x) + \deg\,\phi_{\sigma(1)}(x) - 1 + \cdots + \deg\,\phi_{\sigma(N-1)}(x) - (N-1)\}\\
&= k_0 + k_1 + \cdots + k_{N-1} - \binom{N}{2}.
\end{aligned}
$$

Thus we have

$$
\binom{N}{2}(|Z(\phi_0\phi_1\cdots\phi_N)| - 1) \geq k_N.
$$

And thus we have proven the general form of Mason's Inequality. □

1.4 Stothers' Theorem

In 1981, W. W. Stothers [20] proved a similar result for a special case of Mason's Inequality. Below is Stothers' original theorem.

Theorem 1.4.1. *Suppose that $P(x)$ and $Q(x)$ are polynomials in $\mathbb{C}[x]$ such that*

(i) $P(x)$ and $Q(x)$ have the same positive degree,

(ii) $P(x)$ and $Q(x)$ have the same leading coefficient,

(iii) $P(x)$ and $Q(x)$ have no common zero.

Then

$$deg\ P \leq |Z(P)| + |Z(Q)| + |Z(P-Q)| - 1$$

Note: The proof below actually establishes a more general result where assumption (i) and (ii) are replaced with the assumption that $P(x)$, $Q(x)$ and $P(x) - Q(x)$ are not all constants. This will be a very short proof with the assumption of the Mason's Inequality.

Proof. We will write $R(x)$ as,

$$R(x) = P(x) - Q(x).$$

By Mason's Inequality we have,

$$\begin{aligned} \deg P &\leq \max\{\deg P, \deg Q, \deg R\} \\ &\leq |Z(PQR)| - 1 \\ &= |Z(P)| + |Z(Q)| + |Z(R)| - 1, \end{aligned}$$

since R, P, and Q have no common zeros. □

Observations: This specialized result was proven in three lines, so Mason's Inequality is a helpful tool when proving other like results. Now we will look how Mason's Inequality can prove Fermat's Last Theorem in just a few lines as well.

1.5 Fermat's Last Theorem for Polynomials

1.5.1 Fermat's Last Theorem for Polynomials

Using Mason's Inequality, we quickly can come up with a proof of the polynomial version of Fermat's Last Theorem.

Theorem 1.5.1. *There are no non-constant co-prime polynomials* $A(t), B(t)$ *and* $C(t) \in \mathbb{C}[t]$ *such that*

$$A(t)^N + B(t)^N = C(t)^N \tag{1.4}$$

when $N \geq 3$*.*

Note: If $A(t)$, $B(t)$, and $C(t)$ have a common divisor $d(t) = \gcd(A(t), B(t), C(t))$, then we can divide the gcd out of each term to get polynomials $\tilde{A}(t)$, $\tilde{B}(t)$, and $\tilde{C}(t)$ with no common factors satisfying (1.4).

Proof. Suppose that such polynomials $A(t)$, $B(t)$, and $C(t)$ exist. Apply Mason's Inequality to $A(t)^N$, $B(t)^N$, and $C(t)^N$.

Thus we have,

$$N \max\{\deg A, \deg B, \deg C\} \leq |Z(A^N B^N C^N)| - 1. \tag{1.5}$$

Recall that,

$$\begin{aligned} Z(A^N B^N C^N) &= \{\alpha \in \mathbb{C} : A(\alpha)^N B(\alpha)^N C(\alpha)^N = 0\} \\ &= \{\alpha \in \mathbb{C} : A(\alpha) B(\alpha) C(\alpha) = 0\}. \end{aligned}$$

Also we have,

$$|Z(ABC)| \leq \deg A + \deg B + \deg C \leq 3 \max\{\deg A, \deg B, \deg C\}. \tag{1.6}$$

Combining (1.5) and (1.6) we have,

$$N \max\{\deg\ A,\ \deg\ B,\ \deg\ C\} \leq 3 \max\{\ \deg A,\ \deg\ B,\ \deg\ C\} - 1$$

and thus for $N \geq 3$, we get a contradiction, thus completing our proof. □

Note: When $N = 1$ in (1.4) there are obviously infinitely many solutions, so we will now look at the special case where $N = 2$.

1.5.2 Special Case Where $N = 2$ for Polynomials

Theorem 1.5.2. *There exists infinitely many co-prime non-constant polynomial solutions of*

$$A(t)^2 + B(t)^2 = C(t)^2. \tag{1.7}$$

All the solutions are of the form,

$$A(t) = K(t)^2 - L(t)^2, \quad B(t) = 2K(t)L(t), \quad C(t) = K(t)^2 + L(t)^2,$$

for some $K(t), L(t) \in \mathbb{C}[t]$ *with* $\gcd(K(t), L(t)) = 1$.

Proof. Let $K(t)$ and $L(t) \in \mathbb{C}[t]$ where $\gcd(K(t), L(t)) = 1$. Suppose that
$A(t) = K(t)^2 - L(t)^2, \quad B(t) = 2K(t)L(t), \quad C(t) = K(t)^2 + L(t)^2.$

We want to show that $A(t)^2 + B(t)^2 = C(t)^2$ and $\gcd(A(t), B(t), C(t)) = 1$. Since $A(t)$, $B(t)$, and $C(t)$ satisfy (1.7), it is enough to check that $A(t)$ and $C(t)$ are co-prime.

$$\begin{aligned} A(t)^2 + B(t)^2 = (K(t)^2 - L(t)^2)^2 + (2K(t)L(t))^2 &= K(t)^4 - 2K(t)^2L(t)^2 + L(t)^4 + 4K(t)^2L(t)^2 \\ &= K(t)^4 + 2K(t)^2L(t)^2 + L(t)^4 = (K(t)^2 + L(t)^2)^2 = C(t)^2. \end{aligned}$$

Recall that $\mathbb{C}[t]$ is a Unique Factorization Domain, where primes take the form $p = (t - \alpha)$ and the units are the non-zero constants. Suppose $p \mid A(t)$ and $p \mid C(t)$ then $p \mid A(t)+C(t) = 2K(t)^2$ and $p \mid C(t) - A(t) = 2L(t)^2$, so $p \mid K(t)^2, p \mid L(t)^2$, which implies that $p \mid K(t), p \mid L(t)$, contradicting our assumption $\gcd(K(t), L(t)) = 1$. So $\gcd(A(t), B(t), C(t)) = 1$.

We'll see the other direction. Suppose that $A(t)^2+B(t)^2 = C(t)^2$ where $\gcd(A(t), B(t), C(t)) = 1$ and $A(t)$, $B(t)$, and $C(t) \in \mathbb{C}[t]$.

We want to show that $A(t) = K(t)^2 - L(t)^2, B(t) = 2K(t)L(t), C(t) = K(t)^2 + L(t)^2$ for some $K(t), L(t) \in \mathbb{C}[t]$ with $\gcd(K(t), L(t)) = 1$. From $A(t)^2 + B(t)^2 = C(t)^2$ we have,

$$\frac{B(t)^2}{4} = \frac{C(t)^2 - A(t)^2}{4} = \left(\frac{C(t) - A(t)}{2}\right)\left(\frac{C(t) + A(t)}{2}\right).$$

Factoring into primes,

$$\left(\frac{B(t)}{2}\right)^2 = p_1^{2m_1} \dots p_e^{2m_e} q_1^{2n_1} \dots q_f^{2n_f}$$

where the $p_j s$ divide $\frac{C(t)-A(t)}{2}$ and $q_i s$ divide $\frac{C(t)+A(t)}{2}$ are non-associate primes. To see that the p_j and q_i are not associates, we need to make an observation.

Observe that if p divided both $\frac{C(t)+A(t)}{2}$ and $\frac{C(t)-A(t)}{2}$, then we would have p divides both

$$C(t) = \frac{C(t) + A(t)}{2} + \frac{C(t) - A(t)}{2}, \qquad A(t) = \frac{C(t) + A(t)}{2} - \frac{C(t) - A(t)}{2}. \tag{1.8}$$

This gives us a contradiction since $\gcd(A(t), C(t)) = 1$. Given that the units are squares in $\mathbb{C}$, we can write by Unique Factorization that,

$$\frac{C(t) + A(t)}{2} = (up_1^{m_1} \cdots p_e^{m_e})^2 = K(t)^2$$
$$\frac{C(t) - A(t)}{2} = (u^{-1}q_1^{n_1} \cdots q_f^{n_f})^2 = L(t)^2.$$

Hence from (1.8),

$$C(t) = K(t)^2 + L(t)^2 \text{ and } A(t) = K(t)^2 - L(t)^2$$

and

$$B(t)^2 = C(t)^2 - A(t)^2 = 4K(t)^2L(t)^2$$

giving $B(t) = \pm 2K(t)L(t)$. Replacing $K(t)$ with $-K(t)$ if necessary, we can assume $B(t) = 2K(t)L(t)$. □

Observations: We saw that in order to have a solution of (1.4) with polynomials $A(t)$, $B(t)$, and $C(t)$ taken to the same power N, then $N < 3$. We also saw that there are infinitely many solutions with $N = 1$ and infinitely many solutions like Pythagorean Triples with $N = 2$ when working in $\mathbb{C}[x]$. It's fascinating to imagine that something as bold as the polynomial version of Fermat's Last Theorem could be proven in a couple of lines with just the assumption of Mason's Inequality. Next we will see how Mason's Inequality can be used to prove a more general version of Fermat's Last Theorem.

1.5.3 Generalized Fermat's Equation

Mason's Inequality can be used to tackle Fermat's Last Equation where the exponents are different.

