COLORING PROBLEMS

by

Thomas Antonio Charles Chartier

A thesis

submitted in partial fulfillment

of the requirements for the degree of

Master of Science in Mathematics

Boise State University

December 2011

BOISE STATE UNIVERSITY GRADUATE COLLEGE

DEFENSE COMMITTEE AND FINAL READING APPROVALS

of the thesis submitted by

Thomas Antonio Charles Chartier

Thesis Title: Coloring Problems

Date of Final Oral Examination: 13 October 2011

The following individuals read and discussed the thesis submitted by student Thomas Antonio Charles Chartier, and they evaluated his presentation and response to questions during the final oral examination. They found that the student passed the final oral examination.

Andrés E. Caicedo, Ph.D.	Chair
Jens Harlander, Ph.D.	Member, Supervisory Committee
Marion Scheepers, Ph.D.	Member, Supervisory Committee

The final reading approval of the thesis was granted by Andrés E. Caicedo, Ph.D., Chair. The thesis was approved for the Graduate College by John R. Pelton, Ph.D., Dean of the Graduate College.

Dedicated to Bethany, Parker, and Daxton

ACKNOWLEDGMENTS

I would like to thank Dr. Andrés Caicedo for his patience and support through the entire thesis process. I would also like to express my gratitude to the following: The Boise State University Mathematics department for providing me with a teaching assistantship, Dr. Jens Harlander and Dr. Marion Scheepers for serving as committee members, Dr. Zach Teitler for informing us of several relevant references and Dr. Rodney Forcade for sharing with us his relevant works and data. Lastly, I would like to say thank you to Bethany, I certainly could not have done this without you.

ABSTRACT

This thesis considers several coloring problems all of which have a combinatorial flavor. We review some results on the chromatic number of the plane, and improve a bound on the value of regressive Ramsey numbers. The main work of this thesis considers the problem of whether given any $n \geq 1$, one can color $\mathbb{Z}^+$ in such a way that for all $a \in \mathbb{Z}^+$ the numbers $a, 2a, 3a, ..., na$ are assigned different colors. Such colorings are referred to as *satisfactory*. We provide a sufficient condition for guaranteeing the existence of satisfactory colorings and analyze the resulting structure. Explicit constructions are given for $n \leq 54$. The thesis concludes with some suggestions towards a general argument.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS

$\mathbb{N}$	$\{0, 1, 2, 3, ...\}$
$\mathbb{Z}^+$	$\{1, 2, 3, ...\}$
$\mathbb{Q}$	The set of rational numbers.
$\mathbb{R}$	The set of real numbers.
$\mathbb{Z}_n$	The integers modulo n.
$\mathbb{Z}_n^*$	The group of units modulo n.
(a, b)	The greatest common divisor of a and b.
$\text{ind}_g(a)$	The index of a with respect to the primitive root g.
$\pi(n)$	The number of primes less than or equal to n.
$K = K_n$	The n-th core.
C_{K_n}	The set of satisfactory colorings of K_n.
M_{K_n}	The set of multiplicative colorings of K_n.
$g^{\oplus\alpha}$	$\underbrace{g \oplus \cdots \oplus g}_{\alpha \text{ times}}$, where g is an element of an abelian group.
$\mathbf{n}$	$\{1, 2, \ldots, n\}$

CHAPTER 1

INTRODUCTION

1.1 History of Coloring

Graph Coloring is the assignment of labels or "colors" to the edges or vertices of a graph [6]. Problems in this area (more specifically those seeking to ascertain the properties of a given coloring, or to determine whether colorings with specific properties exist) have given impetus to whole fields in combinatorics (Ramsey theory, see [10]) and set theory (partition calculus); the results often have application in number theory and analysis, among others.

Consider the following question, originally posed by Francis Guthrie in 1852, see [4].

> Is it possible to color any planar map using four colors in such a way that regions sharing a common boundary, excluding boundaries which are comprised of a single point, do not share the same color?

The affirmative answer and its proof were finally attained by Kenneth Appel and Wolfgang Haken some 124 years later with the aid of computers.[1] It was during this time that the still very active area of mathematics known as Graph Coloring came to be.

[1] Here it is noteworthy to mention that this was the first significant mathematical result in which a computer was used in an essential manner. For a more detailed discussion of the result and its subsequent impact on mathematical practice refer to Chapter 21 of [4].

This thesis is organized as follows.

The rest of this chapter is devoted to providing some of the necessary background for our results.

In Chapter 2, we give a brief description of a well–known problem in graph coloring theory, the chromatic number of the plane, and some of the results that have been obtained.

In Chapter 3, we extend a recent result of Andrés Caicedo in [9] concerning regressive functions on pairs.

The remainder of the thesis deals with the main point of this thesis. The question at hand is introduced in Chapter 4, and in full generality remains unsolved. It asks for the existence of certain colorings of positive integers, generalizing a question from KöMaL [3]. We call such colorings *satisfactory.* The key notion of the *n-core* is introduced in Section 4.2 and discussed in detail in Section 4.3.

In Section 5.1, we give a sufficient condition, using elementary number theory, which guarantees a satisfactory coloring exists using n colors, provided certain primes of the form $nk+1$ exist. In Subsection 5.1.1, we give a solution to the question posed in KöMaL. In Section 5.2, we identify all satisfactory colorings with at most 5 colors. Multiplicative colorings are introduced in Section 5.4, and the associated notion of partial G-homomorphism, for G an abelian group, is defined in Section 5.5.

In Chapter 6, we identify all multiplicative colorings with at most 8 colors.

In Chapter 7, we discuss a related problem that provides insight to the inherent difficulty of our problem.

Also, four days after the defense of this thesis, the work of Rodney Forcade, Jack Lamoreaux, and Andrew Pollington in [18] and Forcade and Pollington in [19] was brought to our attention. As such, several of the problems we mention as open have in fact been solved. Rather than rewriting significant portions of the entire thesis, we devote Section 7.2 to discussing how the results in [19] and [18] pertain to our current work and the effect they have on future considerations.

This thesis relied heavily on the use of scientific computing software. More specifically, we used `C++`, Maple, Matlab, and Sage in the acquisition of data and to some extent obtain various results throughout the thesis. As such, the main code that has been used has been included in Appendix A.

