1-1-2013

Coloring Pythagorean Triples and a Problem Concerning Cyclotomic Polynomials

Daniel White
University of South Carolina

Coloring Pythagorean Triples and a Problem Concerning Cyclotomic Polynomials

by

Daniel White

Bachelor of Science
Shippensburg University 2011

Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Arts in

Mathematics

College of Arts and Sciences

University of South Carolina

2013

Accepted by:

Michael Filaseta, Major Professor

Ognian Trifonov, Second Reader

Lacy Ford, Vice Provost and Dean of Graduate Studies

Acknowledgments

I would like to thank my advisor Michael Filaseta for his support and guidance throughout the process of writing this thesis, as well as contributors Joshua Cooper, Josh Harrington, and Lenny Jones. I'm incredibly grateful to have been in the presence of these people during the past few years of my life. In addition, I extend my gratitude to Michael and Josh for warmly welcoming me as an individual into this department. To Ognian Trifonov, I am happy to have studied in this department and have learned so much. It was a fantastic opportunity.

It can't go without mention that if it were not for Lenny believing in my ability to succeed and acting to make sure it happened, I most certainly would not have come this far. Thank you so much. Others who have played pivotal roles in my life are not without mention. My grandmother, Iris, is my number one fan and did everything in her power to help me through the past six years. I can't express my gratitude. My parents Paula and Frank, and step-father Danny, never paused a minute to help when I needed it. The fact is: the same can be said about my whole family. It's tough to fail when you have so many incredible people pushing you forward.

I can't say with certainty that I wouldn't have lost my mind over the past two years if it wasn't for Jessie Fry. Selfishly, I uprooted her from family and friends to pursue my education. Selflessly, she followed and supported me the entire way. I couldn't ask for a better partner in life. To Madré and Steve, I appreciate the roof you put over my head and the food you put on my plate when I'm around. You're the best.

Abstract

One may easily show that there exist $O(\log n)$-colorings of $\{1, 2, \ldots, n\}$ such that no Pythagorean triple with elements $\leq n$ is monochromatic. In Chapter 2, we investigate two analogous ideas. First, we find an asymptotic bound for the number of colors required to color $\{1, 2, \ldots, n\}$ so that every Pythagorean triple with elements $\leq n$ is 3-colored. Afterwards, we examine the case where we allow a vanishing proportion of Pythagorean triples with elements $\leq n$ to fail to have this property.

Unrelated, in 1908, Schur raised the question of the irreducibility over $\mathbb{Q}$ of polynomials of the form $f(x) = (x - a_1)(x - a_2) \cdots (x - a_n) + 1$, where the a_i are distinct integers. Since then, many authors have addressed variations and generalizations of this question. In Chapter 3, we investigate the analogous question when replacing the linear polynomials with cyclotomic polynomials and allowing the constant perturbation of the product to be any integer $d \notin \{-1, 0\}$.

Contents

Acknowledgments iii

Abstract iv

Chapter 1 An Introduction 1

1.1 Diophantine Equations 1

1.2 Colorings 2

1.3 Pythagorean Triples 3

1.4 Asymptotics 4

1.5 Cyclotomic Polynomials 5

Chapter 2 Coloring Pythagorean Triples 7

2.1 Introduction 7

2.2 Preliminaries 8

2.3 The Proof of Theorem 2.1 13

2.4 Outline of the Proof of Theorem 2.2 15

2.5 The Proof of Theorem 2.2 16

2.6 The Proof of Theorem 2.3 21

2.7 The Proof of Theorem 2.4 24

Chapter 3 The Reducibility of Constant-Perturbed Products of Cyclotomic Polynomials 25

3.1 Introduction 25

3.2 Preliminaries 26

3.3 The Reducibility of $\Phi_m(x) + d$ with $d \in \mathbb{Z}^+$ 28

3.4 The Reducibility of $\prod_{i=1}^{k} \Phi_{m_i}(x) + 1$ where $k \geq 1$ 40

3.5 A Non-cyclotomic Version of Theorem 3.8 41

3.6 The Reducibility of $\Phi_m(x) + d$ with $d \in \mathbb{Z}$ 43

Bibliography 45

Chapter 1

An Introduction

The goal of the first chapter is to equip this thesis with a mostly non-technical introduction to vocabulary, ideas, and questions which are used and addressed throughout.

1.1 Diophantine Equations

We begin with a definition.

Definition 1.1. A *Diophantine equation* is a type of equation which allows its variables to take integer values only.

An example of which is the equation $2x^2 + y = 1$, where we allow x and y to take integer values only. Some possible solutions for (x, y) are $(1, -1)$ and $(2, -7)$. It's easily seen that there exist infinitely many pairs (x, y) that satisfy this equation, but not all Diophantine equations have this property. For instance, the *Ramanujan-Nagell* equation $2^y - 7 = x^2$ has solutions for (x, y) as

$$(\pm 1, 3), (\pm 3, 4), (\pm 5, 5), (\pm 11, 7) \text{ and } (\pm 181, 15)$$

and no others. This is not an easy fact to show, as it was first conjectured in 1913 by Indian mathematician *Srinivasa Ramanujan* and not proven until 1948 by Norwegian mathematician *Trygve Nagell*.

Definition 1.2. The *solution set* of an equation with variables $x_1, x_2, \ldots x_n$ is the set of all $(y_1, y_2, \ldots y_n)$ that have the property that substituting $x_i = y_i$ for all i satisfies the equation.

Remark 1.1. When considering a Diophantine equation, each y_i in the definition prior is taken to be integral.

With respect to the Ramanujan-Nagell equation, we'd say that the solution set is

$$\{(1,3),(3,4),(5,5),(11,7),(181,15),(-1,3),(-3,4),(-5,5),(-11,7),(-181,15)\},$$

whereas the solution set to $2x^2 + y = 1$ would be the set $\{(1,-1),(2,-7),\ldots\}$.

1.2 Colorings

A K-coloring of a set $\mathcal{S}$ is just that; we take each element s in $\mathcal{S}$ and assign it a color from a collection of K colors, making sure each color from the collection is assigned at least once. A more concrete definition follows.

Definition 1.3. A K-coloring of a set $\mathcal{S}$ is a surjective function $f : \mathcal{S} \to \{1, 2, \ldots, K\}$.

Usually, one is concerned with finding a coloring of $\mathcal{S}$ that has particular properties. For example, we could ask the next question.

Question 1.1. *What is the least K such that there exists a K-coloring of the set*

$$\mathcal{S} = \Big\{(\clubsuit, \diamondsuit), (\heartsuit, \Delta), (\spadesuit, \diamondsuit), (\diamondsuit, \S), (\S, \clubsuit)\Big\}$$

such that no two pairs which share a symbol have the same color?

Since three of the five pairs contain $\diamondsuit$, we see that no 2-coloring of $\mathcal{S}$ has this property. However, if we assign each pair containing $\diamondsuit$ a unique color and $(\heartsuit, \Delta)$ the color of $(\clubsuit, \diamondsuit)$, and $(\S, \clubsuit)$ the color of $(\spadesuit, \diamondsuit)$, we'll have a 3-coloring of $\mathcal{S}$ with the desired property. Hence, 3 is the answer to Question 1.1.

Definition 1.4. Consider a coloring of $\mathbb{Z}$. We say a subset $\mathcal{Q}$ of $\mathbb{Z}$ is monochromatic if the coloring on $\mathbb{Z}$ restricted to $\mathcal{Q}$ has the property that every element of $\mathcal{Q}$ is assigned the same color.

Definition 1.5. Consider a coloring of $\mathbb{Z}$. We say a subset $\mathcal{Q}$ of $\mathbb{Z}$ is M-colored if the coloring on $\mathbb{Z}$ restricted to $\mathcal{Q}$ has the property that M is the greatest integer such that there exist M elements of $\mathcal{Q}$, each assigned a different color.

In Chapter 2 we'll be asking questions related to coloring the set of integers (henceforth referred to as $\mathbb{Z}$) such that the solution set of a certain Diophantine equation has specific properties. In particular, these questions are related to the following.

Question 1.2. *Let $\mathcal{D}$ be the solution set of a given Diophantine equation. What is the least K such that there exists a K-coloring of $\mathbb{Z}$ such that no element $\mathcal{S}$ of $\mathcal{D}$ is monochromatic?*

Question 1.3. *Let $\mathcal{D}$ be the solution set of a given Diophantine equation of M variables. What is the least K such that there exists a K-coloring of $\mathbb{Z}$ such that each element $\mathcal{S}$ of $\mathcal{D}$ is M-colored?*

Remark 1.2. Do note that it is possible that no such K exists for Questions 1.2 and 1.3, depending on the Diophantine equation at hand.

1.3 Pythagorean Triples

Theorem 1.1. *Let a, b, and c be the side-lengths of a right triangle with c the greatest length. Then $a^2 + b^2 = c^2$.*

The theorem above is known as the *Pythagorean theorem*. If we restrict each variable in the equation above to be integral, we may ask when it has solutions. That is, we may consider the solution set of the following Diophantine equation.

$$a^2 + b^2 = c^2 \tag{1.3.1}$$

Definition 1.6. We say an ordered triple of positive integers (a, b, c) is a Pythagorean triple if it satisfies (1.3.1).

Remark 1.3. We apply the restriction that each term in the Pythagorean triple is positive since identifying all Pythagorean triples in turn identifies all elements of the solution set to (1.3.1). For similar reasons, in Chapter 2 we adopt the convention that (a, b, c) and (b, a, c) are equivalent.

In line with Questions 1.2 and 1.3 we can ask the following for the set of natural numbers (henceforth referred to as $\mathbb{N}$).

Question 1.4. *Let $\mathcal{D}$ be the set of Pythagorean triples. What is the least K such that there exists a K-coloring of $\mathbb{N}$ such that no element $\mathcal{S}$ of $\mathcal{D}$ is monochromatic?*

Question 1.5. *Let $\mathcal{D}$ be the set of Pythagorean triples. What is the least K such that there exists a K-coloring of $\mathbb{N}$ such that each element $\mathcal{S}$ of $\mathcal{D}$ is 3-colored?*

It happens to be unknown if such K exists to answer Question 1.4. However, there's evidence that suggests $K = 2$ may suffice. See [2] and [9]. In turn, this makes the solution to Question 1.5 unknown as well. However, we may ask similar questions that provide insight to Questions 1.4 and 1.5.

Question 1.6. *Let $\mathcal{D}$ be the set of Pythagorean triples with elements $\leq n$. What is the least K such that there exists a K-coloring of $\{1, 2, \ldots, n\}$ such that no element $\mathcal{S}$ of $\mathcal{D}$ is monochromatic?*

Question 1.7. *Let $\mathcal{D}$ be the set of Pythagorean triples with elements $\leq n$. What is the least K such that there exists a K-coloring of $\{1, 2, \ldots, n\}$ such that each element $\mathcal{S}$ of $\mathcal{D}$ is 3-colored?*

These questions (in particular Question 1.7 and a variation) are addressed in Chapter 2.

1.4 Asymptotics

Here we introduce notation used extensively in Chapter 2.

Definition 1.7. We use $f(x) = O(g(x))$ and $f(x) \ll g(x)$ to mean that, for sufficiently large x and some constant C, we have $f(x) \leq Cg(x)$. This is read as "$f(x)$ is big-O of $g(x)$" or "$f(x)$ is less than less than $g(x)$".

Definition 1.8. We use $f(x) = o(g(x))$ to mean that $\lim_{x\to\infty} f(x)/g(x) = 0$. This is read as "$f(x)$ is little-O of $g(x)$".

Definition 1.9. Writing $f(x) \sim g(x)$ means that $\lim_{x\to\infty} f(x)/g(x) = 1$. This is read as "$f(x)$ is asymptotic to $g(x)$".

1.5 Cyclotomic Polynomials

Chapter 3 concerns topics related to the set

$$\mathbb{Z}[x] := \left\{ \sum_{i=0}^{k} a_i x^i : 0 \leq k \in \mathbb{Z}, a_i \in \mathbb{Z} \right\},$$

that is, the set of polynomials whose coefficients are integers. In particular, given polynomials of some prescribed form, we'd like to determine whether they're reducible or irreducible. A polynomial $f(x) \in \mathbb{Z}[x]$ is said to be *reducible* (over $\mathbb{Q}$) if we can write $f(x) = g(x)h(x)$ for $g(x)$ and $h(x)$ in the set $\mathbb{Z}[x]$ such that $\deg f \geq 1$ and $\deg g \geq 1$. $f(x)$ is said to be *irreducible* if it is not reducible.