Theorem 1.5.3. *There are no co-prime non-constant polynomial solutions to the generalized Fermat equation:*

$$A(t)^p + B(t)^q = C(t)^r \tag{1.9}$$

when

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq 1. \tag{1.10}$$

Proof. As before, by Mason's Inequality

$$\max\{p\deg A, q\deg B, r\deg C\} \leq |Z(A^pB^qC^r)| - 1 = |Z(ABC)| - 1. \tag{1.11}$$

By (1.10) we have

$$\begin{aligned}|Z(ABC)| &\leq \deg A + \deg B + \deg C\\ &= \frac{p\deg A}{p} + \frac{q\deg B}{q} + \frac{r\deg C}{r}\\ &\leq \left(\frac{1}{p} + \frac{1}{q} + \frac{1}{r}\right)\max\{p\deg A, q\deg B, r\deg C\}\\ &\leq \max\{p\deg A, q\deg B, r\deg C\}.\end{aligned}$$

Thus we obtain

$$\max\{p\deg A, q\deg B, r\deg C\} \leq \max\{p\deg A, q\deg B, r\deg C\} - 1, \tag{1.12}$$

a contradiction.

□

Chapter 2

The ABC Conjecture

We now consider the integer version of the ABC Conjecture.

2.1 ABC Introduction

We will begin by looking at the analogue for $Z(F)$ and $\deg F$ for integers and see what Mason's Inequality suggests for the ABC Conjecture in the integer case.

2.1.1 Using Mason's Inequality to Motivate ABC-Conjecture

Recall for a polynomial

$$F(x) = a_N(x-\alpha_1)^{e_1}(x-\alpha_2)^{e_2}\cdots(x-\alpha_n)^{e_n}, \tag{2.1}$$

where $\alpha_1, \alpha_2, \cdots, \alpha_n \in \mathbb{C}[x]$ are distinct roots, that we define $\mathrm{ord}_\alpha(F)$ to be the power of $(x-\alpha)$ in the factorization of F

$$\mathrm{ord}_\alpha(F) = \begin{cases} M, & \text{if } (x-\alpha)^M \parallel F, \text{ i.e. } (x-\alpha)^M \mid F \text{ and } (x-\alpha)^{M+1} \nmid F; \\ 0, & \text{if } (x-\alpha) \nmid F, \end{cases} \tag{2.2}$$

and have

$$\sum_{\alpha \in \mathbb{C}} \text{ord}_\alpha(F) = \text{ deg } F. \tag{2.3}$$

Now let A be a nonzero integer. Analogous to (2.1) we can factor A into primes

$$A = \pm p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}, \tag{2.4}$$

with the $p_i s$ for $1 \leq i \leq n$ being distinct primes to positive integer powers. Thus for each distinct prime, we define ord as

$$\text{ord}_p(A) = \begin{cases} e, & \text{if } p^e \parallel A, \text{ i.e. } p^e \mid A \text{ and } p^{e+1} \nmid A; \\ 0, & \text{if } p \text{ is not a prime factor of A,} \end{cases} \tag{2.5}$$

which is the analogue to (2.2). Similar to (2.3) we have,

$$\sum_p \text{ord}_p(A) \log p = \log |A|. \tag{2.6}$$

To see this,

$$\text{ord}_{p_i}(A) = e_i \text{ for primes } p_i \mid A, 1 \leq i \leq n \text{ and}$$

$$\text{ord}_p(A) = 0 \text{ for primes } p \nmid A.$$

Thus we have,

$$\sum_p \text{ord}_p(A) \log p = \sum_{i=0}^{n} e_i \log p_i = \sum_{i=0}^{n} \log p_i^{e_i} = \log p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} = \log |A|.$$

Recall for a polynomial we had

$$|Z(F)| = \text{ deg}\{(x - \alpha_1) \cdots (x - \alpha_N)\}.$$

The analogue for A is called the radical. We define the radical to be the product of the distinct prime factors of A.

$$\text{Rad } (A) = p_1 p_2 \cdots p_n \tag{2.7}$$

In Mason's Inequality, we had no ϵ in the exponent. A natural first thought is to get rid of the ϵ. Will getting rid of the ϵ work?

Suppose that A, B, and C, be integers such that

(i) $A + B = C$

(ii) $A,\ B,$ and C are each nonzero

(iii) $A,\ B,$ and C have no common prime factor.

For the case of polynomials we had

$$\max\{\deg\ A,\ \deg\ B,\ \deg\ C\} < |Z(ABC)|.$$

So we might conjecture the analogue

$$\max\{|A|, |B|, |C|\} < |\mathrm{Rad}(ABC)|. \tag{2.8}$$

However, (2.8) would be false; let's consider

$$1 + 2^3 = 3^2,$$

then (2.8) would have $9 < 6$;

$$3^3 + 5 = 2^5,$$

would have have $32 < 30$;

$$2^5 + 7^2 = 3^4,$$

would have $81 < 42$ and

$$1 + 2^9 = 3^3 \times 19,$$

would have $513 < 114$. Thus (2.8) cannot hold.

Question: Could we modify the inequality with a constant? That is, does there exists a positive constant K such that,

$$\max\{|A|,|B|,|C|\} \leq K\mathrm{Rad}(ABC) \tag{2.9}$$

Unfortunately this cannot hold.

Proof. We will proceed using proof by contradiction.

Let q be a large prime, and

$$A = 1,\ B = 2^{q(q-1)} - 1,\ C = 2^{q(q-1)}.$$

By Euler's Theorem, we have $a^{\phi(q^2)} \equiv 1 \bmod q^2$ for $(a,q) = 1$ where $\phi(q^2) = q(q-1)$.

Hence for odd primes q,

$$2^{q(q-1)} \equiv 1\ \mathrm{mod} q^2$$

and thus,

$$B \equiv 0\ \mathrm{mod} q^2$$

giving

$$q^2 \mid B.$$

Thus we get,

$$\prod_{p|ABC} p \leq \frac{2(2^{q(q-1)} - 1)}{q}.$$

Thus for (2.9) to hold true, we have a constant K that must satisfy

$$2^{q(q-1)} \leq K\left(\frac{2(2^{q(q-1)} - 1)}{q}\right)$$

for all primes q, which is false for suitably large q.

□

We will look at what is needed in the ABC Conjecture in the next section.

2.2 ABCConjecture

In 1988, the following modification of Mason's Inequality was formulated by Masser [12] (a refined version of the conjecture first formulated by Oesterlé [14]).

Theorem 2.2.1. *Suppose that A, B, and C are integers satisfying*

(i) $A + B = C$

(ii) *A, B and C are each nonzero,*

(iii) *A, B and C have no common prime factor.*

Then for every $\epsilon > 0$ there exists a constant $K(\epsilon) > 0$ such that,

$$\max\{|A|, |B|, |C|\} \leq K(\epsilon) Rad(ABC)^{1+\epsilon}. \tag{2.10}$$

2.3 Explicit Forms

In this section we will talk about explicit forms of the ABC Conjecture. First, we will define *ABC-triple* as a triple (A, B, C) with A, B, C being positive co-prime integers that satisfy $A + B = C$ with $A < B$. $(1, 2, 3)$ would be the smallest example of an ABC-triple. Second, we will define *ABC-hit* as an ABC-triple that satisfy $\mathrm{Rad}(ABC) < C$. Looking at $(1, 8, 9)$, we can see that is an ABC-hit since $1 + 8 = 9, \gcd(1, 8, 9) = 1$ and

$$\mathrm{Rad}(1 \cdot 8 \cdot 9) = \mathrm{Rad}(1 \cdot 2^3 \cdot 3^2) = 2 \cdot 3 = 6 < 9.$$

Out of the known $15 \cdot 10^6$ ABC-triples with $C < 10^4$, there exists 120 ABC-hits.

Theorem 2.3.1. *There exists infinitely many ABC-hits.*

Lemma 2.3.1. *For any $k \in \mathbb{N}$, we have $2^{k=2} \mid 3^{2^k} - 1$.*

Proof. By induction on k, let $k \geq 1, A = 1, C = 3^{2^k}, B = C - 1$.

Note: we saw the base case $k = 1$ with $A = 1, C = 3^2 = 9, B = 3^2 - 1 = 8$. We see that $2^{1+2} \mid 3^{2^1} - 1 = B$. Now we will do the induction case.

Suppose we have $A, B,$ and C such that $A = 1, B = 3^{2^n} - 1, C = 3^{2^n}$ for $1 \leq n \leq k$ with $2^{n+2} \mid (3^{2^n} - 1)$. We want to show that $A = 1, B = 3^{2^{n+1}} - 1, C = 3^{2^{n+1}}$ with $2^{n+3} \mid 3^{2^{n+1}} - 1$.

$$3^{2^{n+1}} - 1 = 3^{2^n 2} - 1 = (3^{2^n})^2 - (1)^2 = (3^{2^n} - 1)(3^{2^n} + 1),$$

thus by our assumption we have $2^{n+2} \mid (3^{2^n} - 1)$ and we know at least $2 \mid (3^{2^n} + 1)$, since $3^{2^n} - 1$ is even. Is there more than one power of 2 that divides $3^{2^n} + 1$? No, since $3^{2^n} - 1$ has an even number multiplying 2, so $3^{2^n} + 1$ will have an odd number multiplying 2. Thus we have $2^{n+3} \mid 3^{2^{n+1}} - 1$. and so we showed $2^{k+2} \mid 3^{2^k} - 1$ by induction. □

Now having proved Lemma 2.3, we can prove Theorem 2.3.