1.2 Necessary Background

We begin by providing some number theoretic results that have been fundamental in constructing satisfactory colorings. All of them can be found in [1]. We also establish some basic results on the cardinality of sets.

1.2.1 Linear Congruences

Theorem 1.1. *Let m, a, b be integers with $m \geq 1$. Let $d = (a, m)$ be the gcd of a and m. The congruence*

$$ax \equiv b \pmod{m} \tag{1.1}$$

has solutions if and only if

$$b \equiv 0 \pmod{d}.$$

Proof. Let $d = (a, m)$. Congruence (1.1) has a solution if and only if there exist $x, y \in \mathbb{Z}$ such that

$$ax - my = b.$$

Since $d|a$ and $d|m$ and d is an integer linear combination of a and m by Theorem 1.15 of [1], then $ax - my = b$ has a solution if and only if $d|b$, i.e., $b \equiv 0 \pmod{d}$. □

Theorem 1.2. *Let m, a, b, d be as in Theorem* 1.1. *If $b \equiv 0 \pmod{d}$, then the congruence* (1.1) *has exactly d solutions that are pairwise incongruent modulo m. In particular, if $(a, m) = 1$, then for every b the congruence* (1.1) *has a unique solution* modulo *m.*

Proof. Suppose x and y are solutions to Congruence (1.1), then

$$a(x - y) \equiv ax - ay \equiv b - b \equiv 0 \pmod{m},$$

thus $a(x - y)$ is a multiple of m and so for some integer z

$$a(x - y) = mz.$$

If $(a, m) = d$, then $(a/d, m/d) = 1$ and

$$\frac{a}{d}(x - y) = \frac{m}{d}z.$$

This means that m/d divides $x - y$ and we have that

$$y \equiv x \pmod{\frac{m}{d}}.$$

Moreover, every integer y of this form is a solution to Congruence (1.1). An integer congruent to x modulo m/d is congruent to $x + im/d$ modulo m for some integer $i = 0, 1, 2, ..., d - 1$, and the d integers $x + im/d$ with $i = 1, 2, 3, ..., d - 1$ are pairwise incongruent modulo m. Thus, (1.1) has exactly d pairwise incongruent solutions. □

1.2.2 Power Residues

Let $m, k, a \in \mathbb{Z}$ be such that $m \geq 2$, $k \geq 2$, and $(a, m) = 1$. Refer to a as a *kth power residue modulo* m if, and only if, there is an $x \in \mathbb{Z}$ such that

$$x^k \equiv a \pmod{m}.$$

The order of a *modulo* m is the smallest integer d such that $a^d \equiv 1 \pmod{m}$.

Definition 1.3. *Recall that the Euler totient function $\phi(n)$ counts the number of positive integers less than or equal to n that are relatively prime to n. The number a is a* primitive root modulo m *if a has order $\phi(m)$.*

The following theorem guarantees the existence of primitive roots for all prime moduli. The proof can be found in [1], pp. 87–88.

Theorem 1.4. *For every prime p, there exist $\phi(p-1)$ pairwise incongruent primitive roots* modulo p.

Corollary 1.5. *The group $\mathbb{Z}_p^*$ is cyclic and therefore isomorphic to $\mathbb{Z}_{p-1}$.*

Let p be a prime and g be a primitive root modulo p. If a is an integer and p does not divide a, then there exists a unique integer $k \in \{0, 1, \ldots, p-2\}$ such that

$$a \equiv g^k \pmod{p}.$$

The integer k is called the *index* of a with respect to the primitive root g and is denoted by $k = \text{ind}_g(a)$.

Theorem 1.6. *Let p be prime, $k \geq 2$, and $d = (k, p-1)$. Let $a \in \mathbb{Z}$ be such that $p \nmid a$. Let g be a primitive root modulo p. Then, a is a kth power residue modulo p, if and only if*

$$\operatorname{ind}_g(a) \equiv 0 \pmod{d}$$

if and only if

$$a^{\frac{p-1}{d}} \equiv 1 \pmod{p}.$$

If a is a kth power residue modulo p, then the congruence

$$x^k \equiv a \pmod{p} \tag{1.2}$$

has exactly d solutions that are pairwise incongruent modulo p, and there are precisely $(p-1)/d$ pairwise incongruent kth power residues modulo p.

Proof. Let $l = \operatorname{ind}_g(a)$, where g is a primitive root modulo p. Congruence (1.2) is solvable if and only if there exists an integer y such that

$$g^y \equiv x \pmod{p}$$

and

$$g^{ky} \equiv x^k \equiv a \equiv g^l \pmod{p}.$$

This is equivalent to

$$ky \equiv l \pmod{p-1}. \tag{1.3}$$

Congruence (1.3) has a solution if and only if

$$\operatorname{ind}_g(a) = l \equiv 0 \pmod{d},$$

where $d = (k, p-1)$. Thus, the kth power residues modulo p are the integers in the $(p-1)/d$ congruence classes $g^{id} + p\mathbb{Z}$ for $i = 0, 1, ..., (p-1)/d$. Moreover,

$$a^{(p-1)/d} \equiv g^{(p-1)l/d} \equiv 1 \pmod{p}$$

if and only if

$$\frac{(p-1)l}{d} \equiv 0 \pmod{p-1}$$

if and only if

$$\operatorname{ind}_g(a) = l \equiv 0 \pmod{d}.$$

If Congruence (1.3) is solvable then by Theorem 1.2, it has exactly d solutions y that are pairwise incongruent modulo $p-1$, and so Congruence (1.2) has exactly d solutions $x = g^y$ that are pairwise incongruent modulo p. □

Corollary 1.7. *If $p = nk+1$ is prime, then $\{a^k \pmod{p} : (a, p) = 1\}$ is a group under multiplication modulo p, and is isomorphic to $\mathbb{Z}_n$.*

1.2.3 Principal Number Theoretic Results

We state the well–known theorem of Dirichlet concerning primes in arithmetic progressions. For proof, the reader is directed to [1], pp. 347–349.