Most results obtained in this chapter deal with *cyclotomic* polynomials. Let $\exp(z) := e^z$. By definition, for $n \geq 2$, the n^{th} cyclotomic polynomial is

$$\Phi_n(x) := \left(x - \exp\left(\frac{2\pi i k_1}{n}\right)\right)\left(x - \exp\left(\frac{2\pi i k_2}{n}\right)\right) \ldots \left(x - \exp\left(\frac{2\pi i k_{\varphi(n)}}{n}\right)\right),$$

where φ is Euler's totient function and the k_j's range over the distinct positive integers less than and coprime to n. In addition, we say $\Phi_1(x) = x - 1$. Each $\exp(2\pi i k_j/n)$ is called an n^{th} *primitive root of unity*. If we let $\zeta_n := \exp(2\pi i/n)$, it is common to write

$$\Phi_n(x) = \prod_{\substack{1\leq k\leq n \\ (k,n)=1}} (x - \zeta_n^k).$$

For $n \geq 1$, basic facts about the n^{th} cyclotomic polynomial include: $\Phi_n(x) \in \mathbb{Z}[x]$, $\Phi_n(x)$ has degree $\varphi(n)$, and $\Phi_n(x)$ is irreducible.

A driving force throughout the chapter is the next question.

Question 1.8. *Given a positive integer n and $d \in \mathbb{Z}$, is $\Phi_n(x) + d$ reducible or irreducible?*

For $d = 1$, we also investigate the following related question.

Question 1.9. *Given positive integers $n_1, n_2, \ldots, n_k$, when can $\prod_{j=1}^{k} \Phi_{n_j}(x) + 1$ be reducible?*

Chapter 2

Coloring Pythagorean Triples

The results in this chapter are joint work with Joshua Cooper, Michael Filaseta, and Joshua Harrington from the University of South Carolina.

2.1 Introduction

An ordered triple of positive integers (a, b, c) is called a Pythagorean triple if it satisfies the equation $a^2 + b^2 = c^2$. We adopt the convention that (a, b, c) and (b, a, c) are equivalent. If $\gcd(a, b, c) = 1$, then we say the Pythagorean triple is *primitive*.

One may construct $O(\log n)$-colorings of $\{1, 2, \ldots, n\}$ such that no Pythagorean triple with elements $\leq n$ is monochromatic. Details are given in Remark 2.4. Such a bound may be crude, as it is not even known if just 2 colors would suffice to color $\mathbb{N}$ so that every Pythagorean triple has this property. Cooper and Poirel [2], and later Kay [9], have constructed such 2-colorings for $n = 1344$ and $n = 1514$, respectively.

With connections to these topics, we present four main theorems in this chapter.

Theorem 2.1. *There exist* $\sqrt{3}^{(1+o(1))\log n/\log\log n}$*-colorings of* $\{1, 2, \ldots, n\}$ *such that every Pythagorean triple with elements* $\leq n$ *is* 3*-colored.*

Theorem 2.2. *Let* $\xi(n)$ *be any positive, increasing function that tends to infinity. There exist* $O(\xi(n^{1+\varepsilon})\log^2 n/\log\log n)$*-colorings of* $\{1, 2, \ldots, n\}$ *such that the proportion of Pythagorean triples with elements* $\leq n$ *which are not* 3*-colored vanishes with order at most* $\max\{2^{-\xi(n)}, 1/\log n\}$ *as* $n \to \infty$*.*

Theorem 2.3. *Let $\xi(x)$ be any positive, increasing function that tends to infinity. There exist $O(\xi(n))$-colorings of $\{1, 2, \ldots, n\}$ such that the proportion of Pythagorean triples with elements $\leq n$ which are not 3-colored vanishes with order at most*

$$\max\left\{1/\sqrt{\log\log\log\log n}, 1/\sqrt{\xi(n)}\right\}$$

as $n \to \infty$.

Theorem 2.4. *There exists a 3-coloring of $\mathbb{N}$ such that the proportion of primitive Pythagorean triples with elements $\leq n$ which are not 3-colored vanishes with order at most $1/\sqrt{\log\log n}$ as $n \to \infty$.*

2.2 Preliminaries

It is useful throughout this exposition to generate the set of Pythagorean triples using a method due to Euclid.

Theorem 2.5. *Let $k \geq 1$, $(s,t) = 1$, $s > t > 0$ and one of s or t be even. There is a bijection from the ordered triples (k,s,t) to the Pythagorean triples which is given by $a = k(s^2 - t^2)$, $b = 2kst$, and $c = k(s^2 + t^2)$.*

Remark 2.1. In this chapter, the symbols a, b, and c are reserved solely to denote the elements of an arbitrary Pythagorean triple. In addition, a is always used to represent the element which is generated by $k(s^2 - t^2)$, b is always used to represent the element which is generated by $2kst$, and c is always used to represent the element which is generated by $k(s^2 + t^2)$.

Remark 2.2. We often refer to a Pythagorean triple's representation. In such situations, we refer to the ordered triple (k,s,t).

Let $m = 2^h p_1^{e_1} p_2^{e_2} \ldots p_y^{e_y} q_1^{e_{y+1}} \ldots q_\ell^{e_{y+\ell}}$ be the canonical prime factorization of m, where $p_i \equiv 1 \pmod 4$ and $q_i \equiv 3 \pmod 4$. We recall two facts from Beiler [1]

that are used in computing how many Pythagorean Triples some positive integer m participates in.

Lemma 2.1. *The number of Pythagorean Triples which m participates in as a leg is*

$$P_L(m) = \frac{1}{2}\left(|2h-1|\prod_{j=1}^{y+\ell}(2e_j-1)-1\right).$$

Lemma 2.2. *The number of Pythagorean Triples which m participates in as a hypotenuse is*

$$P_H(m) = \frac{1}{2}\left(\prod_{j=1}^{y}(2e_j-1)-1\right).$$

The following theorem is immediate.

Theorem 2.6. *The number of Pythagorean Triples which m participates in is* $P(m) = P_L(m) + P_H(m)$.

The proof of Theorem 2.1 uses a number of facts regarding graphs. All graphs referenced in this chapter are taken to be undirected and simple.

Definition 2.1. The *chromatic number* of a graph G is the least number of colors required to color the vertex set $V(G)$ such that no adjacent vertices share the same color. We let $\chi(G)$ denote this number.

Definition 2.2. Let $E(G)$ denote the set of edges of G, the elements of which we may represent uniquely as a pair (v_i, v_j), for vertices $v_i, v_j \in V(G)$.

Lemma 2.3. *Define* $\Delta(G)$ *to be* $\max_{v\in V(G)} \deg(v)$. *We have that* $\chi(G)$ *is bounded above by* $1 + \Delta(G)$.

Proof. List the vertices of G arbitrarily as $v_1, \ldots, v_n$. We'll color these vertices using the following algorithm.

1. Let $j = 0$.

2. Let $j \leftarrow j + 1$.

3. If $j > n$, then *terminate*.

4. Define $\phi(v_j)$ to be the minimal element of $[1 + \Delta(G)] \setminus \bigcup_{(v_i,v_j)\in E(G), i<j} \{\phi(v_i)\}$.

5. Go to step (2).

Note that $\phi(v_j)$ is well-defined for each $j \leq n$ since no vertex has more than $\Delta(G)$ neighbors. By the definition of ϕ, no adjacent vertices may be the same color. This completes the proof. □

Corollary 2.1. *Define D to be $\Delta(G_k)$, where G_k is the graph obtained from G by removing the k vertices of highest degree, along with all incident edges. Then $\chi(G) \leq k + D + 1$*

Proof. Color the graph G_k according to the preceding result. Now, assign a new, unique color to each element of $V(G) \setminus V(G_k)$. □

It will be useful to understand the maximal growth rate of the divisor function while constructing a proof of Theorem 2.1. This is given by a theorem of Wigert [20].

Theorem 2.7.

$$\limsup_{m\to\infty} \frac{\log d(m)}{\log m/\log\log m} = \log 2$$

In particular, we'd like to place an upper bound on $d(m)$. In essence, Wigert's theorem captures such a bound. We utilize the following remark.

Remark 2.3. Appealing to the definition of the limit supremum, one may easily prove that

$$\frac{\log d(m)}{\log 2} \leq (1 + o(1))\frac{\log m}{\log\log m}.$$

A main tool used in the proof of Theorem 2.2 is covering systems.

Definition 2.3. A *covering system* (or simply a *covering*) is a finite set of residue classes $\{r_i \pmod{m_i}\}_{i\in I}$ such that every integer is contained in at least one residue

class in the set. We say that a covering system is *exact* if each integer resides in exactly one residue class in the system.

Definition 2.4. Let $\Omega(x)$ be the number of Pythagorean triples with elements $\leq x$. In the context where x is fixed, we'll simply call this Ω.

It is useful to understand how $\Omega(x)$ grows. The following is due to Sierpiński [18].

Theorem 2.8. *We have* $\Omega(x) = 4\pi^{-1}x\log x + Bx + O(x^{2/3})$ *for some constant* B.

Related, we have the next theorem from D.H. Lehmer [3].

Theorem 2.9. *The number of primitive Pythagorean triples with elements* $\leq n$ *is* $\sim n/2\pi$.

In the proof of Theorem 2.3, we utilize a function which is multiplicative on the square-free integers which we define by

$$\rho_s(p) = \begin{cases} 2 & \text{if } p \nmid s \\ 2 & \text{if } p \mid s \text{ and } p = 2 \\ 1 & \text{if } p \mid s \text{ and } p \neq 2 \end{cases}$$

for a prime p and an integer $s \geq 2$. In particular, we exercise the following fact.

Lemma 2.4. *Let* d *be a square-free positive integer. The number of* $t \leq s$ *such that* d *divides* $s^2 - t^2$ *is*

$$\frac{\rho_s(d)s}{d} + O(\rho_s(d)).$$

Proof. We'll establish a base case, then proceed by induction. Let d denote a square-free integer throughout this proof. Fix an integer $s \geq 2$ and let d' be a prime number. Counting $t \leq s$ such that $d' \mid s^2 - t^2$, we consider two cases. Suppose $d' \mid s$. We're then only interested in $t \leq s$ which are divisible by d', of which

$$\left\lfloor \frac{s}{d'} \right\rfloor = \frac{s}{d'} + O(1) = \frac{\rho_s(q)s}{d'} + O(\rho_s(d'))$$

exist.

Now suppose $d' \nmid s$. If $d' \mid s^2 - t^2$, then we must have $t \equiv \pm s \pmod{d'}$. For $\varepsilon \in \{0, 1, 2\}$, there are

$$2\left\lfloor \frac{s}{d'} \right\rfloor + \varepsilon = \frac{\rho_s(d')s}{d'} + O(\rho_s(d'))$$

such $t \leq s$. This establishes the base case where d is divisible by exactly one prime number.

Now, assume our assertion is true for d divisible by n primes. Consider some $d = d'q$ with d' divisible by n primes. Again, we consider two cases. First, suppose $q \mid s$. We'd like to count the number of $t \leq s$ with $d' \mid s^2 - t^2$ that also have $q \mid t$. With this in mind, we write

$$s^2 - t^2 = d'u, \qquad s = q\alpha, \qquad t = q\beta$$

for some positive integers u, α, and β. This leaves us to count the solutions for $\beta \leq \alpha$ in the equation

$$q^2(\alpha^2 - \beta^2) = d'u.$$

Since $(d', q) = 1$, we're counting β where $d' \mid \alpha^2 - \beta^2$. Utilizing our inductive hypothesis, this is

$$\frac{\rho_s(d')\alpha}{d'} + O(\rho_s(d')) = \frac{\rho_s(d)s}{d} + O(\rho_s(d)).$$

Now, suppose $q \nmid s$. If some prime $p \mid d'$ has $p \mid s$, we may switch the role of p and q to use the previous case. Thus, without loss of generality, we may assume $(d, s) = 1$. It suffices to count the number of $t \leq s$ such that $t \equiv \pm s \pmod{p}$ for all primes $p \mid d$. By the Chinese Remainder Theorem, we know there are $\rho_s(d)$ such t between ud and $(u+1)d$ for each integer u. It follows that this number is

$$\rho_s(d)\left\lfloor \frac{s}{d} \right\rfloor + O(\rho_s(d)) = \frac{\rho_s(d)s}{d} + O(\rho_s(d)).$$

□

Definition 2.5. Let $\pi(x)$ denote the number of primes less than or equal to x.

An indispensable tool used throughout is the *Prime number theorem*.

Theorem 2.10. *$\pi(x) \sim x/\log x$, or equivalently, $\sum_{p\leq x} \log p \sim x$.*

Another asympototic result used in this chapter is a strengthened form of Dirichlet's theorem on primes in arithmetic progressions.