Proof. We have for any $k \in \mathbb{N}$,

$$\text{Rad}\left(\left(3^{2^k} - 1\right) \cdot 3^{2^k}\right) \leq \frac{3^{2^k} - 1}{2^{k+1}} \cdot 3 < 3^{2^k}.$$

Thus,

$$(1, 3^{2^k} - 1, 3^{2^k})$$

is an ABC-hit. So there are infinitely many ABC-hits. □

Lemma 2.3.2. *There exists infinitely many ABC-triples (A, B, C) such that*

$$C > \frac{1}{6 \log 3} R \log R$$

where $R = Rad(ABC)$.

It is unknown, whether there exists a ABC-triple (A, B, C) such that $C > \mathrm{Rad}(ABC)^2$. Reyssat's example with

$$A = 2, B = 3^{10} \cdot 109 = 6,436,341, C = 23^5 = 6,436,343,$$

gives the largest known value of λ that satisfies $C > \mathrm{Rad}(ABC)^{\lambda}$ for an existing ABC-triple (A, B, C). We see that $\lambda = 1.62991 \cdots$.

Now we check,

$$2 + 3^{10} \cdot 109 = 23^5, \mathrm{Rad}(2 \cdot 3^{10} \cdot 109 \cdot 23^5) = 2 \cdot 3 \cdot 23 \cdot 109 = 15,042.$$

Next we define the logarithmic radical of an ABC-triple,

$$\lambda(A, B, C) = \frac{\log C}{\log \mathrm{Rad}(ABC)},$$

and observe that $C = \mathrm{Rad}(ABC)^{\lambda(A,B,C)}$. Plugging in the A, B, C values of Reyssat's example, we get

$$\lambda(2, 3^{10} \cdot 109, 23^5) = \frac{\log 6,436,343}{\log 15,042} = 1.62991 \cdots .$$

Besides Reyssat's example, Benne de Weger found the next largest $\lambda(A, B, C)$, with its value being $1.625990 \cdots$ with

$$A = 11^2, B = 3^2 \cdot 5^6 \cdot 7^3 = 48,234,375, C = 2^{21} \cdot 23 = 48,234,496.$$

We can see that

$$11^2 + 3^2 \cdot 5^6 \cdot 7^3 = 2621 \cdot 23, \mathrm{Rad}(2^{21} \cdot 3^2 \cdot 5^6 \cdot 7^3 \cdot 11^2 \cdot 23) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 53,130.$$

Thus we see that $\lambda(11^2, 3^2 \cdot 5^6 \cdot 7^3, 2^{21} \cdot 23) = \frac{\log 48,234,496}{\log 53,130} = 1.625990 \cdots$.

Now we will look at an explicit form of the ABC Conjecture. In 1996, Alan Baker [1] suggested the following statement.

Conjecture 2.3.1. *Let (A, B, C) be an ABC-triple and let $\epsilon > 0$. Then*

$$C \leq K \left(\epsilon^{-\omega} R\right)^{1+\epsilon}$$

where K is an absolute constant, $R = Rad(ABC)$ and $\omega = \omega(ABC)$ is the number of distinct prime factors of ABC.

This was revised by A. Baker [2] when A. Granville found that the minimum of the right hand side occurs when $\epsilon = \frac{\omega}{\log R}$. Baker honed the previous conjecture to where

$$C \leq KR\frac{(\log R)^{\omega}}{\omega!}.$$

Then after some experimental calculations, Baker was able to come with a value for the absolute constant K, thus giving us an explicit version of the ABC-Conjecture.

Conjecture 2.3.2. *Let (A, B, C) be an ABC-triple and let $\epsilon > 0$. Then*

$$C \leq \frac{6}{5}R\frac{(\log R)^{\omega}}{\omega!},$$

where $R = Rad(ABC)$ and $\omega = \omega(ABC)$ is the number of distinct prime factors of ABC.

Thus from 2.3, we can deduce

$$C < \mathrm{Rad}(ABC)^{\frac{7}{4}}.$$

In the next section, we will see proven results.

2.4 What We Can Prove

In this section we will talk about the proven results of Stewart and Tijdeman and Stewart and Yu. In 1986, Stewart and Tijdeman [17] came up with this proven result that for $A + B = C$, $\gcd(A, B, C) = 1$, we have

$$C < \exp\left(k_1 \cdot R^{15}\right)$$

where k_1 is a positive constant and $R = \text{Rad}(ABC)$.

This was later refined by Stewart and Yu in 1991 [18] for positive integers $A, B,$ and C, with $C > 2$ to

$$C < \exp\left(R^{\frac{2}{3}+\frac{k_2}{\log\log R}}\right)$$

where k_2 is a positive constant and $R = \text{Rad}(ABC)$.

In their 2001 paper, Stewart and Yu worked on presenting two further improvements and came up with two theorems. If one would like to see the proof, one could look at their paper [19] and see the extensive proof. Here is their second theorem, which we will use later.

Theorem 2.4.1. *There exists an effectively computable positive number K such that, for all positive integers A, B and C with $A + B = C$ and $\gcd(A, B, C) = 1$,*

$$C < exp\left(KR^{\frac{1}{3}}(\log R)^3\right),$$

where $R = Rad(ABC)$.

In their new proof, Stewart and Yu utilize the "p-adic linear forms in the logarithms of algebraic numbers." Stewart and Yu look at the p-adic order of $A, B,$ and C with p running through the small primes that divide $A, B,$ and C. They refine their first theorem through the focus on the dependence on the parameter p, with the p-adic estimates. Denoting

$p_A, p_B,$ and p_C as the largest prime factor that divides $A, B,$ and C respectively. One can say that 1 is the largest "prime" factor of 1. One will define the smallest of these primes as

$$p' := \min\{p_A, p_B, p_C\}.$$

Now one will denote $\log_i$ as the ith iteration of log, i.e. $\log_1 x = \log x$ and $\log_i x = \log\log_{i-1} x$ for $i = 2, 3\cdots$.

Improving on their first theorem, Stewart and Yu came up with their second theorem.

Theorem 2.4.2. *There exists an effectively computable positive number K such that, for all positive integers A, B and C with $A + B = C$, $\gcd(A, B, C) = 1$, and $C > 2$,*

$$C < exp\left(p' R^{K \log_3 R_* / \log_2 R}\right),$$

where $R_* = \max\{R, 16\}$.

One could deduce from 2.4 that for every $\epsilon > 0$, there exists a constant $K_3(\epsilon)$ that depends on ϵ, which can be computed, such that for all positive integers $A, B,$ and C with $A + B = C, \gcd(A, B, C) = 1$,

$$C < \exp\left(p' K_3 R^{\epsilon}\right).$$

Notice that,

$$p' \leq (p_A p_B p_C)^{\frac{1}{3}} \leq R^{\frac{1}{3}},$$

and thus we get

$$\exp\left(K_3 R^{\frac{1}{3}+\epsilon}\right).$$

We will use this weaker result in one of the applications in a later chapter.

2.5 Fermat's Last Theorem for Integers

2.5.1 Using ABC to Prove Fermat's Last Theorem

We used Mason's Inequality to prove the polynomial version of Fermat's Last Theorem. We will use the explicit version (Bakers-Explicit) of the ABC Conjecture (2.10) with $\epsilon = \frac{3}{4}, K(\frac{3}{4}) = 1$, that is

$$\max\{|A|, |B|, |C|\} \leq \mathrm{Rad}(ABC)^{\frac{7}{4}}, \tag{2.11}$$

to prove the integer version of Fermat's Last Theorem at least for exponent $N \geq 6$. The smaller cases $N = 3, 4, 5$ were proved by the nineteenth century.

Just like for the polynomials, we can also use the ABC Conjecture to prove the general Fermat Last's Theorem, as we see in Section 2.5.3.

Theorem 2.5.1. *There are no co-prime integers A, B, and C such that*

$$A^N + B^N = C^N \tag{2.12}$$

when $N \geq 6$.

Proof. Suppose A, B, and C are co-prime integers satisfying $A^N + B^N = C^N$. By (2.11) we have,

$$\begin{aligned} \max\{|A|^N, |B|^N, |C|^N\} &\leq \mathrm{Rad}(ABC)^{\frac{7}{4}} \\ &\leq |ABC|^{\frac{7}{4}} \\ &\leq \max\{|A|, |B|, |C|\}^{\frac{21}{4}} \end{aligned}$$

If we have $N \geq 6$, we will have a contradiction, thus proving 2.5.1. □

In the next section is the proof of the existence of infinitely many solutions of (2.12) in the case where $N = 2$, the Pythagorean triples. Fermat was able to prove the $N = 4$ case using the method of infinite descent. Euler proved the $N = 3$ case in this mid 18th century and published it in *Algebra* (1770) with a gap in the proof filled by Legendre. In the early 1800's, the next big accomplishment came when Sophie Germain made progress on the $N = 5$ case. Legendre improved on Germain's results and in 1825 published his proof as did Dirichlet independently. See for example the survey article [10].

2.5.2 Special Case $N = 2$

Theorem 2.5.2. *There exists infinitely many co-prime integer solutions satisfying*

$$A^2 + B^2 = C^2, \tag{2.13}$$

where all the solutions are of the form,

$$A = K^2 - L^2, \qquad B = 2KL, \qquad C = \pm(K^2 + L^2)$$

for some integers of opposite parity K,L with $\gcd(K, L) = 1$*.*

Proof. Suppose A, B, and C satisfy are of the form $A = K^2 - L^2$, $B = 2KL$, $C = \pm(K^2 + L^2)$ for some K, L of opposite parity with $\gcd(K, L) = 1$.
Straight away, we can see that A and C are odd and B is even.

We need to show that $A^2 + B^2 = C^2$ and $\gcd(A, B, C) = 1$.

$A^2+B^2 = (K^2-L^2)^2+(2KL)^2 = K^4-2K^2L^2+L^2+4K^2L^2 = K^4+2K^2L^2+L^4 = (K^2+L^2)^2 = C^2$.