Theorem 1.8. (Dirichlet)
Let $a, m \in \mathbb{Z}^+$ be relatively prime. Then, there exist infinitely many primes p such that

$$p \equiv a \pmod{m}.$$

Recall that if p is prime and $n \in \mathbb{Z}$, the *Legendre symbol* $\left(\dfrac{n}{p}\right)$ is defined by

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & \text{if } p|n, \\ 1 & \text{if } n \text{ is a quadratic residue modulo } p, \\ -1 & \text{otherwise.} \end{cases}$$

By Theorem 1.6, $\left(\dfrac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \pmod{p}$. The *Quadratic Reciprocity Law* of Gauß is the following statement, see Theorems 3.13, 3.16, and 3.17 in [1].

Theorem 1.9. (Gauß)

Let p be an odd prime.

1. *The Legendre symbol $\left(\dfrac{\cdot}{p}\right)$ is completely multiplicative, that is*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

for all integers a and b.

2. $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

3. *If $q \neq p$ is also an odd prime, then*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

The following corollary will be particularly useful.

Theorem 1.10. *Let p be an odd prime. Then $2^{(p-1)/2} \equiv 1 \pmod{p}$ if and only if $p \equiv \pm 1 \pmod{8}$.*

Notation 1.11. For $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$, $a \pmod{m}$ denotes the equivalence class of a modulo m, so the statements

$$a \equiv b \pmod{m} \text{ and}$$
$$a \pmod{m} = b \pmod{m}$$

are equivalent. We identify $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ and $\{0, 1, \ldots, n-1\}$ without comment.

1.2.4 Cardinality

Definition 1.12. *Given sets A and B:*

1. $|A| \leq |B|$ *if and only if there is a* $1-1$ *function* $f : A \to B$.

2. $|A| = |B|$ *if and only if there is a bijective function* $f : A \to B$.

3. $|A| < |B|$ *if and only if* $|A| \leq |B|$ *and* $|A| \neq |B|$.

If $|A| = |B|$, we say that A and B are *equipotent* or have the same *cardinality*.

Theorem 1.13. The Schröder-Bernstein theorem.
If $|A| \leq |B|$ *and* $|B| \leq |A|$ *then,*

$$|A| = |B|.$$

The following argument is due to Knaster and Tarski, see [22] and [23].

Proof. Let $f : A \to B$ and $g : B \to A$ be injections. In order to prove the theorem, we need to produce a bijection

$$h : A \to B.$$

The simplest way to accomplish this is by finding a set $C \subseteq A$ such that the function h defined as follows is indeed a bijection:

$$h(x) = \begin{cases} f(x), & \text{if } x \in C \\ g^{-1}(x), & \text{if } x \notin C. \end{cases}$$

If we can find such a C, we are done. If such a C exists, then, since h is a bijection, we must have that $f(C) \cap g^{-1}(A \smallsetminus C) = \varnothing$ and $g^{-1}(A \smallsetminus C) \cup f(C) = B$. Thus, we need that $C = A \smallsetminus g(B \smallsetminus f(C))$. Note that, indeed, for any C satisfying this equation, the function h as defined above is a bijection, as wanted. To show there is such a C, define a function $\pi : \mathcal{P}(A) \to \mathcal{P}(A)$ by

$$\pi(X) = A \smallsetminus g(B \smallsetminus f(X)).$$

Now note that for any $X \subseteq Y$, we have that $\pi(X) \subseteq \pi(Y)$ since if $X \subseteq Y \subseteq A$, then $f(X) \subseteq f(Y)$ so $B \smallsetminus f(X) \supseteq B \smallsetminus f(Y)$ so $g(B \smallsetminus f(X)) \supseteq g(B \smallsetminus f(Y))$ and, finally, $A \smallsetminus g(B \smallsetminus f(X)) \subseteq A \smallsetminus g(B \smallsetminus f(Y))$, thus π is *monotone*. Now, if we show that any monotone $\pi : \mathcal{P}(A) \to \mathcal{P}(A)$ has a fixed point then we are done. For such a map π, consider the collection of subsets

$$S = \{X \subseteq A : X \subseteq \pi(X)\}.$$

Note that S is nonempty since it contains the empty set. Also, if $X \in S$, then $\pi(X) \in S$ by monotonicity. Let $Y = \bigcup S$. Then, $Y \in S$ as $X \subseteq \pi(X) \subseteq \pi(Y)$ for any $X \in S$, again by monotonicity, so also $Y = \bigcup\{X : X \in S\} \subseteq \pi(Y)$. Now, since $Y \in S$,

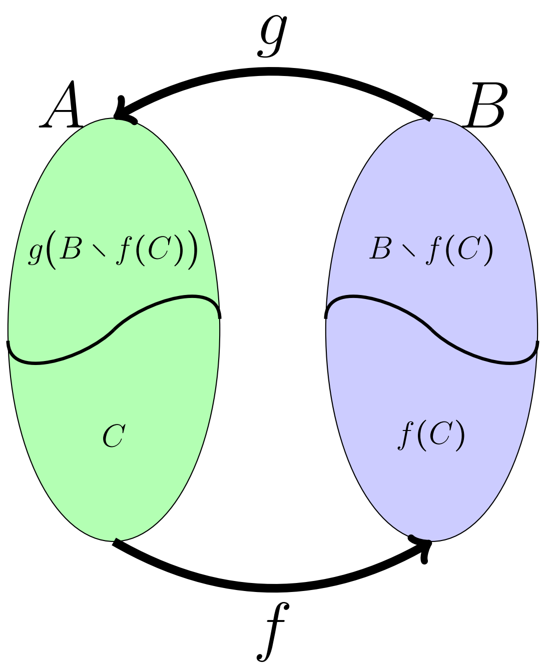

Figure 1.1: The desired mapping

then also $\pi(Y) \in S$, thus $\pi(Y) \subseteq \bigcup S = Y$. This means that $Y = \pi(Y)$, thus Y is a fixed point. □

Note that up to this point, we have not invoked the axiom of choice. Had we done so, the proof of Theorem 1.13 would have been far less involved.