Theorem 2.11. *Let $a \in \mathbb{Z}$ and $m \geq 2$ be a positive integer relatively prime to a. Then $\sum_{\substack{p\leq x \\ p\equiv a \pmod m}} p^{-1} \sim \varphi(m)^{-1} \log\log x$.*

2.3 The Proof of Theorem 2.1

We begin by examining a graph.

Definition 2.6. Construct the graph G_n in the following manner. Take n vertices and label each uniquely using labels from the set $\{1, 2, \ldots, n\}$. Afterwards, join with an edge each pair of vertices with labels participating together in a Pythagorean triple with elements $\leq n$.

May we find $\chi(G_n)$, we'll have found the least number of colors required to color $\{1, 2, \ldots, n\}$ so that each Pythagorean triple $\leq n$ is 3-colored. From Theorem 2.6 and Lemma 2.3, we know

$$\begin{aligned}\chi(G_n) &\leq 1 + \Delta(G_n) \\ &= 1 + \max_{m\in[n]} P(m) \\ &= \frac{1}{2} \max_{m\in[n]} \left\{ |2h-1| \prod_{j=1}^{y+\ell} (2e_j - 1) + \prod_{j=1}^{y} (2e_j - 1) \right\}\end{aligned}$$

where h, y, ℓ, and the e_j's are dependent on m as in Lemmas 2.1 and 2.2. The above is less than

$$\max_{m\leq n} |2h+2| \prod_{j=1}^{y+\ell} (2e_j + 2) \leq \max_{m\leq n} 2^{\omega(m)+1} d(m) < \max_{m\leq n} 2d(m)^2.$$

Evoking Remark 2.3, we find $\chi(G_n) \leq 4^{(1+o(1))\log m/\log\log m}$.

This bound can be improved with an additional argument. Let

$$m = \alpha_1^{\gamma_1} \dots \alpha_u^{\gamma_u} \beta_1^{\gamma_{u+1}} \dots \beta_v^{\gamma_{u+v}}$$

be the canonical prime factorization of m where

$$\alpha_i \leq \frac{\log n}{(\log\log n)^2} \quad \text{and} \quad \beta_i > \frac{\log n}{(\log\log n)^2}.$$

From our previous argument, we know

$$\chi(G_n) \leq \max_{m\in[n]} \left\{ \prod_{j=1}^{u} (2\gamma_j - 1) \prod_{j=u+1}^{u+v} (2\gamma_j - 1) \right\}. \tag{2.3.1}$$

By inspection, we have $2\gamma_j - 1 \leq 3^{\gamma_j/2}$ for $1 \leq \gamma_j \leq 4$. Indeed, for $\gamma_j > 4$ this remains true by examining the derivative (with respect to γ_j) of each side of the inequality. As such, $2\gamma_j - 1 < 3^{\gamma_j/2}$ for all $\gamma_j \geq 1$. By Theorem 2.10, we find

$$\max_{m\in[n]} \prod_{j=u+1}^{u+v} (2\gamma_j - 1) \leq \max_{m\in[n]} \sqrt{3}^{\sum_{j=u+1}^{u+v} \gamma_j} \leq \sqrt{3}^{(1+o(1))\log n/\log\log n}. \tag{2.3.2}$$

To bound the first product in (2.3.1), we note $u \leq \pi(\log n/(\log\log n)^2)$. Since $2^{\gamma_j} \leq n$ for every $j \leq u$, we get each $\gamma_j \leq \log_2 n \leq 2\log n$ for $n \geq 1$. Thus,

$$\prod_{j=1}^{u} |2\gamma_j - 1| \leq \prod_{j=1}^{u} (4\log n) = (4\log n)^{\pi(\log n/(\log\log n)^2)}.$$

Using

$$4\log n = \exp(\log\log n + \log 4) \leq \exp(2\log\log n)$$

and

$$\pi(\log n/(\log\log n)^2) \leq 2\log n/(\log\log n)^3$$

for n large, we obtain

$$\prod_{j=1}^{u} |2\gamma_j - 1| \leq \exp(4\log n/(\log\log n)^2) = 3^{C\log n/(\log\log n)^2} \tag{2.3.3}$$

for some constant C. Hence, (2.3.2) and (2.3.3) in conjunction with (2.3.1) yields the desired bound on $\chi(G_n)$.

2.4 Outline of the Proof of Theorem 2.2

Let n be a positive integer and $\xi(x)$ be some positive, increasing function tending to infinity.

Definition 2.7. Define $\nu_2(m)$ to be the 2-adic order of m. That is, the number of factors of 2 in the canonical factorization of m.

We'll assign to each positive integer $m \leq n$ an ordered pair (u, v). Similar to a non-trivial approach used to color $\{1, 2, \ldots, n\}$ so that triples $\leq n$ are not monochromatic, we begin by letting u be $\nu_2(m)$ if $\nu_2(m) \leq \xi(n)$ and 0 otherwise. Appealing to Theorem 2.5, we find that this will color a and c differently from b "most" of the time in a sense to be made exact.

Remark 2.4. Notice in Theorem 2.5 that both a and c contain at least one less factor of 2 than b. This is why the scheme above works. If we don't restrict u to taking values $\leq \xi(n)$, we could obtain a $O(\log n)$-coloring of $\{1, 2, \ldots, n\}$ so that each Pythagorean triple with elements $\leq n$ is not monochromatic.

One may find an upper bound on the number of Pythagorean Triples with elements $\leq n$ and c such that $\nu_2(c) > \xi(n)$. These are the cases where the coloring scheme may fail in the sense above.

For $\xi(n) \leq \alpha \leq \log_2 n$, we may take each Pythagorean triple $\leq n/2^\alpha$ and multiply each term in the triple by 2^α, resulting in a triple $\leq n$ whose a and c elements have 2-adic order too large. Adding the number of such triples up and utilizing Theorem 2.8 provides the following overestimate.

$$\sum_{\alpha=\xi(n)}^{\log_2 n} \Omega\left(\frac{n}{2^\alpha}\right) \ll n \sum_{\alpha=\xi(n)}^{\log_2 n} \frac{1}{2^\alpha} \log \frac{n}{2^\alpha} \ll \frac{n \log n}{2^{\xi(n)}}$$

Remark 2.5. It follows from Theorem 2.8 that the ratio of Pythagorean Triples for which b is colored the same as a or c is $\ll 1/2^{\xi(n)} \to 0$.

It's left to define v. To do this, we'll prove the existence of a function $\kappa : \mathbb{N} \to X$, for some set X, such that $\kappa(a) \neq \kappa(c)$ "most" of the time. Additionally, the range of κ, when restricted to the domain $\{m : m \leq n\}$, will have cardinality sufficiently small so that assigning v the value of $\kappa(m)$ will provide us with the desired result. The construction of κ will depend largely on the existence of certain covering systems. It will be the goal of the next section to develop the idea by which we may construct such systems and why they work.

2.5 The Proof of Theorem 2.2

Let $n = \prod_{i=1}^{r} p_i$ be an odd square-free integer whose prime factors are indexed so that $p_i < p_j$ for $i < j$. Lifting these restrictions from n will be a topic discussed at the end of the proof.

Definition 2.8. For ℓ with $1 \leq \ell \leq r$, we define the following set of residue classes.

$$K_{n,\ell} := \left\{ \lambda \prod_{i<\ell} p_i \pmod{\prod_{i\leq\ell} p_i} \,:\, \lambda \in \{1, 2, \ldots, p_\ell - 1\} \right\}$$

We have the following lemma.

Lemma 2.5. *The collection of residue classes* $K_n := (\cup_{\ell\geq 1} K_{n,\ell}) \cup \{0 \pmod n\}$ *is an* exact *covering.*

Proof. Each integer is contained in $\lambda \pmod{p_1}$ for exactly one $\lambda \in \{1, 2, \ldots, p_1 - 1\}$ except for the integers which are divisible by p_1. Each such integer divisible by p_1 is contained in $p_1\lambda \pmod{p_1 p_2}$ for exactly one $\lambda \in \{1, 2, \ldots, p_2 - 1\}$ except for those divisible by $p_1 p_2$. Continuing in this manner, we find that each integer is contained in exactly one residue class of exactly one $K_{n,\ell}$ except for the integers divisible by n, which are contained in $0 \pmod n$. □

Now, for such a covering K_n, we may have $\kappa : \mathbb{N} \to K_n$ so that each natural number is sent to the residue class in K_n in which it is contained. Note κ is well-defined by Lemma 2.5.

Remark 2.6. It's our aim to show that κ has the desired properties explained in the previous section. That is, for each integer $m \leq n$, assigning v the value of $\kappa(m)$ we wish for the proportion of triples with elements $\leq n$ that have $\kappa(a) = \kappa(c)$ to vanish as $n \to \infty$ and the range of κ to have cardinality $\ll (\log n)^2 / \log\log n$.

For k, let $*_\ell$ denote the conditions: (i) $\prod_{i=1}^{\ell-1} p_i \mid k$ and (ii) $p_\ell \nmid k$. Consider a Pythagorean triple with a representation (see Remark 2.2) such that, for some ℓ, k satisfies $*_\ell$ and t has $p_\ell \nmid t$. If we were to have $\kappa(a) = \kappa(c)$ here, then $k(s^2 - t^2) \equiv k(s^2 + t^2) \pmod{p_\ell}$. Since k is invertible, one obtains $p_\ell \mid t$, an impossibility. It's left to find the proportion of Pythagorean triples with elements $\leq n$ which are represented by k and t which don't have these properties.

Remark 2.7. Heuristically, this should be bounded above (asymptotically) by $1/p_1$. The next aim is to prove this assertion.

We begin with a useful fact.

Lemma 2.6. *Let $A_1, A_2, \ldots, A_k$ be such that $0 \leq A_i$ and $\sum_{i=1}^k A_i \leq 1$. For $r_1, r_2, \ldots r_k$ with $0 \leq r_i$, we have $\sum_{i=1}^k r_i A_i \leq \max_i r_i$.*

The proof of this is immediate and omitted. Instead of counting the Pythagorean triples which don't have the desired coloring directly, we'll instead examine certain classes of Pythagorean triples.

Definition 2.9. Let Ω' be the number of triples with elements $\leq M \leq n$ where $\kappa(a) = \kappa(c)$, Ω_ℓ be the number of triples with elements $\leq M$ having a representation satisfying $*_\ell$, and Ω'_ℓ be the number of triples with elements $\leq M$ having a representation satisfying $*_\ell$ and $p_\ell \mid t$.

By Lemma 2.6, we have

$$\frac{\Omega'}{\Omega} = \sum_{\ell=1}^{r} \frac{\Omega'_\ell}{\Omega} = \sum_{\ell=1}^{r} \frac{\Omega'_\ell}{\Omega_\ell} \cdot \frac{\Omega_\ell}{\Omega} \leq \max_\ell \left(\frac{\Omega'_\ell}{\Omega_\ell} \right).$$

Remark 2.8. Should we find appropriate bounds on Ω'_ℓ and Ω_ℓ, we'll be able to prove Ω'/Ω vanishes as $n \to \infty$.

For ease of reading and clarity of exposition, we introduce some notation. Given n as considered in the previous section, we write $M' = M/\prod_{i=1}^{\ell-1} p_i$ and $p = p_\ell$. By fixing s and t, and writing $t = p\tau$, then counting the number of permissible values for k, we have Ω'_ℓ is less than or equal to

$$\begin{aligned}
&\sum_{1 \leq s \leq \sqrt{M'}} \sum_{1 \leq \tau \leq \sqrt{M'}} \frac{M'}{s^2 + p^2\tau^2} \\
&\qquad \leq \sum_{1 \leq \tau \leq \sqrt{M'}} \sum_{1 \leq s \leq p\tau} \frac{M'}{s^2 + p^2\tau^2} + \sum_{1 \leq \tau \leq \sqrt{M'}} \sum_{p\tau < s \leq \sqrt{M'}} \frac{M'}{s^2 + p^2\tau^2} \\
&\qquad \leq \sum_{1 \leq \tau \leq \sqrt{M'}} \sum_{1 \leq s \leq p\tau} \frac{M'}{p^2\tau^2} + \sum_{1 \leq \tau \leq \sqrt{M'}} \sum_{p\tau < s < \infty} \frac{M'}{s^2} \\
&\qquad \leq \sum_{1 \leq \tau \leq \sqrt{M'}} \frac{M'}{p\tau} + \sum_{1 \leq \tau \leq \sqrt{M'}} \frac{M'}{p\tau} \\
&\qquad \leq \frac{2M'}{p} \left(1 + \frac{1}{2} \log M' \right) \ll \frac{M'}{p} \log M'.
\end{aligned}$$

Now we find a lower bound on Ω_ℓ. We proceed in similar fashion, but instead consider only even values of t and odd values of s, writing $t = 2v$ and $s = 2u - 1$. In addition, we'll impose the conditions $1 \leq v \leq \sqrt{M'/32}$ and $v < u \leq 2v$. Note that $t \leq s \leq 4v$ and $s^2 + t^2 \leq 20v^2 \leq 20(M'/32) < M'$ so that these conditions are

actually restrictions on s and t. Hence, Ω_ℓ is

$$\begin{aligned}
&\gg M' \sum_{1\le v\le\sqrt{M'/32}} \sum_{\substack{v<u\le 2v\\(2v,2u-1)=1}} \frac{1}{u^2+v^2} \\
&\qquad \ge M'\left(1-\sum_{q \text{ prime}} q^{-2}\right) \sum_{1\le v\le\sqrt{M'/32}} \sum_{v<u\le 2v} \frac{1}{(2v)^2+v^2} \\
&\qquad \gg M' \sum_{1\le v\le\sqrt{M'/32}} \frac{v}{(2v)^2+v^2} \\
&\qquad = (M'/5) \sum_{1\le v\le\sqrt{M'/32}} \frac{1}{v} \\
&\qquad \gg M' \log M'.
\end{aligned}$$

As a result of our bounds on Ω'_ℓ and Ω_ℓ, we find $\max_\ell(\Omega'_\ell/\Omega_\ell) \ll 1/p_1$. Thus, by Remark 2.8, $\Omega'/\Omega \to 0$ provided $p_1 \to \infty$.