Suppose there exists a prime p, such that $p \mid A$ and $p \mid C$, then $p \mid C - A = K^2 + L^2 - (K^2 - L^2) = 2L^2, p \mid C + A = K^2 + L^2 + K^2 - L^2 = 2K^2$. We know $p \neq 2$ since A and C are odd, so $p \mid L^2, K^2$, so $p \mid K, L$. Thus we have a contradiction since $\gcd(K, L) = 1$.

For the converse, suppose that A, B, and C are co-prime integers satisfying (2.13).
Claim: A, B, and C take the form of $A = K^2 - L^2$, $B = 2KL$, $C = \pm(K^2 + L^2)$ for

some K, L. Note that the K, L must be of opposite parity, otherwise A, B and C would all be even. Also $d = \gcd(K, L)$ must equal 1, otherwise $d^2 \mid A, B, C$, contradicting our assumption that $\gcd(A, B, C) = 1$.

Observe, one of A, B is even and the other odd. If both are odd then $A^2 + B^2 \equiv 1 + 1 \bmod 4$, but $C^2 \equiv 0, 1 \bmod 4$. Thus without loss of generality, let B be even and A be odd. So, $A^2 + B^2 = C^2$ implies that

$$\left(\frac{B}{2}\right)^2 = \frac{C^2 - A^2}{4} = \left(\frac{C - A}{2}\right)\left(\frac{C + A}{2}\right)$$

Factoring $\frac{B}{2}$ into primes, we have $\frac{B}{2}^2 = p_1^{2m_1} \dots p_e^{2m_e} q_1^{2n_1} \dots q_f^{2n_f}$, where the $p_j s$ divide $\dfrac{C - A}{2}$ and $q_i s$ divide $\dfrac{C + A}{2}$ are distinct primes. To see that the p_j and q_i are distinct, we need to make an observation.

Observe that if p divided both, then we would have $p \mid \dfrac{C + A}{2}$ and $p \mid \dfrac{C - A}{2} \Rightarrow p \mid A, C$. This gives us a contradiction since $\gcd(A, C) = 1$.

Since $\mathbb{Z}$ is a unique factorization domain, we can write

$$\begin{aligned} \frac{C + A}{2} &= u(p_1^{m_1} \cdots p_e^{m_e})^2 = uK^2 \\ \frac{C - A}{2} &= u^{-1}(q_1^{n_1} \cdots q_f^{n_f})^2 = uL^2, \end{aligned}$$

where u is a unit, i.e. $u = \pm 1$ and so $u = u^{-1}$. Hence,

$$A = \left(\frac{C + A}{2}\right) - \left(\frac{C - A}{2}\right) = u(K^2 - L^2), \quad C = \left(\frac{C + A}{2}\right) + \left(\frac{C - A}{2}\right) = u(K^2 - L^2)$$

, and $B^2 = C^2 - A^2 = 4K^2L^2$ giving us $B = \pm 2KL$. If necessary we could take K to be $-K$ or we can switch K and L, so we have what we claimed with $A = K^2 - L^2$, $B = 2KL$, $C = \pm(K^2 + L^2)$. □

Thus we have shown the Pythagorean Triples in the case of $N = 2$. Now we will look at the generalized integer version of Fermat's Equation.

2.5.3 Generalized Fermat's Equation

In this section we will look at the generalized integer version of Fermat's Equation.

Theorem 2.5.3. *There exists only finitely many co-prime solutions a, b, c to*

$$a^p + b^q = c^r \tag{2.14}$$

when

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1.$$

We make the following observation

Lemma 2.5.1. *If p, q, r are positive integers with*

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1,$$

then

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq \frac{41}{42}.$$

Proof. Suppose $p \leq q \leq r$, we'll attack these by cases.

If $p \geq 3$ and $(p, q, r) \neq (3, 3, 3)$ (otherwise we have 1) then,

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq \frac{1}{3} + \frac{1}{3} + \frac{1}{4} = \frac{11}{12}.$$

So suppose $p = 2$. If $q = 2$ then,

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} = \frac{1}{2} + \frac{1}{2} + \frac{1}{r} > 1,$$

but that gives a contradiction, so $q \geq 3$.

If $q = 3$ then,

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq \frac{1}{2} + \frac{1}{3} + \frac{1}{r} = \frac{1}{r} + \frac{5}{6}.$$

Thus $r \geq 7$ and we have

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq \frac{1}{7} + \frac{5}{6} = \frac{41}{42}.$$

If $q = 4$ then,

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq \frac{1}{2} + \frac{1}{4} + \frac{1}{r} = \frac{1}{r} + \frac{3}{4}.$$

Thus $r \geq 5$ and we have

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq \frac{1}{2} + \frac{1}{4} + \frac{1}{5} = \frac{1}{5} + \frac{3}{4} = \frac{19}{20}.$$

If $q \geq 5$ then,

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq \frac{1}{2} + \frac{1}{5} + \frac{1}{5} = \frac{9}{10}.$$

So we have proven that if $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$ then $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq \frac{41}{42}$. □

Now we will prove Theorem 2.5.3.

Proof. Applying the ABC Conjecture, we get

$$\begin{aligned} \max\{a^p, b^q, c^r\} &\leq K(\epsilon)\text{Rad}(abc)^{1+\epsilon} \\ &= K(\epsilon)\text{Rad}((a^p)^{\frac{1}{p}}(b^q)^{\frac{1}{q}}(c^r)^{\frac{1}{r}})^{1+\epsilon} \\ &\leq K(\epsilon)\max\{a^p, b^q, c^r\}^{(\frac{1}{p}+\frac{1}{q}+\frac{1}{r})(1+\epsilon)} \\ &\leq K(\epsilon)\max\{a^p, b^q, c^r\}^{\frac{41}{42}(1+\epsilon)}, \end{aligned}$$

and so we have,

$$\max\{a^p, b^q, c^r\}^{\frac{1}{42} - \frac{41\epsilon}{42}} \leq K(\epsilon).$$

Thus take $\epsilon < \frac{1}{41}$ we have a finite bound, $K(\epsilon)^{\frac{42}{1-41\epsilon}}$, for a^p, b^q, and c^r. □

When $\frac{1}{p}+\frac{1}{q}+\frac{1}{r}<1$, we have only 10 known solutions (a,b,c,p,q,r) to (2.14) with a, b, and c being relatively prime. In increasing order for c^r, we have:

$$1+2^3=3^2,\ 2^5+7^2=3^4,\ 7^3+13^2=2^9,\ 2^7+17^3=71^2$$
$$3^5+11^4=122^2,\ 33^8+1,549,034^2=15,613^3$$
$$1,414^3+2,213,459^2,\ 9,262^3+15,312,283^2=113^7,$$
$$17^7+76,271^3=21,063,928^2,\ 43^8+96,222^3=30,042,907^2.$$

What about for $\frac{1}{p}+\frac{1}{q}+\frac{1}{r}\geq 1$?

If $\frac{1}{p}+\frac{1}{q}+\frac{1}{r}\geq 1$ then (p,q,r) is a permutation of one of the following

$$(2,2,k) \text{ for } k\geq 2, (2,3,3), (2,3,4), (2,3,5), (2,3,6), (2,4,4), (3,3,3) \tag{2.15}$$

where in each of these cases, all the solutions of (a,b,c) are known, often being infinitely many of them as stated in the Waldschmidt paper [22].

Observations: Andy Beal made a conjecture that, assuming $\frac{1}{p}+\frac{1}{q}+\frac{1}{r}<1$, there's no solution to (2.14) with $p,q,r>2$. There is now \$ 1,000,000 prize money if someone can find another solution (other than the 10 given above) to (2.14) with $p,q,r>2$ or prove that there are no more solutions. One would think there would be no solutions with $p,q,r>2$, $p,q,r\in\mathbb{Z}$ as shown through the polynomial version of General Fermat Equation. We have seen the proof of Fermat's General Equation through Mason's Inequality and the proof of the integer version through the use of the ABC Conjecture. It's fascinating how deep the ABC Conjecture really can be. In the next section, we will look at the explicit form of the ABC Conjecture.

Chapter 3

Applications of ABC Conjecture

3.1 Introduction

In the previous chapter, we looked at the ABC Conjecture, explicit forms of the ABC Conjecture, and what we can prove from the ABC Conjecture. Now, we will look at applications that the ABC conjecture has to offer, which include Wieferich primes, gaps between primes, Erdős-Woods Conjecture, Roth's Theorem, Mordell's Conjecture (Faltings' Theorem), and Baker's Theorem.

3.2 Wieferich Primes

Recall that for any odd prime p, we have by Fermat's Little Theorem

$$2^{p-1} \equiv 1 \bmod p.$$

We call a prime p Wieferich if,

$$2^{p-1} \equiv 1 \bmod p^2. \tag{3.1}$$

The only known Wieferich primes are 1093 and 3511. As of November 2015, the PrimeGrid project search has shown that there are no others less than 4.9×10^{17}. It is conjectured that there are infinitely many Wieferich primes. Here we will show that the ABC Conjecture implies that there are infinitely many non-Wieferich primes.

Theorem 3.2.1. *Assume ABC Conjecture with* $0 < \epsilon < 1$ *and define*

$$U = \{p : 2^{p-1} \not\equiv 1 \mod p^2\}$$

where p *is an odd prime. Then* U *is an infinite set.*

Proof. Let's assume the U is a finite set, and define the set

$$V = \{p : 2^{p-1} \equiv 1 \mod p^2\}.$$

Let n be a large positive integer, not divisible by any prime in U.