Definition 1.14. *Let A be a set. If there is a function $f : A \to \mathbb{N}$ that is injective, we say that A is countable. If there is such an f that is bijective, we say A is countably infinite.*

Proposition 1.15. *Any subset of a countable set is countable.*

Proof. Let A be a countable set, as witnessed by f. Consider $B \subseteq A$. Clearly $f \restriction_B$ is also injective. Thus, B is countable. □

Lemma 1.16. *A set A is countable and nonempty if and only if there exists a surjection $f' : \mathbb{N} \to A$.*

Proof. Suppose A is countable and nonempty, so there exists some $f : A \to \mathbb{N}$ injective. Letting $B = f(A)$, we have that $f : A \to B$ is a bijection. Fix $a \in A$ and define $f' : \mathbb{N} \to A$ by

$$f'(n) = \begin{cases} f^{-1}(n) & \text{if } n \in B \\ a & \text{if } n \notin B \end{cases}$$

Then, f' is surjective. Conversely, if $f' : \mathbb{N} \to A$ is surjective, then A is nonempty. Define $f : A \to \mathbb{N}$ as follows: Given $a \in A$, let $f(a)$ be the least $n \in \mathbb{N}$ such that $f'(n) = a$, which exists since f' is surjective. Then, f is injective and, by definition, A is countable. □

Proposition 1.17. *$A \cup B$ is countable if and only if A and B are countable.*

Proof. If $A \cup B$ is countable, by Proposition 1.15, A and B are countable since they are subsets of a countable set. Now suppose A and B are countable. If $A = \varnothing$, then $A \cup B = B$, and similarly if $B = \varnothing$, so we may assume that A and B are nonempty. By Lemma 1.16, there exist surjections $f' : \mathbb{N} \to A$ and $g' : \mathbb{N} \to B$. Let $C = A \cup B$. Define $h : \mathbb{N} \to C$ by

$$h(2x + 1) = f'(x)$$

and

$$h(2x) = g'(x),$$

for $x \in \mathbb{N}$. Clearly, h is surjective. By Lemma 1.16, it follows that C is countable. □

Corollary 1.18. *A finite union of countable sets is countable.*

Proof. Immediate from Proposition 1.17 and induction. □

Lemma 1.19. *The* Cartesian Product $\mathbb{N} \times \mathbb{N}$ *is countable.*

Proof. Define

$$f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

by

$$f(m, n) = 2^m 3^n.$$

By unique factorization, it is clear that f is injective and therefore $\mathbb{N} \times \mathbb{N}$ is countable. □

Remark 1.20. Since $\mathbb{N}$ injects into $\mathbb{N} \times \mathbb{N}$, it follows that $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N}$ are equipotent, by Theorem 1.13. Actually, it is possible to exhibit a bijection between the two sets without using Theorem 1.13. For example, we can take

$$f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

to be

$$f(n, m) = 2^n(2m + 1) - 1,$$

or

$$\binom{n + m + 1}{2} + m.$$

Proposition 1.21. *A countably infinite union of countable sets is countable.*

Proof. Let A_i be countable for all $i \in \mathbb{N}$. We may assume all A_i are nonempty. Let $f_i : \mathbb{N} \to A_i$ be surjective for all $i \in \mathbb{N}$. Now define

$$g : \mathbb{N} \times \mathbb{N} \to \bigcup_{i=0}^{\infty} A_i$$

by

$$g(i,m) = f_i(m), \text{ for all } i, m \in \mathbb{N}.$$

Now to see that g is surjective consider $a \in \bigcup_{i=0}^{\infty} A_i$. Then, $a \in A_j$ for some j. Since f_j is surjective, there is an $m \in \mathbb{N}$ such that $f_j(m) = a$, so $g(j,m) = a$ and thus g is surjective. Let $g' : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ be the inverse of an f as in Remark 1.20. Then, $g \circ g' : \mathbb{N} \to \bigcup_{i=0}^{\infty} A_i$ is surjective and the result follows. □

Remark 1.22. The argument above uses the axiom of choice, by simultaneously picking a surjection $f_i : \mathbb{N} \to A_i$ for each i. In many specific applications of Proposition 1.21, we can exhibit these surjections explicitly, and therefore avoid the need to use the axiom of choice.

For A and B sets, let A^B denote the set of functions from A to B and let $|A|^{|B|}$ be its cardinality.

Corollary 1.23. *$\mathbb{Q}$ is countable.*

Proof. $\mathbb{Q} = \bigcup_{n=1}^{\infty} \{m/n \mid m \in \mathbb{Z}\}$. □

On the other hand, it is a well–known result of Cantor that $\mathbb{R}$ is uncountable. We omit the argument.

Lemma 1.24. $2^{|\mathbb{N}|} = |\mathbb{R}|$.

Proof. It is well–known that the standard Cantor middle set $\mathcal{C} \subseteq \mathbb{R}$ consists of all reals of the form

$$x = \sum_{n=1}^{\infty} \frac{2a_n}{3^n}$$

where each a_n is 0 or 1. This gives us an obvious bijection between $\mathcal{C}$ and the set $\{0,1\}^{\mathbb{N}}$. Hence,

$$2^{|\mathbb{N}|} = \left|\{0,1\}^{\mathbb{N}}\right| = |\mathcal{C}| \leq |\mathbb{R}|.$$

Conversely, any real x is uniquely determined by $A_x = \{q \in \mathbb{Q} \mid q < x\}$, hence $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{Q})|$. But there is an obvious bijection (via *characteristic functions*) between $\mathcal{P}(\mathbb{Q})$ and $\{0,1\}^{\mathbb{Q}}$. Since $\mathbb{Q}$ is countable, this set is in bijection with $\{0,1\}^{\mathbb{N}}$, and we have

$$|\mathbb{R}| \leq 2^{|\mathbb{N}|}.$$

The result follows from the Schröder-Bernstein theorem. □

Corollary 1.25. *For any $n \in \mathbb{Z}^+$, if $n > 1$, then $n^{|\mathbb{N}|} = |\mathbb{R}|$.*

Proof. It suffices to prove that $n^{|\mathbb{N}|} \leq 2^{|\mathbb{N}|}$, by Lemma 1.24 and the Schröder-Bernstein theorem. But note that $n \leq 2^{|\mathbb{N}|}$, so $n^{|\mathbb{N}|} \leq (2^{|\mathbb{N}|})^{|\mathbb{N}|}$. We claim that for any (nonempty) sets A, B, C, we have

$$(|A|^{|B|})^{|C|} = |A|^{|B \times C|}.$$

From this, it follows that $(2^{|\mathbb{N}|})^{|\mathbb{N}|} = 2^{|\mathbb{N}|}$, and we are done.