To complete the proof, we consider the set $\mathcal{S} = \left\{\prod_{x<p\le 2x} p : x > 2\right\}$. Clearly, this is a subset of the square-free odd integers. For $n \in \mathcal{S}$, we'll show that the coloring we've constructed for $\{1, 2, \ldots, n\}$ has $\ll \xi(n)\log^2 n/\log\log n$ colors.

The number of residue classes in K_n is less than $\sum_{p|n} p < (\pi(2x)-\pi(x))2x \ll \frac{x^2}{\log x}$ by Theorem 2.10. Further, $\log n = \sum_{p|n}\log p \sim x$, which allows us to conclude that the number of residue classes in K_n is $\ll \log^2 n/\log\log n$. The desired bound on the number of colors used follows. Also, by Remark 2.5, we see that the ratio of Pythagorean triples with elements $\le n$ which are not 3-colored is $\ll \max\{2^{-\xi(n)}, 1/x\}$, or $\ll \max\{2^{-\xi(n)}, 1/\log n\}$, as desired.

We wish to extend this to arbitrary $n \in \mathbb{N}$. To do so, we use the following fact.

Lemma 2.7. *For $\varepsilon > 0$ there exists an infinite sequence $\{s_i\}_{i=1}^\infty$ with $s_i \in \mathcal{S}$ such that $s_i < s_{i+1} < s_i^{1+\varepsilon}$.*

Proof. Fix $\varepsilon > 0$. For all $\delta > 0$ there exists sufficiently large x such that $x_1 > x$ and

$s_1 \in \mathcal{S}$ with $s_1 = \prod_{x_1 \leq p < 2x_1} p$ has

$$e^{(1-\delta)x_1} < s_1 < e^{(1+\delta)x_1}$$

by Theorem 2.10. Planning to fix such an x_1, we first want to choose δ such that there exists some x_2 with

$$e^{(1+\delta)x_1} < e^{(1-\delta)x_2} < e^{(1+\delta)x_2} < e^{(1-\delta)(1+\varepsilon)x_1} \tag{2.5.1}$$

so that letting $x_2 = \prod_{x_2 \leq p < 2x_2} p$ will force $s_1 < s_2 < s_1^{1+\varepsilon}$. This will occur if

$$x_1 < \frac{1-\delta}{1+\delta} x_2 \quad \text{and} \quad x_2 < \frac{1-\delta}{1+\delta}(1+\varepsilon)x_1. \tag{2.5.2}$$

Choosing δ small enough so that

$$\frac{(1+\delta)^2(1+\varepsilon/2)}{(1-\delta)^2(1+\varepsilon)} < 1,$$

letting $x_2 = x_1 \frac{1+\delta}{1-\delta}(1+\varepsilon/2)$ satisfies (2.5.2), thus satisfying (2.5.1). As such, fix an x_1 satisfying the properties at the beginning of the proof. Recursively, for $i \geq 2$, pick $x_i = x_{i-1}\frac{1+\delta}{1-\delta}(1+\varepsilon/2)$, letting $s_i = \prod_{x_i \leq p < 2x_i} p$ so that $\{s_1, s_2, \ldots\} \subseteq \mathcal{S}$ with $s_i < s_{i+1} < s_i^{1+\varepsilon}$. □

By Lemma 2.7, our result extends as written in Theorem 2.2 to any $n \in \mathbb{N}$ by the logarithmic nature of our bound on the number of colors used. That is, given an arbitrary $n \in \mathbb{N}$ we take the least $m \in \mathcal{S}$ such that $n \leq m$ and restrict the coloring of $\{1, 2, \ldots, m\}$ induced by our methods to the set $\{1, 2, \ldots, n\}$.

Letting $\xi(n) = \log\log n$, we have the following corollary to Theorem 2.2.

Corollary 2.2. *There exist $O(\log^2 n)$-colorings of $\{1, 2, \ldots, n\}$ such that the proportion of Pythagorean triples with elements $\leq n$ which are not 3-colored vanishes with order at most $(\log n)^{-\log 2}$ as $n \to \infty$.*

2.6 The Proof of Theorem 2.3

Again, let n be a positive integer and $\xi(n)$ be some positive, increasing function tending to infinity. We'll assign to each positive integer $m \leq n$ an ordered pair (u, v). In fact, we define u exactly the same as in the previous proof. Reference Remark 2.5 and its preceding material. However, we take a different approach when assigning v a value.

Theorem 2.12. *For a prime p congruent to 3 modulo 4, -1 is not a quadratic residue modulo p.*

This yields a useful fact.

Corollary 2.3. *Any number of the form $s^2 + t^2$ with $(s, t) = 1$ can not be divisible by a prime congruent to 3 modulo 4.*

If we allowed v to be the number of distinct primes congruent to 3 modulo 4 that divide each m, the a and c terms in a Pythagorean triple with elements $\leq n$ could only have the same coloring if each such prime dividing $s^2 - t^2$ also divided k. If the previous sections were skipped, see Remark 2.2.

Two concerns arise. First, we need to count the number of Pythagorean triples that this coloring fails for. It also becomes necessary to limit how large we allow v to become since we'd like to use few colors. To limit this value, we'll let v be the number of distinct primes congruent to 3 modulo 4 dividing m if this number is $\leq z < \xi(n)$ and 0 otherwise, where z is to be chosen later.

Remark 2.9. That is, for some Pythagorean triple (a, b, c) with elements $\leq n$, the only way a and c may be colored the same is if all $p \leq z$ with $p \equiv 3 \pmod 4$ that have $p \mid s^2 - t^2$ also have $p \mid k$.

Definition 2.10. Let $A(s, n)$ is the number of pairs (t, k) with $t \leq s$ and $k(s^2+t^2) \leq n$ such that all $p \leq z$ with $p \equiv 3 \pmod 4$ that have $p \mid s^2 - t^2$ also have $p \mid k$.

To over count the number of Pythagorean triples where a and c fail to be colored differently, we consider $\sum_{s\leq\sqrt{n}} A(s,n)$. In addition, to over count $A(s,n)$, we may instead consider (t,k) with $ks^2 \leq n$. This will simplify the following work. Let $\mathcal{P}$ be the product of all primes $\leq z$ that are congruent to 3 modulo 4.

First, we take the number of pairs (t,k) with $t \leq s$ and $k \leq n/s^2$, then we subtract from that, for each $p \mid \mathcal{P}$, the number of pairs (t,k) such that $p \mid s^2 - t^2$ and p is coprime to k. We've under counted, so we must add back to this the number of pairs (t,k) such that, for all $p_1p_2 \mid \mathcal{P}$, $p_1p_2 \mid s^2 - t^2$ and p_1p_2 is coprime to k. Continuing in this manner by the principle of inclusion-exclusion, we may determine that

$$A(s,n) \leq \sum_{d\mid\mathcal{P}} \mu(d)\left(\frac{\rho_s(d)\varphi(d)n}{d^2s} + O\left(\rho_s(d)\varphi(d)\left(\frac{n}{ds^2}+\frac{s}{d}+1\right)\right)\right)$$

by Lemma 2.4 and the fact that the number of $k \leq n/s^2$ coprime to d is $\varphi(d)n/(ds^2) + O(\varphi(d))$. We use that there are at most $\pi(z) \leq z$ primes dividing $\mathcal{P}$. For the error term above, observe that $d \mid \mathcal{P}$ implies that

$$\rho_s(d)\varphi(d)\left(\frac{n}{ds^2}+\frac{s}{d}+1\right) \leq 2^z d\left(\frac{n}{ds^2}+\frac{s}{d}+1\right) \leq \frac{n\,2^z}{s^2} + 2^z s + 2^z d \leq \frac{n\,2^z}{s^2} + 2^z s + 2^z z^z.$$

Also,

$$\sum_{d\mid\mathcal{P}} |\mu(d)| \leq \sum_{d\mid\mathcal{P}} 1 \leq 2^z.$$

Hence,

$$A(s,n) \leq \left(\sum_{d\mid\mathcal{P}} \mu(d)\frac{\rho_s(d)\varphi(d)}{d^2}\right)\frac{n}{s} + O\left(\frac{n\,2^{2z}}{s^2} + 2^{2z}s + 2^{2z}z^z\right). \tag{2.6.1}$$

The multiplicativity of ρ_s and φ implies that

$$\begin{aligned}
\sum_{d\mid\mathcal{P}} \mu(d)\frac{\rho_s(d)\varphi(d)}{d^2} &= \prod_{\substack{p\leq z\\ p\equiv 3 \pmod 4}} \left(1 - \frac{\rho_s(p)\varphi(p)}{p^2}\right) \\
&\leq \prod_{\substack{p\leq z\\ p\equiv 3 \pmod 4}} \left(1 - \frac{p-1}{p^2}\right) \\
&= \prod_{\substack{p\leq z\\ p\equiv 3 \pmod 4}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p\leq z\\ p\equiv 3 \pmod 4}} \left(1 + \frac{1}{p(p-1)}\right),
\end{aligned}$$

where

$$\sum_{\substack{p\le z\\ p\equiv 3 \pmod 4}} \log\left(1+\frac{1}{p(p-1)}\right) < \sum_{p} \log\left(1+\frac{1}{p(p-1)}\right)$$

$$= \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} \sum_{p} \left(\frac{1}{p(p-1)}\right)^n$$

which is easily seen to converge. Further, by Theorem 2.11,

$$\sum_{\substack{p\le z\\ p\equiv 3 \pmod 4}} -\log\left(1-\frac{1}{p}\right) = \sum_{n=1}^{\infty} n^{-1} \sum_{\substack{p\le z\\ p\equiv 3 \pmod 4}} p^{-n}$$

$$\sim \sum_{\substack{p\le z\\ p\equiv 3 \pmod 4}} p^{-1} + \sum_{n=2}^{\infty} n^{-1} \sum_{\substack{p\le z\\ p\equiv 3 \pmod 4}} p^{-n}$$

$$\sim \frac{1}{2}\log\log z + \sum_{n=2}^{\infty} (\sum_{p} p^{-2})^{n/2}$$

$$\sim \frac{1}{2}\log\log z$$

since $\sum_p p^{-2} < 1$. In light of these facts, in conjunction with (2.6.1), we deduce that

$$A(s,n) \ll \frac{n}{s\sqrt{\log z}} + \frac{n\,2^{2z}}{s^2} + 2^{2z}s + 2^{2z}z^z.$$

Using the above estimate for $A(s,x)$, our bound on the number of Pythagorean triples whose a and c terms are colored differently is now

$$\sum_{s\le\sqrt{n}} A(s,n) \ll \frac{n\log n}{\sqrt{\log z}} + n\,2^{2z} + 2^{2z}z^z\sqrt{n}. \tag{2.6.2}$$

We want this to be asymptotically small compared to $\Omega(n) \asymp n\log n$. Recall also that we want $z \le \xi(n)$. To obtain what we want, we can take

$$z = \min\{\log\log\log n, \xi(n)\}. \tag{2.6.3}$$

Technically, we've used $\ll \xi(n)^2$ colors here, but substituting $\sqrt{\xi(n)} \leftarrow \xi(n)$ gives us Theorem 2.3 as stated at the beginning of the chapter.