We write,

$$2^n - 1 = U_n V_n$$

where the primes divisors of U_n are contained in U, and the prime divisors of V_n are contained in V.

We want to show that

$$\text{if } p \mid U_n, \text{ then } p^2 \nmid U_n, \tag{3.2}$$

$$\text{if } p \mid V_n, \text{ then } p^2 \mid V_n. \tag{3.3}$$

Let $m = \mathrm{ord}_p(2)$ and $N = \mathrm{ord}_{p^2}(2)$. So

$$2^m = 1 + \lambda p$$

giving

$$\begin{aligned} 2^{mp} &= (1 + \lambda p)^p \\ &= 1 + \lambda p^2 + \lambda p^2(\cdots) \equiv 1 \bmod p^2 \end{aligned}$$

and $N \mid mp$. Since

$$2^N \equiv 1 \bmod p^2 \Rightarrow 2^N \equiv 1 \bmod p,$$

we have $m \mid N$. Thus $N = m$ or $N = mp$.

Suppose $p \mid U_n$. If $N = m$ then, $m \mid p - 1$ implies that $N \mid p - 1$ and $2^{p-1} \equiv 1 \bmod p^2$.

But, this gives us a contradiction since $2^{p-1} \not\equiv 1 \bmod p^2$ since p is in U.

So we assume $N = mp$, but $p \nmid n \Rightarrow N \nmid n \Rightarrow 2^n \not\equiv 1 \bmod p^2$.

Thus we have shown (3.2) holds.

Suppose $p \mid V_n$. Then $2^{p-1} \equiv 1 \bmod p^2$ since primes in V_n are contained in V.

Therefore, $N \mid p - 1$ and so $p \nmid N$ and $N = m$ and so $p \mid 2^n - 1$ implies $m \mid n$ so $N \mid n$ and so $p^2 \mid 2^n - 1$.

Recall the definition of radical as product of prime factors. Since U is a finite set, we define a constant

$$L := \prod_{p \in U} p.$$

Following from (3.2), we have

$$U_n = \prod_{p \mid U_n} p \leq L.$$

Also following from (3.3), we have

$$\mathrm{Rad}(V_n) \leq (V_n)^{\frac{1}{2}}$$

Applying the ABC Conjecture to

$$(2^n - 1) + 1 = 2^n$$

we see that

$$\begin{aligned} V_n &\leq U_n V_n + 1 \\ &= 2^n \\ &\leq K(\epsilon)\mathrm{Rad}(2^n U_n V_n)^{1+\epsilon} \\ &\leq K(\epsilon)\mathrm{Rad}(V_n)^{1+\epsilon}\mathrm{Rad}(2U_n)^2 \\ &\leq 4K(\epsilon)L^2(V_n)^{\frac{1+\epsilon}{2}}, \end{aligned}$$

implying that $V_n \leq (4K(\epsilon)L^2)^{\frac{2}{1-\epsilon}}$ is bounded in n. However, V_n is unbounded since $2^n - 1 = U_n V_n$ is unbounded and U_n is bounded. Thus we have a contradiction. Thus U is infinite. □

Observations: We know that there are infinitely many primes, so what about infinitely many primes with a certain property or that lack a certain property. We will see this by looking at this application with the Wieferich primes, p, of the form $V = \{p : 2^{p-1} \equiv 1 \bmod p^2\}$ and non Wieferich primes, p, of the form $U = \{p : 2^{p-1} \not\equiv 1 \bmod p^2\}$. We see that the ABC conjecture shows us there are infinitely many non Wieferich primes. We expect that most primes are going to be non Wieferich primes, so the result is not surprising, but are there infinitely many Wieferich primes? There are no other known way to prove infinitely many non Wieferich primes, so that gives the ABC Conjecture added proof of how deep a result it is in Number Theory.

3.3 Gaps Between Primes (Cochrane and Dressler)

3.3.1 Introduction

Cochrane and Dressler [4] made several conjectures about gaps between integers having the same prime factors. We will look at some properties that can be proven by the ABC Conjecture.

Conjecture 3.3.1. *Between any two positive integers having the same prime factors there is a prime.*

Conjecture 3.3.2. *For any $\epsilon > 0$ there exists a constant $C(\epsilon)$ such that if $a < c$ are positive integers having the same prime factors, then*

$$c - a \geq C(\epsilon)a^{\frac{1}{2}-\epsilon}. \tag{3.4}$$

One observation that we can make is that one can see that Conjecture 3.3.1 follows from Conjecture 3.3.2 assuming Cramér's Conjecture for prime spacing, since $\log^2 n \ll n^{\frac{1}{2}-\epsilon}$. Cramér's conjecture is that the gap $p_{n+1} - p_n$ between two consecutive primes p_n and p_{n+1} is $\mathcal{O}(\log^2 p_n)$. Assuming Riemann's Hypothesis, Cramér [5] showed that a prime exists between n and $n + \mathcal{O}(n^{\frac{1}{2}} \log n)$, but this is not quite good enough to obtain Conjecture 3.3.1 from Conjecture 3.3.2.

Conjecture 3.3.2 can be tackled using the ABC Conjecture.

Theorem 3.3.1. *The ABC Conjecture implies Conjecture 3.3.2.*

Cochrane and Dressler used the 1991 Stewart and Yu's result to get:

If $a < c$ are positive integers having the same prime factors, then

$$c - a \geq C(\epsilon)(\log c)^{\frac{3}{4}-\epsilon}. \tag{3.5}$$

We will improve their result by using the improved Stewart and Yu's result from 2001.

Theorem 3.3.2. *If $a < c$ are positive integers having the same prime factors, then*

$$c - a \geq C(\epsilon)(\log c)^{\frac{3}{2}-\epsilon}. \tag{3.6}$$

Cochrane and Dressler state "If the prime factors of a and c are restricted to a fixed finite set S of prime, then we have the much stronger lower bound"

$$c - a > \frac{a}{(\log a)^C}. \tag{3.7}$$

where the constant C depends on S.

How good is the bound? Can we replace $\frac{1}{2} - \epsilon$ by $\frac{1}{2}$? In the example below given in the Cochrane and Dressler paper, we see that the exponent in (3.4) cannot be exactly $\frac{1}{2}$. In their findings they found an infinite family of pairs of positive integers $a < c$ containing the same prime factors and satisfying,

$$c - a \leq 2\sqrt{2\log 2}\frac{a^{\frac{1}{2}}}{(\log a)^{\frac{1}{2}}}. \tag{3.8}$$

Below the example is stated exactly as it is in the Cochrane and Dressler paper.

Example Let k be any positive integer and define a_1, c_1 by

$$a_1 = 2(2^k - 1)^2, \text{ and } c_1 = 2^{k+1}(2^k - 1).$$

Then c_1, a_1 have the same prime divisors and $c_1 - a_1 = \sqrt{2}a_1^{\frac{1}{2}}$. Suppose that $k = 2 \times 3^{j-1}$, where $j \geq 2$ is a positive integer. Then we have $3^j \mid (2^k - 1)$ and so we can divide a_1 and c_1 by 3^{j-1} and end up with two smaller numbers

$$a = \frac{2(2^k-1)^2}{3^{j-1}}, \text{ and } c = \frac{2^{k+1}(2^k-1)}{3^{j-1}}$$

having the same prime factors and satisfying

$$c - a = \frac{\sqrt{2}}{3^{\frac{j-1}{2}}}a^{\frac{1}{2}} = \frac{2}{\sqrt{k}}a^{\frac{1}{2}}.$$

Now,

$$\log a = \log 2 + 2\log(2^k - 1) - (j-1)\log 3 < 2k \log 2$$

that is, $k > \log a/(2\log 2)$, i.e. $c - a \leq \frac{2\sqrt{2\log 2}a^{\frac{1}{2}}}{(\log a)^{\frac{1}{2}}}$ and thus we obtain (3.8).

Observation: The example helps us to clarify why we have $a^{\frac{1}{2}-\epsilon}$ in Conjecture 2. It is also noted in the Cochrane and Dressler paper that "similar examples may be obtained by dividing out other prime powers or replacing $(2^k - 1)$ with $(2^k + 1)$, or by replacing 2 with any other positive integer $m > 1$." They could not find any examples where the order of magnitude was less than what they've found in (3.8).

Note: According to Cochrane and Dressler, if a and c have only two prime divisors in common, then one can take the exponent in (3.4) to be exactly $\frac{1}{2}$ on the assumption of the ABC Conjecture. Thus we have,

Theorem 3.3.3. *Suppose that $a < c$ are positive integers having the same two prime divisors. Then, on the assumption of the ABC Conjecture, $c - a \gg a^{\frac{1}{2}}$.*

3.3.2 ABC and Gaps

In this section we will prove the first theorem in the Cochrane and Dressler paper.

Recall, $Rad(a) = p_1 \cdots p_n$, where the $p_i s$ are the distinct primes in the factorization of A and recall the ABC Conjecture.