To prove the claim, we exhibit a bijection π between $(A^B)^C$ and $A^{B \times C}$. Given $f : C \to A^B$, define $\pi(f) : B \times C \to A$ by $\pi(f)(b,c) = (f(c))(b)$ for any $b \in B$ and $c \in C$. It is straightforward to check that π is indeed a bijection. □

CHAPTER 2

THE CHROMATIC NUMBER OF THE PLANE

While the Four Color Theorem is by far the most celebrated result in Graph Coloring, another result, if attained, would be heralded as equally important. The result in question is the determination of the chromatic number of the plane, as yet unknown.

Definition 2.1. *The chromatic number of the plane, denoted by χ, is the smallest number of colors sufficient for coloring the plane in such a way that no two points of the same color are unit distance apart.*

Question 2.2. *What is the value of χ?*

Perhaps, it is the fact that this problem can be formulated in such an easy to understand fashion that makes it so intriguing. However, the simplicity of this question is merely the facade of an historically difficult problem. In fact, the best known results say that χ is either 4, 5, 6, or 7. If a coloring of the plane is such that no two points at distance 1 have the same color, we say it is a χ coloring. If a graph cannot be colored such that no two points at distance 1 have the same color, we say the graph cannot be χ colored.

Lemma 2.3. *The Chromatic number of the plane is at least 3.*

The following proof corresponds to Figure 2.1.

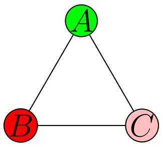

Figure 2.1: A χ coloring of an equilateral triangle of side length 1.

Proof. Consider a χ coloring of the plane, and an equilateral triangle of side length 1. Call the vertices of this triangle A, B, and C. Since A and B are a unit apart, they must be colored differently. Since C is a unit apart from A and B, it cannot be the same color as A or B. Thus, we need at least 3 colors. □

Proposition 2.4. $\chi \geq 4$.

The following proof corresponds to Figure 2.2.

Proof. We proceed by contradiction. Consider a χ coloring of the plane using 3 colors, and consider an equilateral triangle of side length 1. Call its vertices A, B, and C. Let A' be the reflection of A across the segment BC. Note that this gives us that $d(A', B) = d(A', C) = d(B, C) = 1$ and $d(A, A') = \sqrt{3}$. Thus, since A, B, and C all receive different colors, it must be the case that A and A' have the same color. In fact, this means that every point on the circumference of the circle of radius $\sqrt{3}$ centered at A must have the same color as A. However, for any circle with a radius at least $\frac{1}{2}$, we can find 2 points on its circumference that are a unit distance apart (in fact there are infinitely many such points), which gives us the contradiction. □

Proposition 2.5. $\chi \leq 7$.

The following proof corresponds to Figure 2.3.

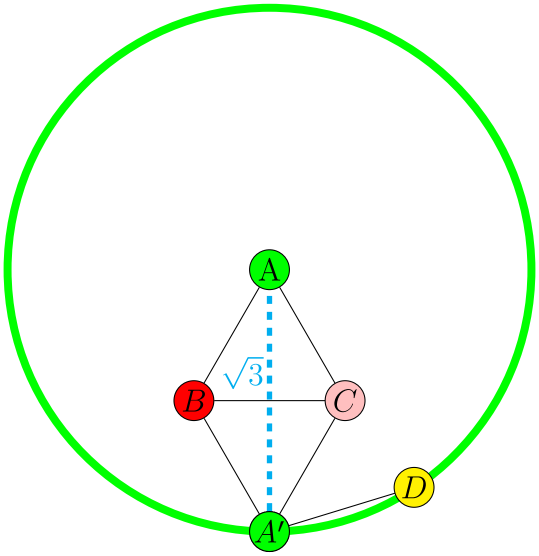

Figure 2.2: A graph that cannot be χ colored with 3 colors.

Proof. Begin with a tessellation of the plane by hexagons of side length one. Pick some hexagon, and color it with one of the colors. Color each hexagon adjacent to the chosen hexagon with the remaining colors. Denote by $\mathcal{P}$ the polygon comprised of the 7 aforementioned hexagons. Now, tile the plane by translations of $\mathcal{P}$. If this coloring is to work, then we must ensure that the maximum distance between any two points of one of the given hexagons must be less than a unit. Additionally, we must ensure that the distance between any two points of hexagons, which are colored the same, must be greater than a unit. This is accomplished by shrinking the polygon $\mathcal{P}$ by a factor x where $2 < x < \sqrt{7}$. That is, if we make the hexagons to have a side length slightly less than $\frac{1}{2}$, what results is a χ coloring of the plane. (There is a slight ambiguity in this description as each edge of a hexagon receives two possible colors, but our choice of x ensures that either choice we follow to eliminate the ambiguity will work.) This completes the proof. □

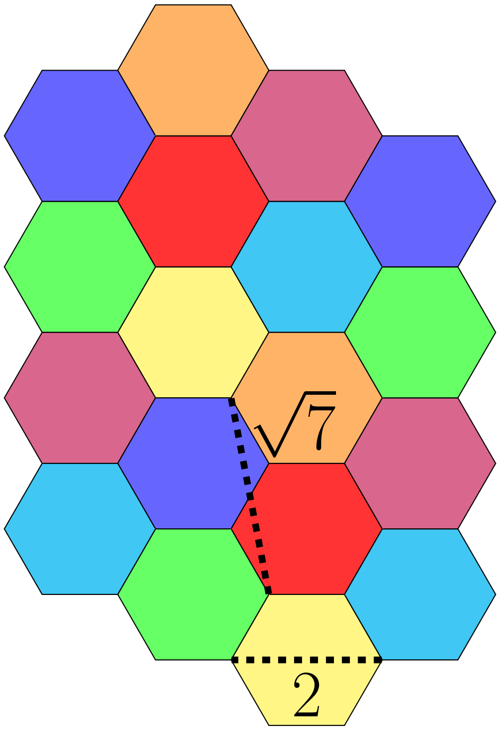

Figure 2.3: An Hexagonal Tessellation of $\mathbb{R}^2$, which cannot be χ colored.