Remark 2.1. Utilizing Remark 2.5 and (2.6.3) with (2.6.2), we may easily deduce the bound on the proportion of Pythagorean triples which are not 3-colored that is given in Theorem 2.3 with respect to the comment above.

2.7 The Proof of Theorem 2.4

To begin, we'll state the coloring of $\mathbb{N}$ that we use. First, color all positive even integers as 0. Next, color each odd positive integer divisible by a prime congruent to 3 modulo 4 as 1. Color the remaining elements of $\mathbb{N}$ as 2. By Corollary 2.3, and Theorem 2.5, we see that if a primitive Pythagorean triple with elements $\leq n$ happens to not be 3 colored, it must be that $a = s^2 - t^2$ has no prime divisors congruent to 3 modulo 4. It's left to count how many times this can happen.

According to Theorem 2.5, for an upper bound it will suffice to count

$$\sum_{s \leq \sqrt{n}} \Big\{ \text{the number of } t \leq s \text{ such that } p \mid (s-t) \Rightarrow p \equiv 1 \pmod 4 \text{ or } p > z \Big\}$$

where z is some number to be chosen later, dependent on n. By an argument similar to one used in the previous section, we find this is

$$\sum_{s \leq \sqrt{n}} \left(s \prod_{\substack{p \equiv 3 \pmod 4 \\ p \leq z}} \left(1 - \frac{1}{p}\right) + O\Big(2^{\pi(z)}\Big) \right) \ll \frac{n}{\sqrt{\log \log n}}.$$

Letting $z = \log n$ and dividing by the total number of primitive Pythagorean triples with elements $\leq n$ (See Theorem 2.9), we have a bound of

$$\ll \frac{1}{\sqrt{\log \log n}}$$

on the number of primitive Pythagorean triples with elements $\leq n$ that are not 3-colored.

Chapter 3

The Reducibility of Constant-Perturbed Products of Cyclotomic Polynomials

The results in this chapter are joint work with Joshua Harrington from the University of South Carolina and Lenny Jones from Shippensburg University.

3.1 Introduction

Throughout this chapter, unless stated otherwise, when we say "irreducible", we mean "irreducible over $\mathbb{Q}$". Let $g(x) = (x-a_1)(x-a_2)\cdots(x-a_n)$, where the a_i are distinct integers. In 1908, Schur raised the question of the irreducibility of polynomials of the form $f_\pm(x) = g(x) \pm 1$. One year later, Westlund [19] showed that $f_-(x)$ is always irreducible, and that if $f_+(x)$ is reducible, then $f_+(x)$ must be the square of a polynomial. Also in 1909, Flügel [6] showed that $f_+(x)$ is reducible if and only if there exists an integer d such that $f_+(x-d) = (x-1)^2$ or $f_+(x-d) = (x^2-3x+1)^2$. Since that time, numerous authors have addressed variations and generalizations of these questions. For example, Seres [17], answering another question of Schur, proved that the polynomial $g(x)^{2^n} + 1$ is irreducible for all positive integers n. For some more recent generalizations, and a complete history and bibliography chronicling these results, see [8].

In this chapter we investigate a slightly different modification of Schur's original question. Our main, although not exclusive, focus is on the reducibility of polynomials

of the form

$$\prod_{i=1}^{k} \Phi_{m_i}(x) + d \tag{3.1.1}$$

with $d \in \mathbb{Z}^+$, where $\Phi_{m_i}(x)$ denotes the cyclotomic polynomial of index m_i, and the cyclotomic polynomials in (3.1.1) are not necessarily distinct. The special case of $k = 1$ is treated separately in Section 3.3 for $d > 0$, and in Section 3.6 for $d \in \mathbb{Z}$ with $d \notin \{-1, 0, 1\}$.

We should point out that perturbations of products of cyclotomic polynomials have been studied by other authors, but not to examine these polynomials for irreducibility. In [12], the authors perturb the middle coefficient, and also the two adjacent coefficients, to investigate the Mahler measure of the resulting polynomials.

One interesting consequence of our investigations in this chapter is that we are able to construct, for any positive integer N, an infinite set S of cyclotomic polynomials such that 1 plus the product of any k (not necessarily distinct) polynomials from S, where $k \not\equiv 0 \pmod{2^{N+1}}$, is reducible (see Theorem 3.8). In Section 3.5 we provide a non-cylotomic version of this result.

3.2 Preliminaries

We begin this section with some definitions and notation. Let n be a positive integer, and let $\prod_{i=1}^{k} p_i^{a_k}$ be its canonical factorization into distinct prime powers. Then the *squarefree kernel* of n, denoted $\kappa(n)$, is $\prod_{i=1}^{k} p_i$.

Let $f(x), g(x) \in \mathbb{Z}[x]$ with respective degrees of m and n, and respective leading coefficients of a and b. Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ and $\beta_1, \beta_2, \ldots, \beta_n$ be the respective zeros of $f(x)$ and $g(x)$. Then the *resultant* of $f(x)$ and $g(x)$, denoted $R(f, g)$, is defined as

$$R(f, g) = a^n b^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j).$$

It is easy to see from this definition that

$$R(f, g) = a^n \prod_{i=1}^{m} g(\alpha_i) \quad \text{and} \quad R(f, g) = (-1)^{nm} R(g, f). \tag{3.2.1}$$

The *reciprocal* of a polynomial $f(x) \in \mathbb{Z}[x]$ is defined to be the polynomial

$$\widetilde{f}(x) := x^{\deg f} f\left(\frac{1}{x}\right).$$

We say that $f(x)$ is *reciprocal* if $f(x) = \pm\widetilde{f}(x)$. Suppose $f(0) \neq 0$ and that $f(x)$ factors over $\mathbb{Q}$ into irreducibles as $g_1(x)g_2(x)\cdots g_k(x)$, where $g_i(x)$ is reciprocal exactly when $1 \leq i \leq j$ and the leading coefficient of each $g_i(x)$ is positive. Then $g_1(x)g_2(x)\cdots g_j(x)$ is called the *reciprocal part* of f and $g_{j+1}(x)\cdots g_k(x)$ is called the *non-reciprocal part* of f.

For the sake of completeness, we list the following well-known identities for cyclotomic polynomials, which we use in several proofs.

Proposition 3.1. *Let p be an odd prime.*

1. $\Phi_{pn}(x) = \dfrac{\Phi_n(x^p)}{\Phi_n(x)}$ *if* $n \not\equiv 0 \pmod{p}$.
2. $\Phi_{pn}(x) = \Phi_n(x^p)$ *if* $n \equiv 0 \pmod{p}$.
3. $\Phi_{2n}(x) = \Phi_n(-x)$ *if* $n \equiv 1 \pmod{2}$.

We present, without proof, some additional theorems that are useful in this chapter. The first theorem is originally due to E. Lehmer [11].

Theorem 3.1. *Suppose that $n \geq m \geq 1$. Then*

$$R\left(\Phi_n(x), \Phi_m(x)\right) = \begin{cases} 0 & \text{if } m = n, \\ p^{\phi(m)} & \text{if } \frac{n}{m} = p^e \text{ for some positive integer } e, \\ 1 & \text{otherwise,} \end{cases}$$

where ϕ is Euler's ϕ-function.

The next two theorems are due to Capelli [15].

Theorem 3.2. *Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{Q}[x]$ with $f(x)$ irreducible. Suppose that $f(\alpha) = 0$. Then $f(g(x))$ is reducible over $\mathbb{Q}$ if and only if $g(x) - \alpha$ is reducible over $\mathbb{Q}(\alpha)$.*

Theorem 3.3. *Let $r \geq 2$ be an integer and let $\alpha \in \mathbb{C}$ be algebraic. Then $x^r - \alpha$ is reducible over $\mathbb{Q}(\alpha)$ if and only if either there is a prime p dividing r such that $\alpha = \beta^p$ for some $\beta \in \mathbb{Q}(\alpha)$ or $4 \mid r$ and $\alpha = -4\beta^4$ for some $\beta \in \mathbb{Q}(\alpha)$.*

If $f(x) = \sum_{j=0}^{n} a_j x^j$, we define $\|f\| := \sqrt{\sum_{j=0}^{n} a_j^2}$. The following theorem is due to Filaseta, Ford, and Konyagin [5].

Theorem 3.4. *Suppose that $f(x), g(x) \in \mathbb{Z}[x]$ with $f(0) \neq 0$, $g(0) \neq 0$ and*

$$\gcd_{\mathbb{Z}}(f(x), g(x)) = 1.$$

Let r_1 and r_2 denote the number of non-zero terms in $f(x)$ and $g(x)$, respectively. If

$$n \geq \max\left\{2 \cdot 5^{2N-1}, 2 \cdot \max\{\deg f, \deg g\}\left(5^{N-1} + \frac{1}{4}\right)\right\},$$

where

$$N = 2\|f\|^2 + 2\|g\|^2 + 2r_1 + 2r_2 - 7,$$

then the non-reciprocal part of $x^n f(x) + g(x)$ is irreducible or identically 1 or -1 unless one of the following holds:

1. *The polynomial $-f(x)g(x)$ is a p^{th} power for some prime p dividing n.*
2. *For either $\epsilon = 1$ or $\epsilon = -1$, one of $\epsilon f(x)$ and $\epsilon g(x)$ is a 4^{th} power, the other is 4 times a 4^{th} power, and n is divisible by 4.*

3.3 The Reducibility of $\Phi_m(x) + d$ with $d \in \mathbb{Z}^+$

Using Theorems 3.2 and 3.3, we first derive the following useful proposition that allows us to reduce, in many situations, to the case when m is squarefree.

Proposition 3.2. *Let d and m be integers with $m \geq 2$, and let $\kappa(m)$ denote the squarefree kernel of m. Suppose that $|d+1| \neq b^p$ for any $b \in \mathbb{Z}$ and any prime divisor p of m. Then $\Phi_m(x) + d$ is reducible if and only if $\Phi_{\kappa(m)}(x) + d$ reducible.*

Furthermore, if $\kappa(m) = 2n$ for some odd integer $n \geq 3$, then $\Phi_m(x) + d$ is reducible if and only if $\Phi_n(x) + d$ is reducible.

Proof. Let $p_1, p_2, \cdots, p_t$ be distinct primes. Fix $d \in \mathbb{Z}$ so that $|d+1| \neq b^{p_i}$ for any $b \in \mathbb{Z}$ and $i \in \{1, \ldots, t\}$. Let $m = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ with $e_i \in \mathbb{Z}^+$. Then $\kappa(m) = p_1 p_2 \cdots p_t$ and

$$\Phi_m(x) = \Phi_{\kappa(m)}\left(x^{p_1^{e_1-1} p_2^{e_2-1} \cdots p_t^{e_t-1}}\right).$$

We deduce from this that if $\Phi_{\kappa(m)}(x) + d$ is reducible, then $\Phi_m(x) + d$ is reducible. So suppose that $\Phi_{\kappa(m)}(x) + d$ is irreducible and that $\alpha \in \mathbb{C}$ is a zero of $\Phi_{\kappa(m)}(x) + d$. For

$$g(x) = x^{p_1^{e_1-1} p_2^{e_2-1} \cdots p_t^{e_t-1}}$$

we have by Theorem 3.2 that $\Phi_m(x) + d = \Phi_{\kappa(m)}(g(x)) + d$ is reducible over $\mathbb{Q}$ if and only if $g(x) - \alpha$ is reducible over $\mathbb{Q}(\alpha)$. Theorem 3.3 then implies that $g(x) - \alpha$ is reducible over $\mathbb{Q}(\alpha)$ if and only if either $\alpha = b^{p_i}$ for some $b \in \mathbb{Q}(\alpha)$ and some $i \in \{1, 2, \ldots, t\}$ or 8 divides m and $\alpha = -4b^4$ for some $b \in \mathbb{Q}(\alpha)$. However, examining norms gives $\mathcal{N}(\alpha) = \pm(d+1)$, while $\mathcal{N}(b^{p_j}) = \mathcal{N}(b)^{p_j}$ with $\mathcal{N}(b) \in \mathbb{Q}$ and $\mathcal{N}(-4b^4) = \mathcal{N}(2b^2)^2$ with $\mathcal{N}(2b^2) \in \mathbb{Q}$. From this we deduce that $g(x) - \alpha$ is irreducible over $\mathbb{Q}(\alpha)$ since $|d+1| \neq b^{p_j}$ for any $b \in \mathbb{Z}$ and $j \in \{1, \ldots, t\}$.