ABC Conjecture For any $\epsilon > 0$ there exist a constant $C(\epsilon)$ such that for any non zero relatively prime integers a, b, and c with $a + b = c$ we have

$$\max\{|a|, |b|, |c|\} \leq C(\epsilon)\text{Rad}(abc)^{1+\epsilon}. \tag{3.9}$$

Theorem 3.3.4. *If the ABC Conjecture is true and if $a < c$ are positive integers having the same prime factors, then for any $\epsilon > 0$ there exists a constant $C(\epsilon)$ such that*

$$c - a \geq C(\epsilon)a^{\frac{1}{2}-\epsilon}. \tag{3.10}$$

Proof. Suppose that $a < c$ are positive integers where a and c have the same prime factors. Rearranging, we get $b = c - a$.
Let,

$$P = \text{Rad}(a) = \text{Rad}(c) \text{ and } d = \gcd(a, b) = \gcd(a, c) = \gcd(b, c).$$

Then we have,

$$\frac{a}{d} + \frac{b}{d} = \frac{c}{d} \text{ with the integers } \frac{a}{d}, \frac{b}{d}, \text{ and } \frac{c}{d} \text{ being relatively prime.}$$

We have,

$$\text{Rad}\left(\frac{a}{d}\frac{b}{d}\frac{c}{d}\right) \leq \text{Rad}(ac)\text{Rad}\left(\frac{b}{d}\right) \leq P\frac{b}{d} \leq \frac{b^2}{d}, \tag{3.11}$$

where we get the last inequality from $P \mid b$, since $P \mid a$, and $P \mid c$ imply that $P \mid c - a = b$.

By (3.9), we have

$$\frac{c}{d} \leq C(\epsilon)\left(\frac{b^2}{d}\right)^{1+\epsilon},$$

and thus

$$c \leq C(\epsilon)b^{2(1+\epsilon)},$$

so it follows that

$$b \geq C'(\epsilon)c^{\frac{1}{2}-\epsilon} > C'(\epsilon)a^{\frac{1}{2}-\epsilon}. \tag{3.12}$$

Thus proving Theorem 3.3.1. □

Observation: We see how the ABC Conjecture proves Conjecture 3.3.2, which was used in the work of Cochrane and Dressler to eventually show gaps between integers that have prime factors. Conjecture 3.3.2 shows us a lower bound for b, the difference between c and a, with some connection to the Riemann Hypothesis and Cramér Conjecture. The ABC Conjecture offer some progress on the studies of gaps between primes. the ultimate goal to understand gaps between primes is to see if the Twin Prime Conjecture can be proven. Twin Prime Conjecture states there are infinitely many twin primes or primes that are two apart. In the next proof, we will see another bound through a weaker, but proven result by Stewart and Yu.

3.3.3 Gap Bounds

At the time of the paper, Cochrane and Dressler [4] had used Stewart and Yu's 1991 results

$$\max\{\log|a|, \log|b|, \log|c|\} \leq C(\epsilon)\text{Rad}(abc)^{\frac{2}{3}+\epsilon} \tag{3.13}$$

to prove (3.5). Next we use the improved estimate of Stewart and Yu to prove Theorem 3.3.2.

Proof. We follow the steps as above, but instead of implementing the ABC Conjecture we implement the weaker, but proven, result of Stewart and Yu from 2001,

$$\max\{\log|a|, \log|b|, \log|c|\} \leq C(\epsilon)\mathrm{Rad}(abc)^{\frac{1}{3}+\epsilon}. \tag{3.14}$$

Following the steps as above we have, using (3.14) instead of ABC Conjecture,

$$\log\left(\frac{c}{d}\right) \leq C(\epsilon)\left(\frac{b^2}{d}\right)^{\frac{1}{3}+\epsilon}.$$

Claim: For $2 \leq d \leq \frac{c}{2}$ and $0 < \epsilon < 3$ we have,

$$d\left(\log\left(\frac{c}{d}\right)\right)^{3-\epsilon} \geq .25(\log c)^{3-\epsilon}. \tag{3.15}$$

Observing that the claim follows from

$$\begin{aligned} d\left(1-\frac{\log d}{\log c}\right)^{3-\epsilon} &\geq d\left(1-\frac{\log d}{\log 2d}\right)^{3-\epsilon} \\ &= d\left(\frac{\log 2d}{\log 2d}-\frac{\log d}{\log 2d}\right)^{3-\epsilon} \\ &= d\left(\frac{\log 2}{\log 2d}\right)^{3-\epsilon} \\ &\geq 2\left(\frac{\log 2}{\log 4}\right)^{3} \\ &= .25. \end{aligned}$$

Thus, we deduce that

$$b^2 \geq \frac{1}{C(\epsilon)}d(\log(\frac{c}{d}))^{3-\epsilon} \geq \frac{1}{4C(\epsilon)}(\log c)^{3-\epsilon},$$

which implies

$$b \geq \frac{1}{2\sqrt{C(\epsilon)}}(\log c)^{\frac{3}{2}-\epsilon},$$

or equivalently,

$$b \gg_\epsilon (\log c)^{\frac{3}{2}-\epsilon}, \tag{3.16}$$

Thus proving Theorem 3.3.2. □

Observation: This seems to be a fun little application of results similar to that of the ABC Conjecture. It's interesting what sort of bounds we could get with weaker arguments proven by Stewart and Yu and their work on the ABC Conjecture. One must wonder what other bounds we can find using the ABC Conjecture or results similar to it. The next theorem will be a special case where a and c are positive integers with the same two primes.

3.3.4 Two Prime Factors

Suppose that $a < c$ are positive integers composed of the same two prime factors p, q. Let $\gcd(a, c) = p^e q^f$ and say,

$$c = p^{e+g} q^f, \;\; a = p^e q^{f+h}, \text{ and } b = c - a = p^e q^f (p^g - q^h). \tag{3.17}$$

We want to prove,

$$c - a \gg a^{\frac{1}{2}}. \tag{3.18}$$

Claim: (3.18) is equivalent to

$$p^g - q^h \gg p^{\frac{g}{2}(1-\frac{f}{h}-\frac{e}{g})}. \tag{3.19}$$

There will be two cases to consider, $\begin{cases} q^h < \frac{1}{2}p^g, \\ \frac{1}{2}p^g \leq q^h < p^g. \end{cases}$

If the former case holds, then (3.18) and (3.19) are trivially true

$$\text{i.e. } c - a \geq \frac{a}{2} \gg a^{\frac{1}{2}}, \quad p^g - q^h \geq \frac{p^g}{2} \gg p^{\frac{g}{2}(1-\frac{f}{h}-\frac{e}{g})}.$$

If the latter case holds, then (3.18) is equivalent to

$$c - a = p^e q^f (p^g - q^h) \gg p^{\frac{e}{2}} q^{\frac{f+h}{2}}.$$

That is

$$p^g - q^h \gg p^{\frac{-e}{2}} q^{\frac{-f+h}{2}}. \tag{3.20}$$

Substituting $q \approx p^{\frac{g}{h}}$ into the right-hand side of (3.20) gives (3.19).

Now we use ABC to prove (3.19) in the case where $\frac{1}{2}p^g \leq q^h < p^g$.

Proof. We may assume $e = f = 1$, otherwise divide A and C by $p^{e-1}q^{f-1}$. Now applying the ABC-Conjecture with $A = p^g, B = q^h, C = p^g - q^h$, we have

$$p^g \leq \max\{|q^h|, |(p^g - q^h)|, |p^g|\} \leq C(\epsilon)\text{Rad}(pq|p^g - q^h|)^{1+\epsilon}$$

and so we have, on substituting $q \approx p^{\frac{g}{h}}$,

$$|p^g - q^h| \geq \frac{p^{\frac{g}{1+\epsilon}}}{C(\epsilon)^{\frac{1}{1+\epsilon}}} p^{-1-\frac{g}{h}} \geq C_1(\epsilon')p^{g(1-\frac{1}{g}-\frac{1}{h}-\epsilon')}.$$

□

3.4 Erdős Woods Conjecture

3.4.1 Introduction

Erdős was a famous Hungarian mathematician and published over a thousand articles. Woods [23] first conjectured that there exists a constant k such that every integer a is uniquely determined by the prime divisors of a, $a + 1, \cdots, a + k$. Erdős built off of that conjecture.

Recall that the radical, $\text{Rad}(n)$ is the product of the distinct prime divisors of n. Also recall that for any *abc*-triple (a, b, c), from Baker's inspired conjecture for $\epsilon = \frac{3}{4}$, we can take

$K(\epsilon) = 1$. That is, for positive co-prime integers $a, b,$ and c where $a + b = c$.

$$c < \text{ Rad}(abc)^{\frac{7}{4}}. \tag{3.21}$$

Theorem 3.4.1. *There are infinitely many pairs of positive integers x, y with $x < y$ such that,*

$$Rad(x) = \ Rad(y) \ and \ Rad(x+1) = \ Rad(y+1). \tag{3.22}$$

Proof. Suppose $k \geq 1$. We will define x and y as

$$x = 2^k - 2 = 2(2^{k-1} - 1) \text{ and } y = (2^k - 1)^2 - 1 = 2^{k+1}(2^{k-1} - 1).$$

Then

$$x + 1 = 2^k - 1 \text{ and } y + 1 = (2^k - 1)^2,$$

$$\text{Rad}(x) = \text{Rad}(y) = 2\text{Rad}(2^{k-1} - 1),$$

$$\text{Rad}(x+1) = \ \text{Rad}(y+1) = \text{Rad}(2^k - 1).$$

Thus we have proven 3.4.1. □

There is another example that doesn't follow the form above. We have $(x, y) = (75, 1215)$ where,

$75 = 3 \times 5^2$ and $1215 = 3^5 \times 5$ with $\text{Rad}(75) = \text{Rad}(1215) = 3 \times 5 = 15$,
$76 = 2^2 \times 19$ and $1216 = 2^6 \times 19$ with $\text{Rad}(76) = \text{Rad}(1216) = 2 \times 19 = 38$.

No other further example is known. No one has yet to discover if there exists two different integers x, y such that

Rad$(x) =$ Rad(y), Rad$(x+1) =$ Rad$(y+1)$, and Rad$(x+2) =$ Rad$(y+2)$.

We could extend this to the Erdős-Woods Conjecture.