Note that the argument of Proposition 2.4 can be easily rephrased so only 7 points need to be considered, see Figure 2.4. In some sense, this is optimal:

Proposition 2.6. *Any set of at most 6 points in $\mathbb{R}^2$ can be χ colored with at most 3 colors.*

Proof. First note that if all subsets of $\mathbb{R}^2$ of size at most k can be χ colored using 3 colors, then if $k+1$ given points cannot be χ colored with 3 colors, their resulting unit distance graph must be connected and each point must have degree at least 3.

Throughout this proof, by a *circle* we mean the circumference of a circle of radius 1. Now note that any circle admits a χ coloring with 2 colors. This is because any point x on the circle is a vertex of a unique regular hexagon inscribed in the circle, and the vertices of this hexagon can be 2-colored in a χ way by alternating the colors.

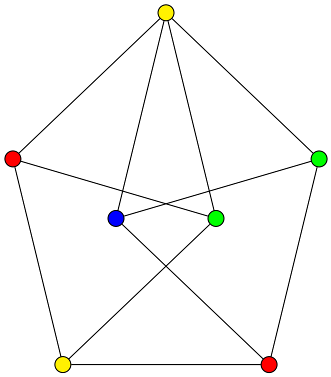

Figure 2.4: A graph that cannot be χ colored with 3 colors.

But the only neighbors of x in the corresponding unit distance graph are vertices connected to x in this hexagon.

It follows in particular that a circle together with its center admits a χ coloring with 3 colors.

Therefore, any 4 points on $\mathbb{R}^2$ can be χ colored using 3 colors, since from the above we may assume that three of the points are on the circle of radius 1 and center the fourth point.

Lemma 2.7. *Any 5 points in $\mathbb{R}^2$ can be χ colored with 3 colors.*

Proof. In a finite graph, the sum of the degrees of the vertices is twice the number of edges, so in particular it is even, and it follows that in no graph on 5 vertices can all the vertices have degree 3.

From the observations above, given 5 points on the plane, we may assume that the degree of each of them in the corresponding graph is at least 3, and therefore that one of them must in fact have degree 4 (i.e., we may assume that 4 of the 5 points lie on a circle with center the fifth point). But then the graph can be χ colored using 3 colors. □

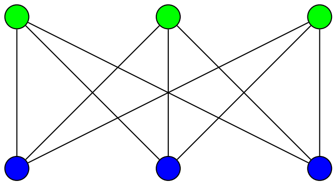

Figure 2.5: G_1

Now consider the graph defined by 6 points on the plane. As above, we may assume it is connected, and each point has degree at least 3. As above, if a point has degree 5, we are done. Suppose first that there is a point x of degree 4. We claim that the sixth point is connected to at most 2 other points, which is a contradiction. In effect, the circle centered at that point meets the circle centered at x in at most 2 points, and does not contain x.

We are left with the case where the graph is 3-regular, i.e., each vertex has degree 3. But there are only 2 connected 3-regular graphs in 6 vertices, see for example [12] and references therein.

One of these graphs, call it G_1, is just the complete bipartite graph $K_{3,3}$. To describe the other, call it G_2, consider the vertices of a hexagon. Join opposite vertices and every other vertex.

Note that since G_1 is bipartite, it can be χ colored with 2 colors (see Figure 2.5). Also, G_2 can be χ colored with 3 colors: Color two consecutive vertices of the hexagon with color 1, the following two with color 2, and the remaining pair with color 3 (see Figure 2.6). This completes the proof. □

Remark 2.8. As a matter of fact, G_1 cannot be realized as the distance-1 graph of 6 points in the plane. To see this, call A, B, C the points in one side of the partition.

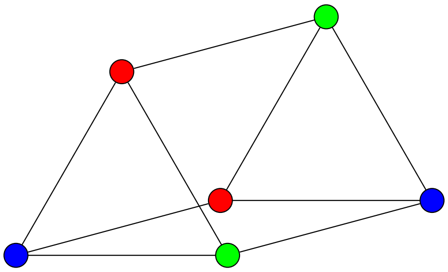

Figure 2.6: G_2

There is a unique circle (possibly a line) that contains them, but then the 3 points on the other side of the partition cannot all be centers of unit circles containing A, B, C.

On the other hand, G_2 can be realized: Start with the 3 vertices of an equilateral triangle, and translate them by one unit in some appropriate direction.

It is worth pointing out that the observation immediately preceding Proposition 2.6 that the chromatic number of the plane being larger than 3 can be verified by considering an appropriate finite graph (in this case, of size 7) is not an isolated incident. This is the content of the following:

Theorem 2.9. (De Bruijn-Erdős)
Given any graph G and any positive integer k, the chromatic number of G is at most k iff the chromatic number of any finite subgraph of G is at most k.

For a proof, see for example Theorem 3.6 in [11].

It follows in particular that there is a finite set of points in the plane whose unit distance graph has the same chromatic number as the plane. However, there are two drawbacks with the theorem.

First, even if the chromatic number of the plane is larger than 4, any finite *witness* may be enormous and therefore very difficult to detect. The best result to date is due to Dan Pritkin in [14], where it is shown that the distance-1 graph of any 12 points in $\mathbb{R}^2$ is 4-colorable.

Second, the proof of the De Bruijn-Erdős Theorem is strictly non-constructive, as it uses in an essential way the axiom of choice, in the form of the compactness of an appropriate product of (Hausdorff) compact spaces. Given our current knowledge, it is not unconceivable that there are models of set theory where the axiom of choice fails, every finite subset of the plane has chromatic number at most 4, and the plane itself a has larger chromatic number. These matters are discussed in detail in [4].

The situation above is not entirely hypothetical. For example, it is shown in [13] that if we restrict our attention to *Lebesgue measurable* colorings, then the chromatic number of the plane is at least 5. See also [4].