Now, suppose that $\kappa(m) = 2n$ for some $n \geq 3$. We've already shown that $\Phi_m(x) + d$ is reducible if and only if

$$\Phi_{\kappa(m)}(x) + d = \Phi_{2n}(x) + d = \Phi_n(-x) + d$$

is reducible. Clearly, $\Phi_n(-x) + d$ is reducible if and only if $\Phi_n(x) + d$ is as well. $\square$

$d = 1$

We begin this section with a lemma that gives an explicit formula for evaluating cyclotomic polynomials, whose index is an odd squarefree integer, at certain roots

of unity. While other authors have investigated values of cyclotomic polynomials at roots of unity [4, 10, 13, 14], our result appears to be new.

Lemma 3.1. *Let s be a positive integer, and let $p_1, p_2, \ldots, p_n$ be distinct odd primes such that $p_1 \equiv -1 \pmod{2^s}$ and $p_i \equiv a_i \pmod{2^s}$ for all i with $2 \leq i \leq n$. Suppose that ζ is a primitive 2^rth root of unity, for some integer r with $1 \leq r \leq s$. Then*

$$\Phi_{p_1 p_2 \cdots p_n}(\zeta) = \begin{cases} -\zeta^{-1} & \text{if } n = 1 \\ \zeta^{-\prod_{j=2}^{n}(a_j - 1)} & \text{if } n \geq 2 \end{cases}$$

Proof. When $n = 1$, we have

$$\Phi_{p_1}(\zeta) = \frac{\zeta^{p_1} - 1}{\zeta - 1} = \frac{\zeta^{-1} - 1}{\zeta - 1} = -\zeta^{-1}.$$

The proof is by induction on n for $n \geq 2$. When $n = 2$, we have

$$\Phi_{p_1 p_2}(\zeta) = \frac{\Phi_{p_1}(\zeta^{p_2})}{\Phi_{p_1}(\zeta)} = \frac{-(\zeta^{a_2})^{-1}}{-\zeta^{-1}} = \zeta^{-(a_2 - 1)},$$

and the base case is established. Thus, for $n \geq 3$, we have by induction that

$$\begin{aligned} \Phi_{p_1 p_2 \cdots p_n}(\zeta) = \frac{\Phi_{p_1 p_2 \cdots p_{n-1}}(\zeta^{p_n})}{\Phi_{p_1 p_2 \cdots p_{n-1}}(\zeta)} &= \frac{\Phi_{p_1 p_2 \cdots p_{n-1}}(\zeta^{a_n})}{\Phi_{p_1 p_2 \cdots p_{n-1}}(\zeta)} \\ &= \frac{(\zeta^{a_n})^{-\prod_{j=2}^{n-1}(a_j - 1)}}{\zeta^{-\prod_{j=2}^{n-1}(a_j - 1)}} \\ &= \zeta^{-\prod_{j=2}^{n}(a_j - 1)}. \end{aligned}$$

□

Lemma 3.1 can be used to generate infinite families of polynomials of the form $\Phi_m(x) + 1$ that are reducible. The key idea is to choose the primes in Lemma 3.1 such that $\zeta^{-\prod_{j=2}^{n}(a_j - 1)} = -1$. Using Lemma 3.1, we give two such explicit families.

Theorem 3.5. *Let a be a nonnegative integer. Let m and n be positive integers such that $n \geq 2$ and $2^a \prod_{i=1}^{n} p_i^{b_i}$ is the canonical factorization of m into distinct prime powers. If $p_i \equiv -1 \pmod{2^n}$ for all i, then $\Phi_m(x) + 1$ is reducible.*

Proof. By Proposition 3.2, it is enough to show that $F(x) = \Phi_{p_1 p_2 \cdots p_n}(x) + 1$ is reducible. Let $\zeta = \exp(2\pi i/2^n)$. Since $n \geq 2$ and $a_i = -1$ for all i in Lemma 3.1, we have that

$$\zeta^{-\prod_{j=2}^{n}(a_j-1)} = \zeta^{(-1)^n 2^{n-1}} = -1.$$

Then $F(\zeta) = 0$ and so $F(x)$ is reducible since $F(x)$ is divisible by $\Phi_{2^n}(x)$. □

Theorem 3.6. *Let a be a nonnegative integer. Let m, n and s be positive integers such that $s \geq n \geq 2$ and $2^a \prod_{i=1}^{n} p_i^{b_i}$ is the canonical factorization of m into distinct prime powers. If $p_i \equiv 2^{s-i+1} - 1 \pmod{2^s}$ for all i with $1 \leq i \leq n-1$ and $p_n \equiv 2^{s-n+1} + 1 \pmod{2^s}$, then $\Phi_m(x) + 1$ is reducible.*

Proof. By Proposition 3.2, it is enough to show that $F(x) = \Phi_{p_1 p_2 \cdots p_n}(x) + 1$ is reducible. Let $\zeta = \exp(2\pi i/2^s)$. Then

$$\zeta^{-\prod_{j=2}^{n}(a_j-1)} = \zeta^{-2^{s-n+1}\prod_{j=2}^{n-1}\left(2^{s-j+1}-2\right)} = \left(\zeta^{-\prod_{j=2}^{n-1}\left(2^{s-j}-1\right)}\right)^{2^{s-1}} = -1.$$

Hence, $F(x)$ is reducible since $F(x)$ is divisible by $\Phi_{2^s}(x)$. □

Computer evidence suggests that the condition $p \equiv 3 \pmod{4}$ for some prime p dividing m is necessary for the reducibility of $\Phi_m(x) + 1$ (see Conjecture 3.1). However, it is not sufficient since, for example, $\Phi_{15}(x) + 1$ is irreducible.

We end this section with two conjectures.

Conjecture 3.1. *Let a be a nonnegative integer. Let m be a positive integer such that $2^a \prod_{i=1}^{n} p_i^{b_i}$ is the canonical factorization of m into distinct prime powers. If $p_i \equiv 1 \pmod{4}$ for all i, then $\Phi_m(x) + 1$ is irreducible.*

Remark 3.1. When $n = 2$, the only situation not addressed modulo 4 by Theorem 3.5 (or Theorem 3.6) and Conjecture 3.1 is when $p \equiv -q \pmod{4}$. This situation is ambiguous in the sense that examples exist where $\Phi_{2^a p^b q^c}(x) + 1$ is reducible and examples exist where $\Phi_{2^a p^b q^c}(x) + 1$ is irreducible. One can attempt to dispel this

ambiguity by "splitting" this case into smaller cases modulo higher powers of 2, but this approach does not appear to rectify the problem. For example, if we split this case into four cases modulo 8, then three out of the four cases seem to be unambiguous, but the fourth case, $p \equiv -q \pmod 8$, is again ambiguous.

Conjecture 3.2. *Let n be a positive integer. Then $F(x) = \Phi_n(x) + 1$ is reducible if and only if $F(x)$ has a cyclotomic factor.*

Based on results in this section one might be tempted to strengthen Conjecture 3.2 to state that if $F(x)$ is reducible, then $\Phi_{2^m}(x)$ divides $F(x)$ for some positive integer m. However, this is not true and the smallest counterexample is $n = 195$. In this case, $F(x) = \Phi_{24}(x)g(x)$, where $g(x)$ is irreducible and not cyclotomic.

$d \geq 1$

Lemma 3.2. *Let p be a prime and let d be a positive integer. Then all zeros of $f(x) = \Phi_p(x) + d$ are in $\{z \in \mathbb{C} : |z| > 1\}$.*

Proof. Suppose that $f(\alpha) = 0$. Then $\alpha^p + d\alpha - (d+1) = (\alpha - 1)f(\alpha) = 0$, and so $d + 1 = \alpha^p + d\alpha$. Assume, by way of contradiction, that $|\alpha| \leq 1$. It follows that $d+1 = |\alpha||\alpha^{p-1} + d|$, from which it is clear α must be a $(p-1)^{\text{th}}$ root of unity. Hence, $\alpha = 1$. This is a contradiction since $f(1) \neq 0$. □

Proposition 3.3. *Let a and b be non-negative integers. Let p and q be primes with p odd. Then $\Phi_{2^b p^a}(x) + q - 1$ is irreducible.*

Proof. By Proposition 3.2, it is enough to show that $f(x) = \Phi_p(x)+q-1$ is irreducible. Now assume that $f(x)$ is reducible and write $f(x) = g(x)h(x)$. Then

$$q = f(0) = g(0)h(0).$$

Since q is prime, we may assume without loss of generality that $|h(0)| = 1$. This, however, is a contradiction, since all zeros of $h(x)$ are in $\{z \in \mathbb{C} : |z| > 1\}$ by Lemma 3.2. Hence, $f(x)$ must be irreducible. □

We use Theorem 3.4 to deduce the following result.

Proposition 3.4. *Let d be a positive integer and let $p \geq 2 \times 5^{8(d^2+d+1)-3}$ be a prime. Then $F(x) = \Phi_p(x) + d$ is irreducible.*

Proof. Since $F(x)$ has no zeros in $\{z \in \mathbb{C} : |z| \leq 1\}$ by Lemma 3.2, we conclude that $F(x)$ has no reciprocal factors. Notice then that $F(x)$ is the non-reciprocal part of the polynomial

$$(x-1)F(x) = x^p + dx - (d+1).$$

The proposition then follows immediately from Theorem 3.4 by letting $f(x) = 1$ and $g(x) = dx - (d+1)$. □

The following corollary is an immediate consequence of Proposition 3.2 and Proposition 3.4.

Corollary 3.1. *Let d be a fixed positive integer. Then there are at most finitely many odd primes p, independent of k, such that $\Phi_{p^k}(x) + d$ is reducible.*

$d \geq 2$

Theorem 3.7. *Let a, b, d, m, n be positive integers. Define three infinite families of polynomials of the form $\Phi_m(x) + d$:*

1. $\mathbb{F}_1 = \left\{ \Phi_m(x) + d \,\middle|\, m = 2^a, d = 4n^4 - 1, a \geq 3, n \geq 1 \right\}$,
2. $\mathbb{F}_2 = \left\{ \Phi_m(x) + d \,\middle|\, m = 2^a 3^b, d = 4n^2(n+1)^2 - 1, a \geq 2, b \geq 1, n \geq 1 \right\}$,
3. $\mathbb{F}_3 = \left\{ \Phi_m(x) + d \,\middle|\, m = 2^a 5^b, d = 11, a \geq 0, b \geq 1 \right\}$.

Then, for any i, all polynomials in $\mathbb{F}_i$ are reducible.

Proof. To prove the result for (1), let $F(x) \in \mathbb{F}_1$. Then, since $\Phi_{2^a}(x) = x^{2^{a-1}} + 1$, we have

$$\begin{aligned} F(x) &= \Phi_{2^a}(x) + 4n^4 - 1 \\ &= x^{2^{a-1}} + 4n^4 + 4x^{2^{a-2}}n^2 - 4x^{2^{a-2}}n^2 \\ &= \left(x^{2^{a-2}} - 2x^{2^{a-3}}n + 2n^2\right)\left(x^{2^{a-2}} + 2x^{2^{a-3}}n + 2n^2\right). \end{aligned}$$

To prove the result for (2), let $F(x) \in \mathbb{F}_2$. Then, since $\Phi_{2^a3^b}(x) = x^{2^a3^{b-1}} - x^{2^{a-1}3^{b-1}} + 1$, we have

$$\begin{aligned} F(x) &= \Phi_{2^a3^b}(x) + 4n^2(n+1)^2 - 1 \\ &= x^{2^a3^{b-1}} - x^{2^{a-1}3^{b-1}} + 4n^2(n+1)^2 \\ &= x^{2^a3^{b-1}} + 4n(n+1)x^{2^{a-1}3^{b-1}} - (2n+1)^2x^{2^{a-1}3^{b-1}} + 4n^2(n+1)^2 \\ &\qquad \times \left(x^{2^{a-1}3^{b-1}} + (2n+1)x^{2^{a-2}3^{b-1}} + 2n(n+1)\right). \end{aligned}$$

Finally, to establish the theorem for (3), let $F(x) \in \mathbb{F}_3$. First suppose that $a = 0$. Then, since

$$\Phi_{5^b}(x) = x^{4\cdot5^{b-1}} + x^{3\cdot5^{b-1}} + x^{2\cdot5^{b-1}} + x^{5^{b-1}} + 1,$$

we have

$$\begin{aligned} F(x) &= \Phi_{5^b}(x) + 11 \\ &= x^{4\cdot5^{b-1}} + x^{3\cdot5^{b-1}} + x^{2\cdot5^{b-1}} + x^{5^{b-1}} + 12 \\ &= \left(x^{2\cdot5^{b-1}} - 2x^{5^{b-1}} + 3\right)\left(x^{2\cdot5^{b-1}} + 3x^{5^{b-1}} + 4\right). \end{aligned}$$

Now suppose that $a \geq 1$. Then, since

$$\Phi_{2^a5^b}(x) = x^{2^{a+1}5^{b-1}} - x^{2^{a-1}3\cdot5^{b-1}} + x^{2^a5^{b-1}} - x^{2^{a-1}5^{b-1}} + 1,$$

we have

$$\begin{aligned} F(x) &= \Phi_{2^a5^b}(x) + 11 \\ &= x^{2^{a+1}5^{b-1}} - x^{2^{a-1}3\cdot5^{b-1}} + x^{2^a5^{b-1}} - x^{2^{a-1}5^{b-1}} + 12 \\ &= \left(x^{2^a5^{b-1}} + 2x^{2^{a-1}5^{b-1}} + 3\right)\left(x^{2^a5^{b-1}} - 3x^{2^{a-1}5^{b-1}} + 4\right). \end{aligned}$$

□

Remark 3.2. The factorizations of $F(x)$ in Theorem 3.7 are perhaps related to Aurifeuillian factorizations [7], but no attempt has been made in this chapter to establish such a connection.