3.4.2 Erdős-Woods Conjecture

Erdős asked whether this question of whether there exists $x \neq y$ with Rad$(x) =$ Rad(y), Rad$(x+1) =$ Rad$(y+1)$, and Rad$(x+2) =$ Rad$(y+2)$ could be extended. He came up with the following.

Conjecture 3.4.1. *There exists an absolute constant k such that, if x and y are positive integers satisfying*

$$Rad(x+i) = Rad(y+i)$$

for $i = 0, 1, \cdots, k-1$, then $x = y$.

The ABC-conjecture implies that this conjecture holds with $k = 2$ for all but finitely many x.

Theorem 3.4.2. *If the ABC Conjecture holds, then there are only finitely many positive integers $y < x$ such that*

$$\begin{aligned} Rad(x) &= Rad(y), \\ Rad(x+1) &= Rad(y+1), \\ Rad(x+2) &= Rad(y+2). \end{aligned} \tag{3.23}$$

Proof. Suppose $0 < y < x$ satisfy (3.23). Then we have prime power factorization,

$$x = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_u^{\alpha_r}, \quad y = p_1^{\beta_1} p_2^{\beta_2} \cdots p_u^{\beta_r},$$

$$x + 1 = q_1^{\gamma_1} q_2^{\gamma_2} \cdots q_t^{\gamma_t}, \quad y + 1 = q_1^{\epsilon_1} q_2^{\epsilon_2} \cdots q_t^{\epsilon_t},$$

and

$$x+2 = r_1^{\delta_1} r_2^{\delta_2} \cdots r_l^{\delta_l}, \qquad y+2 = r_1^{\mu_1} r_2^{\mu_2} \cdots r_l^{\mu_l}.$$

Note:

$$\begin{aligned} p_j &\mid x-y, \\ q_i &\mid x-y = (x+1)-(y+1), \\ r_h &\mid x-y = (x+2)-(y+2). \end{aligned}$$

Applying the ABC Conjecture to $x+1 = (x+1)$ and $(x+1)+1 = (x+2)$, and $x+2 = (x+2)$ we get

$$\begin{aligned} (x+1) &\le C(\epsilon)(\prod p_j \prod q_i)^{1+\epsilon} \\ (x+2) &\le C(\epsilon)(\prod q_i \prod r_h)^{1+\epsilon} \\ (x+2) &\le C(\epsilon)(2\prod p_j \prod r_h)^{1+\epsilon}. \end{aligned} \tag{3.24}$$

We could have two of x, $x+1$, and $x+2$ have 2 as a prime factor, but otherwise the primes p_j,q_i, r_h, and s_g are distinct. so we have

$$x^3 < (x+1)(x+2)^2 \le C(\epsilon)^3(2\prod p_j \prod q_i \prod r_h)^{2+2\epsilon} \le C(\epsilon)^3(2(x-y))^{2+2\epsilon} < C(\epsilon)^3(2x)^{2+2\epsilon} = 2^{2+2\epsilon}x^{2+2\epsilon}.$$

Thus taking $\epsilon < \frac{1}{2}$ we have,

$$\begin{aligned} x^{1-2\epsilon} &\le C(\epsilon)^3 2^{2+2\epsilon} \\ x &\le C(\epsilon)^{\frac{3}{1-2\epsilon}} 2^{\frac{2+2\epsilon}{1-2\epsilon}} \end{aligned}$$

Thus we have a bound and have shown Theorem 3.4.2. □

If $k = 3$, we can make the bounds on x effective.

Theorem 3.4.3. *If $y < x$ are positive such that*

$$\begin{aligned} Rad(x) &= Rad(y), \\ Rad(x+1) &= Rad(y+1), \\ Rad(x+2) &= Rad(y+2), \\ Rad(x+3) &= Rad(y+3), \end{aligned} \tag{3.25}$$

and the effective ABC Conjecture (3.21) holds, then $x < 6^7$.

Proof. Suppose that $0 < y < x$ satisfy (3.25). We will let

$$x = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_u^{\alpha_r}, \qquad y = p_1^{\beta_1} p_2^{\beta_2} \cdots p_u^{\beta_r}$$

$$x + 1 = q_1^{\gamma_1} q_2^{\gamma_2} \cdots q_t^{\gamma_t}, \qquad y + 1 = q_1^{\epsilon_1} q_2^{\epsilon_2} \cdots q_t^{\epsilon_t}$$

$$x + 2 = r_1^{\delta_1} r_2^{\delta_2} \cdots r_l^{\delta_l}, \qquad y + 2 = r_1^{\mu_1} r_2^{\mu_2} \cdots r_l^{\mu_l}$$

$$x + 3 = s_1^{\omega_1} s_2^{\omega_2} \cdots s_m^{\omega_m}, \qquad y + 3 = s_1^{\zeta_1} s_2^{\zeta_2} \cdots s_m^{\zeta_m}.$$

Thus we have,

$$\begin{aligned} p_j &\mid x - y, \\ q_i &\mid x - y, \\ r_h &\mid x - y, \\ s_g &\mid x - y. \end{aligned}$$

By (3.21) applied to $x+1=(x+1)$ and $(x+2)+1=(x+3)$ we have,

$$(x+1)\leq (\prod p_j \prod qi)^{\frac{7}{4}}$$

and

$$(x+3)\leq (\prod r_h \prod s_g)^{\frac{7}{4}}.$$

Then worst case is that 2 and 3 can appear twice, otherwise the primes are distinct. If a prime divides two different numbers, then it divides the length of the gap between them, which in this case is at most 3. Thus we have,

$$x^2 < (x+1)(x+3) \leq (\prod p_j \prod q_i \prod r_h \prod s_g)^{\frac{7}{4}} \leq (6(x-y))^{\frac{7}{4}} \leq 6^{\frac{7}{4}} x^{\frac{7}{4}}.$$

Thus we have $x \leq 6^7 = 279,936$ and so proving Theorem 3.4.2. □

3.5 Baker's Theorem

In this section, I will talk about Baker's Theorem. In 1968, Baker obtained lower bounds on linear forms of logarithms that can, for example, be used to find effective bounds on the size of the integer solutions to certain Diophantine equations. For this breakthrough, Baker earned the Fields Medal in 1970. Let $p_1, p_2, \cdots, p_k$ be prime numbers and define

$$L := \log|\log(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k})| \tag{3.26}$$

where the $a_i \in \mathbb{Z}$. Baker showed that when the exponents a_i are bounded,

$$|a_i| \leq W, \tag{3.27}$$

then the value of L cannot be too small. For example, Baker and Wüstholz [3] obtained the lower bound

$$L \geq -18(k+1)!k^{k+1}32^{k+2}\log(2k)\left(\log W\right)\prod_{i=1}^{k}\log p_i.$$

This result is likely not best possible. In the next section we consider results in the other direction, namely how small we know that L can be.

3.5.1 Box Principle

To see what's best possible for such a bound, let's consider what the box principle will give us.

Theorem 3.5.1. *For any integer $W > 1$, there exists integers a_i with $|a_i| \leq W$ such that,*

$$L \leq -\left(k-1\right)\log W + \log\log\left(p_1 p_2 \cdots p_k\right). \tag{3.28}$$

Proof. Equivalently, we need to show that for any integer $W > 1$, there exists $a_i \in \mathbb{Z}$ with $|a_i| \leq W$ such that,

$$|a_1 \log p_1 + a_2 \log p_2 + \cdots + a_k \log p_k| \leq \frac{\sum_{i=1}^{k}\log p_i}{W^{k-1}}. \tag{3.29}$$

Consider the values

$$x_1 \log p_1 + x_2 \log p_2 + \cdots + x_k \log p_k \tag{3.30}$$

with the $x_i \in \{0, 1, \cdots, W\}$. The number of these, looking at the possibilities (we have $(W+1)$ choices k times), is $(W+1)^k$.

We have $(W+1)^k \geq W^k + 1$ and since $\sum_{i=1}^{k} x_i \log p_i \leq \sum_{i=1}^{k} W \log p_i$, all the sums (3.30) lie within the interval $\left[0, W\left(\sum_{i=1}^{k}\log p_i\right)\right]$. Then we will divide $\left[0, W\left(\sum_{i=1}^{k}\log p_i\right)\right]$ into

W^k sub-intervals, each of length

$$\frac{W\left(\sum_{i=1}^{k}\log p_i\right)}{W^k}=\frac{\left(\sum_{i=1}^{k}\log p_i\right)}{W^{k-1}}.$$

By the box principle, two of the sums

$$x_1\log p_1+x_2\log p_2+\cdots+x_k\log p_k,\qquad x_1'\log p_1+x_2'\log p_2+\cdots+x_k'\log p_k$$

say, must lie in the same sub-interval, and hence

$$|\,(x_1\log p_1+x_2\log p_2+\cdots+x_k\log p_k)-(x_1'\log p_1+x_2'\log p_2+\cdots+x_k'\log p_k)\,|\le\frac{\left(\sum_{i=1}^{k}\log p_i\right)}{W^{k-1}}.$$

Let $x_i-x_i'=a_i, 1\le i\le k$, so we have $-A\le a_i\le A$ and thus have (3.29). If we take the logarithm of both sides of (3.29), then we get (3.28). □

3.5.2 Explicit ABC Conjecture and Baker's Theorem

In this section, we will see how an explicit form of the ABC Conjecture would improve Baker's Theorem. We will come close to a bound that we know is optimal coming from the box principle. We will need to make the epsilon dependence in the ABC Conjecture explicit and we will use a form conjectured by Baker [1].