Conjecture 3.3. *Let d and m be positive integers with $d \geq 2$, and let $F(x) = \Phi_m(x) + d$. If $F(x)$ is reducible, then $F(x) \in \mathbb{F}_i$ for some $\mathbb{F}_i$ in Theorem 3.7.*

The proof of Conjecture 3.3 seems intractable. Nevertheless, we provide the following results in this direction that partially address polynomials of the form $\Phi_m(x)+d$, where the prime divisors of m are exactly the prime divisors of the indices in the families in Theorem 3.7.

Proposition 3.5. *Let a and d be positive integers. If $F(x) = \Phi_{2^a}(x)+d$ is reducible, then $F(x) \in \mathbb{F}_1$.*

Proof. Since $\Phi_{2^a}(x) = x^{2^{a-1}} + 1$, it follows from Theorem 3.2 and Theorem 3.3 that $F(x)$ is reducible if and only if either $-(d+1) = n^2$ or $-(d+1) = -4n^4$ for some $n \in \mathbb{Z}$. □

Proposition 3.6. *Let a, b and d be positive integers with $d \geq 2$. If $F(x) = \Phi_{2^a3^b}(x)+d$ is reducible, then $F(x) \in \mathbb{F}_2$.*

Proof. Let $f(x) = \Phi_3(x) + d$ and $g(x) = -x^{2^{a-1}3^{b-1}}$. Then $F(x) = f(g(x))$. Suppose that $f(\alpha) = 0$. Then, since $f(x)$ is irreducible and $F(x)$ is reducible, we have by

Theorem 3.2 that $g(x) - \alpha$ is reducible. Hence,

$$-(g(x) - \alpha) = x^{2^{a-1}3^{b-1}} - (-\alpha)$$

is also reducible. Therefore, by Theorem 3.3, we have for some $\beta \in \mathbb{Q}(\alpha)$ that one of the following conditions holds:

(i) $\alpha = -\beta^2$

(ii) $\alpha = -\beta^3$

(iii) $a \geq 3$ and $\alpha = 4\beta^4$.

For the sake of brevity of notation, we let $C = d + 1$. Note that $\alpha^2 = -\alpha - C$.

Assume first that (i) holds. Note that this possibility can only occur if $a \geq 2$. Since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$, we can write $\beta = r + s\alpha$ for some $r, s \in \mathbb{Q}$. Thus,

$$\alpha + (r + s\alpha)^2 = r^2 - s^2C - (s^2 - 2rs - 1)\alpha = 0.$$

Since $\{1, \alpha\}$ is a basis for the vector space $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$, we conclude that

$$r^2 - s^2C = 0 \qquad \text{and} \qquad s^2 - 2rs - 1 = 0. \tag{3.3.1}$$

Then from the first equation in (3.3.1), we have $r = \pm s\sqrt{C}$. Substituting this into the second equation in (3.3.1) and solving for s, we get

$$s = \pm\sqrt{\frac{1}{1 \pm 2\sqrt{C}}}.$$

However, C is a positive integer and $s \in \mathbb{Q}$. Consequently,

$$2\sqrt{C} + 1 = y^2, \tag{3.3.2}$$

for some odd integer $y \geq 3$. Write $y = 2n+1$, where $n \geq 1$, and recall that $C = d+1$. Thus, solving for d in (3.3.2) gives

$$d = 4n^2(n + 1)^2 - 1$$

and the proof is complete in this case.

Now assume that (ii) holds. We proceed as in the proof for case (i). Write $\beta = r + s\alpha$ for some $r, s \in \mathbb{Q}$. Then

$$\alpha + (r + s\alpha)^3 = r^3 + s^3C - 3rs^2C + (s^3 + 3r^2s - s^3C - 3rs^2 + 1)\alpha = 0,$$

from which we conclude that $r^3 + s^3C - 3rs^2C = 0$. Write $\dfrac{r}{s} = \dfrac{u}{v}$, where u, v are nonzero integers with $\gcd(u, v) = 1$. Thus,

$$C = \frac{r^3}{3rs^2 - s^3} = \frac{\left(\dfrac{r}{s}\right)^3}{3\left(\dfrac{r}{s}\right) - 1} = \frac{\left(\dfrac{u}{v}\right)^3}{3\left(\dfrac{u}{v}\right) - 1} = \frac{u^3}{3uv^2 - v^3} = \frac{u^3}{v^2\,(3u - v)}.$$

Then, since C is a positive integer and $\gcd(u, v) = 1$, we deduce that $v = 1$. But then, since $3u - 1 \neq \pm 1$ and $\gcd(u^3, 3u - 1) = 1$, we see that $C = \dfrac{u^3}{3u - 1}$ cannot be an integer. Hence, this case is impossible.

Finally, assume that (iii) holds. Let $\gamma = 2b^2$. Then $\alpha = 4\beta^4 = \gamma^2$, so that α is a square in $\mathbb{Q}(\alpha)$. Proceeding as in the proof for case (i), we write $\gamma = r + s\alpha$ for some $r, s \in \mathbb{Q}$. Then

$$-\alpha + (r + s\alpha)^2 = r^2 - s^2C - (s^2 - 2rs + 1)\alpha = 0,$$

from which we deduce that

$$r^2 - s^2C = 0 \qquad \text{and} \qquad s^2 - 2rs + 1 = 0. \tag{3.3.3}$$

We solve for r in the first equation in (3.3.3), substitute into the second equation in (3.3.3), and then solve for s to get

$$s = \pm\sqrt{\frac{-1}{1 \pm 2\sqrt{C}}}.$$

Since C is a positive integer and $s \in \mathbb{Q}$, it follows that

$$2\sqrt{C} - 1 = y^2, \tag{3.3.4}$$

for some odd integer $y \geq 3$. Write $y = 2n+1$, where $n \geq 1$, and recall that $C = d+1$. Thus, solving for d in (3.3.4) gives $d = (2n^2 + 2n + 1)^2 - 1$, and hence

$$\alpha^2 = -\alpha - (2n^2 + 2n + 1)^2. \tag{3.3.5}$$

Since $\beta \in \mathbb{Q}(\alpha)$, there exist $u, v \in \mathbb{Q}$ such that $\beta = u + v\alpha$. Expanding the equation $\alpha = 4\beta^4$ and using (3.3.5) to simplify, we get an equation of the form $E_1\alpha + E_2 = 0$, where E_1 and E_2 are rational expressions in u, v and n. By linear independence, we have that both E_1 and E_2 must be zero. Using MAPLE to solve this system of equations results in the possibilities that either

$$v = \frac{2y}{2n+1} \qquad \text{or} \qquad v = z, \tag{3.3.6}$$

where either

$$p_1(y) = (256n^2 + 256n + 192)y^4 + (32n + 16)y^2 - 1 = 0 \quad \text{or}$$

$$p_2(y) = (256n^2 + 256n + 192)y^4 - (32n + 16)y^2 - 1 = 0,$$

and

$$p_3(z) = (65536n^{12} + 393216n^{11} + 1212416n^{10} + 2457600n^9 + 3600384n^8 + 3981312n^7$$

$$+3387392n^6 + 2224128n^5 + 1113856n^4 + 413184n^3 + 107136n^2 + 17280n + 1296)z^8$$

$$+(1536n^6 + 4608n^5 + 7808n^4 + 7936n^3 + 5408n^2 + 2208n + 504)z^4 + 1 = 0.$$

However, none of the polynomials $p_i(x)$ has a rational zero. To see that this is so, we give details only for $p_1(x)$ since the proofs in the other two cases are similar. Using the quadratic formula, we get that the four zeros of $p_1(x)$ are

$$\pm\sqrt{\frac{\pm 2\sqrt{2n^2 + 2n + 1} - 2n - 1}{8\,(4n^2 + 4n + 3)}}.$$

Clearly, two of these zeros are nonreal, so consider the zero

$$y = \sqrt{\frac{2\sqrt{2n^2 + 2n + 1} - 2n - 1}{8\,(4n^2 + 4n + 3)}}.$$

Since $v \in \mathbb{Q}$, we must have $y \in \mathbb{Q}$ by (3.3.6), and so we can write $y = \frac{q}{w}$, where $q, w \in \mathbb{Z}$ with $\gcd(q, w) = 1$. Then

$$w^2 \left(2\sqrt{2n^2 + 2n + 1} - 2n - 1\right) = 8q^2 \left(4n^2 + 4n + 3\right).$$

Since $2\sqrt{2n^2 + 2n + 1} - 2n - 1$ must be an odd integer, it follows that $w^2 \equiv 0 \pmod{16}$. Hence $q \equiv 0 \pmod{2}$ since $4n^2 + 4n + 3 \equiv 1 \pmod{2}$, which contradicts the fact that $\gcd(q, w) = 1$. The same parity contradiction occurs when examining the other cases. Therefore, (iii) is impossible and the proof of the theorem is complete. □

Proposition 3.7. *Let a be a nonnegative integer. Let b and d be positive integers with $d \neq n^2 - 1$ and $d \neq n^5 - 1$ for any $n \in \mathbb{Z}$. If $F(x) = \Phi_{2^a 5^b}(x) + d$ is reducible, then $F(x) \in \mathbb{F}_3$.*

Proof. Since $d \neq n^2 - 1$ and $d \neq n^5 - 1$, we know by Proposition 3.2 that $f(x) = \Phi_5(x) + d$ is reducible. Since $\Phi_5(x)$ has no real zeros and $d \geq 1$, it follows that $f(x)$ as no real zeros. Hence,

$$f(x) = x^4 + x^3 + x^2 + x + d + 1 = (x^2 + rx + s)(x^2 + tx + u), \tag{3.3.7}$$

where $r, s, t, u \in \mathbb{Z}$. Equating coefficients gives, via MAPLE, the system of equations

$$\begin{aligned} r &= -t + 1, & s &= \frac{t(t^2 - 2t + 2)}{2t - 1}, \\ u &= \frac{t^3 - t^2 + t - 1}{2t - 1}, & d &= \frac{t^6 - 3t^5 + 5t^4 - 5t^3 + 2t - 1}{(2t - 1)^2}, \end{aligned} \tag{3.3.8}$$

where t is a free variable. Note that we may assume that $t \neq 0$ since $t = 0$ does not yield a valid solution in (3.3.7). Then $\frac{s}{t} = \frac{(t^2 - 2t + 2)}{2t - 1} \in \mathbb{Z}$ since $\gcd(t, 2t - 1) = 1$, and so

$$\frac{t - 3}{2t - 1} = u - s - \frac{s}{t} \in \mathbb{Z}.$$

Thus, $2t - 1$ divides $2t - 1 - 2(t - 3) = 5$. Since $|2t - 1| > 1$, we have that $|2t - 1| = 5$ and hence $t = -2$ or $t = 3$. In either case, $d = 11$ in (3.3.8) and the proof is complete. □

3.4 The Reducibility of $\prod_{i=1}^{k} \Phi_{m_i}(x) + 1$ where $k \geq 1$

Theorem 3.8. *Let a be a positive integer, and let*

$$S = \left\{ \Phi_{pq}(x) \,\middle|\, p \neq q \text{ primes}, \ p \equiv q \equiv -1 \pmod{2^{a+1}} \right\}.$$

Suppose that $k \geq 1$ and $k \not\equiv 0 \pmod{2^a}$. Let $[f_1(x), f_2(x), \ldots, f_k(x)]$ be a multi-subset of S. Then the polynomial

$$F(x) = \prod_{i=1}^{k} f_i(x) + 1$$

is reducible.