Conjecture 3.5.1. *There is an absolute constant κ, such that if A, B, C are integers with $A+B=C$ and $\gcd(A,B,C)=1$ then for any $\epsilon>0$,*

$$\max\{|A|,|B|,|C|\}\ll\epsilon^{-\kappa\omega(AB)}Rad(ABC)^{1+\epsilon}. \tag{3.31}$$

If we assume this conjecture, we will obtain the following lower bound on L.

Theorem 3.5.2. *If Conjecture 3.5.1 holds, then*

$$L \gg -k \log W - \log(p_1 \cdots p_k). \tag{3.32}$$

Proof. Let $A = \prod_{a_i > 0} p_i^{a_i}$, $B = \prod_{a_i < 0} p_i^{a_i}$ and $C = A - B$. We need to show that

$$L = \log \left| \log \left(\frac{A}{B} \right) \right| \gg -k \log W - \log(p_1 \cdots p_k).$$

Assume without loss of generality that $A > B$. We can also assume that $0 < \log \left(\frac{A}{B} \right) < 1$, otherwise the claim is trivial. By assuming the form (3.31) of the ABC Conjecture, we have

$$A = \max\{|A|, |B|, |C|\} \ll \epsilon^{-\kappa k} \left(C p_1 \cdots p_k \right)^{1+\epsilon}.$$

From this, we will get

$$C \gg \frac{A^{\frac{1}{1+\epsilon}} \epsilon^{\frac{\kappa k}{1+\epsilon}}}{p_1 \cdots p_k}. \tag{3.33}$$

Now consider,

$$\frac{C}{A} \leq \frac{C}{B} = \frac{A}{B} - 1 = e^{\log\left(\frac{A}{B}\right)} - 1 \ll \log \left(\frac{A}{B} \right), \tag{3.34}$$

the latter inequality since by concavity $e^x \leq 1 + (e-1)x$ for $0 \leq x \leq 1$. Substituting (3.33) in (3.34) yields

$$\log \left(\frac{A}{B} \right) \gg \frac{\epsilon^{\frac{\kappa k}{1+\epsilon}}}{A^{\frac{\epsilon}{1+\epsilon}} (p_1 \cdots p_k)}. \tag{3.35}$$

Taking $\delta = \frac{\epsilon}{1+\epsilon}$ and observing that $A \leq (p_1 \cdots p_k)^W$, and $\epsilon^{\frac{1}{1+\epsilon}} \geq \frac{\epsilon}{1+\epsilon}$ for $\epsilon \geq 0$, we get,

$$\log \left(\frac{A}{B} \right) \gg \frac{\delta^{\kappa k}}{(p_1 \cdots p_k)^{W\delta + 1}}, \tag{3.36}$$

for any $0 < \delta < 1$. Now pick $\delta = \frac{1}{W}$, and we get,

$$\log\log\left(\frac{A}{B}\right) \gg -k\log W - \log(p_1 \cdots p_k), \tag{3.37}$$

as claimed. □

3.6 Other Applications

In this section, we will see two other applications. We will look at Roth's theorem and Mordell's Conjecture. If there were more time, we would go into lengthy proofs, but at least we will see the statements.

Looking at a survey article by Andrew Granville and Thomas J. Tucker [9], we will see how the ABC Conjecture plays a part with Roth's Theorem.

Let α be a real algebraic irrational number of degree d. Using the box principle, gives infinitely many rational numbers $\frac{m}{n}$ such that $|\alpha - \frac{m}{n}| < \frac{1}{n^2}$. When we substitute $\frac{m}{n}$ into the minimal polynomial for α, we get a constant C_α for which

$$\left|\alpha - \frac{m}{n}\right| > \frac{C_\alpha}{n^d}. \tag{3.38}$$

In 1955, Roth [15] came up with the best possible lower bound for (3.38) with his theorem, earning a Fields Medal in 1958.

Theorem 3.6.1 (Roth's Theorem). *If α is a real algebraic number, then for any $\epsilon > 0$, there exists a constant $C_{\alpha,\epsilon} > 0$ such that,*

$$\left|\alpha - \frac{m}{n}\right| \geq \frac{C_{\alpha,\epsilon}}{n^{2+\epsilon}},$$

for all rationals $\frac{m}{n}$.

Let, $F(x, y) \in \mathbb{Z}[x, y]$ be a binary homogeneous form with no repeating factors. Then applying Roth's Theorem, it is readily seen that we have for any co-prime integers m and n,

$$\begin{aligned} |F(m,n)| &\gg_F n^{\deg(F)} \prod_{\alpha : F(\alpha,1)=0} \left|\alpha - \frac{m}{n}\right| \\ &\gg_{F,\epsilon} n^{\deg(F)-2-\epsilon}. \end{aligned}$$

In fact it is not hard to see that this is equivalent to Roth's Theorem.

Applying the ABC Conjecture, it turns out that we get a slightly stronger form,

$$\prod_{p|F(m,n)} p \gg_{F,\epsilon} (\max\{|m|,|n|\})^{\deg(F)-2-\epsilon}.$$

Next, we will look at Mordell's Conjecture. In 1922, L.J. Mordell [13] conjectured the following.

Conjecture 3.6.1. *Let C be an algebraic curve defined over $\mathbb{Q}$ of genus $g \geq 2$. Then the set of rational points on C is finite.*

In 1983, this was proved by Faltings [7] who was awarded a Fields Medal in 1986. Elkies [6] showed that the Mordell's Conjecture (Faltings' Theorem) can be proved using the ABC Conjecture. Machiel van Frankenhuysen [8] writes up a proof using Beylĭ's Map to show how ABC Conjecture proves both Roth's Theorem and Mordell's Conjecture.

3.7 Final Thoughts

In this final section, I will compose a poem about the ABC Conjecture.

ABC, how spectacular one can be.
Its truth holds power in many different branches of Number Theory, one can see.
Explicit forms showing bounds in conjectures related to Erdős-Woods and prime gaps.
Countless number of non-Wieferich primes can be proven by using ABC, oh snap.
Not as easy as the alphabet, a long ways to go to being proved.
Improving results inching closer thanks to Stewart and Yu.
Deep in the fields, polynomial version and integer version as well.
Brief proof showing Fermat's Last Theorem or General Fermat's Equation, the details one can spell.
Countless number of applications, the list keeps going on as it seems.
Oh the ABC Conjecture to Number Theory is truly extraordinary, one could deem.

Bibliography

[1] A. Baker, *Logarithmic forms and the abc-conjecture.* Number Theory: Diophantine Computational, and Algebra Aspects (1998), 37-44, Berlin, New York.

[2] A. Baker, *Experiments on the abc-conjecture.* Publ. Math. Debrecen Volume 65, Number 3-4 (2004), 253-260.

[3] A. Baker and Wüstholz, G., *Logarithmic forms and group varieties.* J. Reine Angew. Math. 442 (1993), 19-62.

[4] Todd Cochrane and Robert E. Dressler, *Gaps between integers with the same prime factors.* Mathematics of Computations, Volume 68, Number 225 (1999), 395-401.

[5] H. Cramér, *On the order of magnitude of the difference between consecutive prime numbers.* Acta Arith., Volume 2 (1937), 23-46.

[6] N. Elkies, *ABC implies Mordell.* Int. Math. Res. Not. Volume 7 (1991), 99-109; Duke Math Journal 64 (1991).

[7] G. Faulting, *Endlichkeitssätze für abelsche Varietä ten über Zahlkörpern.* Invent. Math. Volume 73 (1983), 349-66.

[8] Machiel van Frankenhuysen, *The ABC conjecture implies Roth's theorem and Mordell's conjecture* (1991), University of California, Riverside.

[9] Andrew Granville and Thomas J. Tucker, *It's as easy as abc.* Notices of the AMS, Volume 49, Number 10 (2002), 1224-1231.

[10] J. J. O'Connor and E. F. Robertson, *Fermat's last theorem* (1996): MacTutor

[11] R. C. Mason, *Diophantine equations over function fields* London Math Soc. Lecture Notes ser. 96, Cambridge Univ. Press (1984).

[12] D. W. Masser, *Open Problems.* In: Proc. Symp. Analytic Number Theory (edit by W. W. L. Chen) (1984). Imperial Coll. London.

[13] L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees.* Proc. Cambridge Philos. Soc. Volume 21 (1922), 179-92.

[14] J. Osterlé, *Nouvelles approches du "Théorème" de Fermat.* Astérisque 161-2 (1998), 165-186

[15] K. F. Roth, *Rational approximations to algebraic numbers.* Mathematika, Volume 2 (1955), 1-20.

[16] J. H. Silverman, *The S-unit equation over function fields.* Math. Proc. Cambridge Philos. Soc. Volume 95 (1984) 3–4.

[17] C. L. Stewart and R. Tijdeman, *On the Oesterlé-Masser conjecture.* Monatsh. Math. Volume 102 (1986), 251-257.

[18] C. L. Stewart and Kunrui Yu, *On the abc conjecture.* Math. Ann. Volume 291 (1991), 225-230.

[19] C. L. Stewart and Kunrui Yu, *On the abc conjecture, II.* Duke Mathematical Journal, Volume 108, Number 1 (2001).

[20] W. W. Stothers, *Polynomial identities and Hauptmoduln.* Quart. J. Math. Oxford Ser. (2) Volume 32 (1981), 349–370.

[21] Jeff Vaaler, *The ABC Conjecture.* Dressler Lecture (2009), Kansas State University

[22] Michel Waldschmidt, *Lecture on the abc conjecture and some of its consequences.* Abdus Salam School of Mathematical Sciences (ASSMS), Lahore 6th World Conference on 21st Century Mathematics (2013), Université Pierre et Marie Curie-Paris.

[23] A. R. Woods, *Some problems in logic and number theory, and their connections.* Ph. D. Thesis (1981), University of Manchester.