Proof. From the conditions on k, there exists a positive integer $b \leq a$ such that $k \equiv 2^{b-1} \pmod{2^b}$. Let $\zeta = \exp\left(2\pi i / 2^{b+1}\right)$. Then, since $b + 1 \leq a + 1$, it follows from Lemma 3.1 that $f_i(\zeta) = \zeta^2$ for each i. Therefore,

$$F(\zeta) = \prod_{i=1}^{k} f_i(\zeta) + 1 = \left(\zeta^2\right)^k + 1 = (-1) + 1 = 0.$$

Hence, $F(x)$ is reducible since $F(x)$ is divisible by $\Phi_{2^{b+1}}(x)$. □

The following corollary is immediate from Theorem 3.8.

Corollary 3.2. *Given any positive integer k, there exists a positive integer m such that $\Phi_m(x)^k + 1$ is reducible.*

In light of Theorem 3.8, one is led to ask the following question.

Question 3.1. *Does there exist an infinite set S of cyclotomic polynomials such that 1 plus the product of any number of elements from S is reducible?*

Using the polynomials $\Phi_{pq}(x)$ to construct such a set S seems to be doomed to failure because of the phenomenon described in Remark 3.1. Other infinite sets S exist that satisfy the conditions of Theorem 3.8, but they also seem to suffer from similar deficiencies. We suspect that Theorem 3.8 represents the best possible result in the direction of Question 3.1, although we cannot provide a proof of this belief.

Note that Question 3.1 can be answered affirmatively quite easily if the word "cylotomic" is removed. An example is

$$S = \left\{ (x+a)^3 \;\middle|\; a \in \mathbb{Z} \right\}.$$

In the next section, we prove a non-cyclotomic version of Theorem 3.8 in the sense that every element of S is irreducible and no element of S is cyclotomic.

3.5 A Non-cyclotomic Version of Theorem 3.8

Theorem 3.9. *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial with $\deg(f) \geq 1$ and for $m \geq 0$ let $g_m(x)$ be an irreducible factor of $f(x)^{2^m} + 1$. Let N be a positive integer and let*

$$S = \left\{ f(x) + q(x) \prod_{j=0}^{N} g_j(x) \;\middle|\; q(x) \in \mathbb{Z}[x] \right\} \setminus \{g_0(x) - 1\}.$$

Let T be a finite multi-subset of S such that $|T| \not\equiv 0 \pmod{2^{N+1}}$, then the polynomial

$$\prod_{h(x) \in T} h(x) + 1$$

is reducible.

Proof. Suppose that $|T| = k$. Since $k \geq 1$ and $k \not\equiv 0 \pmod{2^{N+1}}$, we deduce that $k \equiv 2^j \pmod{2^{j+1}}$ for some $0 \leq j \leq N$. Thus, for some $G(x) \in \mathbb{Z}[x]$ and $r \in \mathbb{Z}$,

$$\begin{aligned}
F(x) &= \prod_{h(x) \in T} h(x) + 1 \\
&= f(x)^k + G(x) \prod_{j=0}^{N} g_j(x) + 1 \\
&= f(x)^{r2^{j+1}+2^j} + G(x) \prod_{j=0}^{N} g_j(x) + 1 \\
&= \left(f(x)^{2^j} \right)^{2r} f(x)^{2^j} + G(x) \prod_{j=0}^{N} g_j(x) + 1 \\
&\equiv (-1)^{2r+1} + 1 \pmod{g_j(x)} \\
&\equiv 0 \pmod{g_j(x)}.
\end{aligned}$$

Notice that if $k \geq 2$, then $\deg(F) > \deg(g_j)$ and thus $F(x) \neq g_j(x)$. If $k = 1$, then $j = 0$ and $F(x) - 1 \in S$. From this we deduce that $F(x) \neq g_j(x)$ since $g_0(x) - 1 \notin S$. Hence, $F(x)$ must be reducible. □

Corollary 3.3. *Let N and k be positive integers with $k \not\equiv 0 \pmod{2^{N+1}}$. Then there exists an infinite set R of non-cyclotomic irreducible polynomials such that 1 plus the product of any (not necessarily distinct) k elements of R is reducible.*

Proof. We construct an infinite subset R of the set S in Theorem 3.9 so that no polynomial in R is cyclotomic and every polynomial in R is irreducible. Write

$$f(x) = \sum_{j=0}^{n} a_j x^j \qquad \text{and} \qquad G(x) = \prod_{j=0}^{N} g_j(x) = \sum_{j=0}^{m} b_j x^j.$$

Let p be a prime not dividing $a_j b_i$ when $a_j b_i \neq 0$ for $i \in \{0, \ldots, m\}$ and $j \in \{0, \ldots, n\}$. Since $b_0 \not\equiv 0 \pmod{p}$, b_0 has an inverse modulo p. Thus, we can choose c_0 so that $a_0 + c_0 b_0 \equiv 0 \pmod{p}$ while $a_0 + c_0 b_0 \not\equiv 0 \pmod{p^2}$. Similarly, we choose c_1 so that $a_1 + b_0 c_1 + b_1 c_0 \equiv 0 \pmod{p}$. Continuing in this way, we construct a polynomial

$$q(x) = \sum_{j=0}^{t} c_j x^j$$

so that the coefficients of $f(x) + q(x)G(x)$ satisfy Eisenstein's Criterion. Since each c_j need only satisfy a certain congruence modulo p, we can construct infinitely many such $q(x)$. Let

$$Q = \left\{ q(x) \,\middle|\, f(x) + q(x)G(x) \text{ satisfies Eisenstein's Criterion} \right\}.$$

Then the set

$$R = \left\{ f(x) + q(x) \prod_{j=0}^{N} g_j(x) \,\middle|\, q(x) \in Q \right\} \setminus \{g_0(x) - 1\}$$

is an infinite subset of S so that every polynomial in R is irreducible. Since no cyclotomic polynomial is Eisenstein, it follows that no element of R is cyclotomic, and hence the proof is complete. □

3.6 The Reducibility of $\Phi_m(x) + d$ with $d \in \mathbb{Z}$

Although the focus of this chapter has been on the situation when $d \in \mathbb{Z}^+$, the main result in this section (Corollary 3.4) addresses the more general situation of when $d \in \mathbb{Z}$, with $d \notin \{-1, 0, 1\}$. In particular, we give necessary conditions on d under the assumption that $F(x)$ has a cyclotomic factor.

Theorem 3.10. *Let n and m be distinct, positive integers and let $\zeta_m = \exp(2\pi i/m)$. If $\Phi_n(\zeta_m) \in \mathbb{Q}$, then either $\Phi_n(\zeta_m) = \pm 1$ or $\Phi_n(\zeta_m) = \pm p$ for some prime p, and $n = mp^k$ for some positive integer k.*

Proof. Let n and m be positive integers and let $\zeta_m = \exp(2\pi i/m)$. Suppose that $\Phi_n(\zeta_m) = r \in \mathbb{Q}$. Since $\Phi_m(x)$ is irreducible, we deduce that

$$\Phi_n(x) - r = \Phi_m(x)g(x) \tag{3.6.1}$$

for some $g(x) \in \mathbb{Z}[x]$. We proceed by considering $R(\Phi_m(x), \Phi_n(x))$. Write $\Phi_m(x) = \prod_{j=1}^{\phi(m)}(x - \alpha_j)$. Then, from (3.2.1), we have that

$$R(\Phi_m(x), \Phi_n(x)) = \prod_{j=1}^{\phi(m)} \Phi_n(\alpha_j) = \prod_{j=1}^{\phi(m)} (\Phi_m(\alpha_j)g(\alpha_j) + r) = r^{\phi(m)}. \tag{3.6.2}$$

Suppose that $n \neq mp^k$ for any prime p and nonzero integer k. Then it follows from Theorem 3.1 and (3.6.2) that

$$\pm 1 = R(\Phi_m(x), \Phi_n(x)) = r^{\phi(m)}.$$

Thus, $\Phi_n(\zeta_m) = r = \pm 1$.

Now suppose that $n = mp^k$ for some integer $k \neq 0$. If $k < 0$, then $n < m$ and

$$\phi(m) = \phi(np^{-k}) \geq \phi(n),$$

which contradicts (3.6.1). Hence, $k > 0$ and $n > m$. With this, the result follows from Theorem 3.1 and (3.6.2) since

$$p^{\phi(m)} = R(\Phi_n(x), \Phi_m(x)) = r^{\phi(m)}$$

implies that $\Phi_n(\zeta_m) = r = \pm p$. $\square$

The following corollary is immediate from Theorem 3.10

Corollary 3.4. *Let n and d be integers with $n \geq 2$ and $d \notin \{-1, 0, 1\}$. If $\Phi_n(x) + d$ has a cyclotomic factor, say $\Phi_m(x)$, then $|d| = p$ for some prime divisor p of n. Furthermore, $n = mp^k$ for some positive integer k.*

Based on Corollary 3.4 and computer evidence, we end this section with the following conjecture.

Conjecture 3.4. *Let n and d be integers with $n \geq 2$ and $d \notin \{-1, 0, 1\}$. Let $F(x) = \Phi_n(x) + d$. Then $F(x)$ has a cyclotomic factor $\Phi_m(x)$ if and only $F(x)$ is reducible with $d = -p$ for some prime divisor p of n. Moreover, in this case, we have that $\Phi_{n/p}(x)$ divides $F(x)$.*

Bibliography

[1] A. Beiler, *The Eternal Triangle*, Recreations in the Theory of Numbers: The Queen of Mathematics Entertains, New York: Dover, 1966.

[2] J. Cooper and C. Poirel, Note on the pythagorean triple system. (2008), URL `http://www.math.sc.edu/~cooper/pth.pdf`

[3] D.N. Lehmer, Asymptotic evaluation of certain totient sums, Amer. J. Math. 22 (1900), 293–335.

[4] M. Filaseta, Coverings of the integers associated with an irreducibility theorem of A. Schinzel. *Number theory for the millennium, II (Urbana, IL, 2000)*, 1–24, A K Peters, Natick, MA, 2002.

[5] M. Filaseta, K. Ford, and S. Konyagin, On an irreducibility theorem of A. Schinzel associated with coverings of the integers. *Illinois J. Math.* 44 (2000), no. 3, 633–643.

[6] W. Flügel, Solution to problem 226, *Archiv. der Math. und Physik* 15 (1909), 271.

[7] A. Granville and P. Pleasants, Aurifeuillian factorization. *Math. Comp.* 75 (2006), no. 253, 497–508.

[8] K. Győry, L. Hajdu and R. Tijdeman, Irreducibility criteria of Schur-type and Pólya-type. *Monatsh. Math.* 163 (2011), no. 4, 415–443.

[9] W. Kay, An Overview of the Constructive Local Lemma. *Master's Thesis - University of South Carolina* (2012)

[10] R. P. Kurshan and A. M. Odlyzko, Values of cyclotomic polynomials at roots of unity. *Math. Scand.* 49 (1981), no. 1, 15–35.

[11] E. Lehmer, A numerical function applied to cyclotomy. *Bull. Amer. Math. Soc.* 36 (1930), no. 4, 291–298.

[12] M. Mossinghoff, C. Pinner and J. Vaaler, Perturbing polynomials with all their roots on the unit circle. *Math. Comp.* 67 (1998), no. 224, 1707–1726.

[13] K. Motose, On values of cyclotomic polynomials. VII. *Bull. Fac. Sci. Technol. Hirosaki Univ.* 7 (2004), no. 1, 1–8.

[14] K. Motose, On values of cyclotomic polynomials. VIII. *Bull. Fac. Sci. Technol. Hirosaki Univ.* 9 (2006), no. 1, 15–27.

[15] A. Schinzel, *Polynomials with Special Regard to Reducibility*, Encyclopedia of Mathematics and Its Applications, Cambridge University Press, 2000.

[16] I. Schur, Problem 226, *Archiv Math. Physik* (3) 13 (1908), 367.

[17] I. Seres, Lösung und Verallgemeinerung eines Schurschen Irreduzibilitätsproblems für Polynome. (German) *Acta Math. Acad. Sci. Hungar.* 7 (1956), 151–157.

[18] W. Sierpiński, Sur la sommation de la série $\sum_{a<n\leq b} \tau(n)F(n)$, où $\tau(n)$ signifie le nombre de décompositions du nombre n en une somme de deuz carrés de nombres entiers, Prace Mat. Fiz. 18 (1908) 1–59 (in Polish); Oeuvres Choises, Vol. 1 (Varsovie, 1974) 109–154 (in French).

[19] J. Westlund, On the irreducibility of certain polynomials. *Amer. Math. Monthly* 16 (1909), 66–67.

[20] S. Wigert. Sur l'ordre de grandeur du nombre des diviseurs d'un entier. *Arkiv Mat. Astr. Fys.* 3 (1907), paper 18, 1–9.