CHAPTER 3

REGRESSIVE FUNCTIONS ON PAIRS

This short chapter builds on Caicedo [9]. It concerns the following coloring problem:

For $m \leq l$ positive integers, consider the complete graph $G = G(m,l)$ on the set of vertices $V = \{m, m+1, \ldots, l\}$. A *regressive coloring* of G is a function that assigns to each edge $\{a,b\}$ of G a color c, that is a natural number strictly less than both a and b: $0 \leq c < \min\{a,b\}$. These colorings are natural to consider in the context of canonical Ramsey theory.

Given a coloring f of G, a *min-homogeneous* set is a subset H of V such that whenever $a < b < c$ are in H, then $f(\{a,b\}) = f(\{a,c\})$, i.e., whenever d is an edge with vertices in H, $f(d)$ only depends on the minimum of d. We say that H is *homogeneous* if f is constant on edges from H.

Typically, in Ramsey theory, one proves that a coloring of a large graph admits appropriately sized homogeneous sets. This is not possible in general in this context: Simply consider the coloring $f(d) = \min(d) - 1$.

On the other hand, as shown in Section 3 of [9], for any m and n there is an l such that any regressive coloring of $G(m,l)$ admits a min-homogeneous set of at least n elements.

Denote by $g(n,m)$ the smallest possible l such that the above holds. The following values of g are established in [9]:

1. $g(4,2) = 15$.

2. $g(4,3) = 37$.

3. $g(4,4) \leq 85$.

We now give the following result.

Theorem 3.1. $g(4,4) = 85$.

Proof. This follows by constructing a regressive coloring f of $G(4,84)$ which contains no min-homogeneous set of size 4. The function was constructed and verified using Matlab, modifying a coloring from [9] that proves the weaker bound $g(4) \geq 2g(3)+3 = 77$. Its definition, and the code that verifies it works, can be found in Appendix A.1. □

Let us remark that the arguments of [9] give in general that

$$g(4,n) \leq 2^n n + 12 \cdot 2^{n-3} + 1$$

for $n \geq 3$. We close the chapter by stating without proof an improvement:

Fact 3.2. (Caicedo)
For all positive n, we have that $g(4,n) \leq 2^{n-1}(n+7) - 3$.

CHAPTER 4

SATISFACTORY COLORINGS

4.1 The Problem

Question 4.1. *Is it possible to color the positive integers using n colors, in such a way that for any a, the numbers $a, 2a, 3a, ..., na$ receive different colors?*

We call *satisfactory* a coloring witnessing a positive answer to Question 4.1. Question 4.1 was posted by Palvolgyi Dömötör to MathOverflow.net [2], a website whose stated primary goal is for users to ask and answer research level mathematics questions. The question, as Dömötör states in his post, is an extension of a problem originally published in the Hungarian journal KöMaL (Középiskolai Matematikai és Fizikai Lapok), a Mathematics and Physics journal primarily aimed at High School Students. In the April, 2010 issue, problem $A.506$ asked to show that there is a satisfactory coloring whenever $n + 1$ is prime [3]. In full generality, Question 4.1 remains open.

In addition to asking the question of whether there are satisfactory colorings for a given n, it is natural to ask the following:

Question 4.2. *Given n, how many satisfactory colorings for n are there, if any at all?*

We start by discussing an example. Then, we use the insight gained there to answer Question 4.2. We begin approaching Question 4.1 in the next chapter.

4.2 An Example

Here we discuss how one can approach building a satisfactory coloring for 5 colors "by hand."

The idea is to create a table in which every column contains each color and contains no repetition. The first column, whose entries are to the left **and** right of the first vertical line, contains the numbers being colored on the left, and the color each receives on the right. A column is referred to as *complete* if the column uses all available colors. So, for any satisfactory coloring, every column will be complete. For instance, the following complete column represents the first column of the table used for 5 colors, and the *ith* column is the column whose left entries are the numbers $i, 2i, \ldots, 5i$. The table is read as: Number 1 is being colored yellow, 2 is being colored red, 3 is being colored blue, 4 is being colored green and 5 is being colored orange.

1	yellow
2	red
3	blue
4	green
5	orange

Since the colors we decide to use are not important, we identify them from now on with the numbers 1,2,3,4,5. Something important to notice at this point is that if we construct a satisfactory coloring using 5 colors, we may create a "new" coloring by simply permuting the colors. This means that for every satisfactory coloring there are precisely 5! ways in which the colors can be assigned for the first column. However, this “new” coloring is merely a permutation of the original coloring and, thus, offers no additional information and we regard any two colorings obtained this way as identical.

Suppose that c is a satisfactory coloring using 5 colors,

$$c : \mathbb{Z}^{+} \to \{1, 2, 3, 4, 5\}.$$

We may assume that $c(i) = i$ for $i \in \{1, 2, 3, 4, 5\}$. So we begin with the following table:

1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	12	14	16	18	20
3	3	6	9	12	15	18	21	24	27	30
4	4	8	12	16	20	24	28	32	36	40
5	5	10	15	20	25	30	35	40	45	50

Now, we can fill in the values that are determined by the assignment of column 1. This gives us:

1	1	2	2	3	3	4	4	5	5	6	7	8	9	10
2	2	4	4	6		8		10		12	14	16	18	20
3	3	6		9		12		15		18	21	24	27	30
4	4	8		12		16		20		24	28	32	36	40
5	5	10		15		20		25		30	35	40	45	50

Next, note that $c(6)$ cannot be 2 since $c(2) = 2$ and 2 and 6 are both in column 2. Similarly, $c(6) \neq 4$ since $c(4) = 4$. Also, $c(6) \neq 3$ since $c(3) = 3$ and 3 and 6 are both in column 3. So we have that $c(6) = 1$ or $c(6) = 5$. In fact, in Section 5.2, we will show that both choices result in a satisfactory coloring. For now, we will assume that $c(6) = 1$, and that this choice results in a satisfactory coloring. This gives us the following table:

1	1	2	2	3	3	4	4	5	5	6	1	7		8		9		10	
2	2	4	4	6	1	8		10		12		14		16		18		20	
3	3	6	1	9		12		15		18		21		24		27		30	
4	4	8		12		16		20		24		28		32		36		40	
5	5	10		15		20		25		30		35		40		45		50	

Now, consider $c(10)$. Since 10 is in both column 2 and 5, $c(10) \neq 1, 2, 4, 5$ and thus $c(10) = 3$. Thus, since column 2 now contains the colors $1, 2, 3$, and 4, we see that $c(8) = 5$. Now our table is:

1	1	2	2	3	3	4	4	5	5	6	1	7		8	5	9		10	3
2	2	4	4	6	1	8	5	10	3	12		14		16		18		20	
3	3	6	1	9		12		15		18		21		24		27		30	
4	4	8	5	12		16		20		24		28		32		36		40	
5	5	10	3	15		20		25		30		35		40		45		50	

The following table is obtained by the same reasoning:

1	1	2	2	3	3	4	4	5	5	6	1	7		8	5	9	5	10	3
2	2	4	4	6	1	8	5	10	3	12	2	14		16	3	18	3	20	1
3	3	6	1	9	5	12	2	15	4	18	3	21		24	4	27	4	30	5
4	4	8	5	12	2	16	3	20	1	24	4	28		32	1	36	1	40	2
5	5	10	3	15	4	20	1	25	2	30	5	35		40	2	45	2	50	4

At this point, notice that no colors have been assigned yet to column 7. This is because column 7 is not dependent upon our choice of the first column. This follows from the fact that 7 is relatively prime with all numbers less than or equal to 5 or, equivalently, with $2 \cdot 3 \cdot 5 = 30$. As a matter of fact, for every column x for which $(x, 30) = 1$, we have that $c(x), c(2x), c(3x), c(4x)$, and $c(5x)$ are not determined by $c(y)$ for any $y < x$. This is quite intriguing, since this means, for example, that for every prime we encounter greater than 5 we will, in some sense, be starting from the beginning. By this, we mean that for every integer $x > 5$ with $(x, 30) = 1$, there will be 5! ways in which we can color column x that will result in a satisfactory coloring. This observation leads us to the key notion of the *n-core*, and to the following results, the first of which deals with extending a coloring of the core to all positive integers and the second, a corollary of the first, identifies the number of satisfactory colorings there are in the case of n colors, provided a coloring of the core does in fact exist.

4.3 The Core

Definition 4.3. *The n-*core*, or simply the* core *if n is understood, is the set $K = K_n$ of all positive integers whose prime decomposition only involves primes less than or equal to n.*

Definition 4.4. *Say that $X \subseteq \mathbb{Z}^+$ is n-*appropriate *iff X is nonempty and contains ai and a/j whenever $a \in X$, $i, j \leq n$, and j divides a.*

If X is n-appropriate, say that $c : X \to \{1, \ldots, n\}$ is satisfactory iff $c(ai) \neq c(aj)$ whenever $a \in X$ and $i < j \leq n$. Note that this notion coincides with the previous notion of satisfactory when $X = \mathbb{Z}^+$.

We denote by A_n the set of numbers relatively prime to $n!$, i.e., those positive integers whose prime decomposition only involves prime numbers strictly larger than n.

If $X \subseteq \mathbb{Z}^+$ and $k \in \mathbb{Z}^+$, we denote by $k \cdot X$ the *dilation* of X by factor k:

$$k \cdot X = \{ka : a \in X\}.$$

The notation $X = \dot{\bigcup}_{a \in B} X_a$ means both that X is the union of the X_a for $a \in B$, and that the sets X_a are pairwise disjoint.

Lemma 4.5. *A set $X \subseteq \mathbb{Z}^+$ is n-appropriate iff there is a nonempty set $B \subseteq A_n$ such that*

$$X = \dot{\bigcup_{k \in B}} k \cdot K_n.$$

Moreover, if this is the case, then we have $B = A_n \cap X$.

Proof. Note that K_n is n-appropriate and therefore so is $k \cdot K_n$ for any $k \in A_n$. It follows that any X of the form $\dot{\bigcup}_{k \in B} k \cdot K_n$ for $B \subseteq A_n$ and nonempty is n-appropriate as well.

Towards the converse, suppose now that X is n-appropriate. From the uniqueness of prime factorization, it follows that each $m \in \mathbb{Z}^+$ can be uniquely written in the form $m = k_m b_m$ where $k_m \in A_n$ and $b_m \in K_n$. Let $B = \{k_m : m \in X\}$. We claim that $X = \dot{\bigcup}_{k \in B} k \cdot K_n$.

First, note that if $x \neq y$ are in A_n, then $x \cdot K_n$ and $y \cdot K_n$ are pairwise disjoint. Now, if $k \in B$, then there is some $m \in X$ such that $k = k_m$. By assumption, $h/j \in X$ whenever $h \in X$ and $j \leq n$ divides h. It follows immediately that in fact $h/j \in X$ whenever $h \in X$ and $j \in K_n$ divides h. In particular, $k = k_m = m/b_m \in X$. Similarly, by assumption $hi \in X$ whenever $h \in X$and $i \leq n$, and it follows immediately that $hi \in X$ whenever $h \in X$ and $i \in K_n$. Therefore, $k \cdot K_n \subseteq X$. This means that

$$\bigcup_{k \in B} k \cdot K_n \subseteq X.$$

But, if $m \in X$, then $m \in k_m \cdot K_n$, and we have that

$$\bigcup_{k\in B} k\cdot K_n \supseteq X.$$

This proves the equality, and since (as addressed above) the union is disjoint, this completes the proof.

Note that we have shown that if X is n-appropriate and B is as above, then in fact $B = A_n \cap X$. Since the sets $k\cdot K_n$ are pairwise disjoint as k varies over K_n, it follows that for any n-appropriate X there is a unique $B \subseteq A_n$ such that $X = \bigcup_{k\in B} k\cdot K_n$, and we are done. □

For X n-appropriate, let

$$C_X = \{c : X \to \{1,\ldots,n\} : c \text{ is satisfactory}\},$$

and denote by C the set $C_{\mathbb{Z}^+}$.

The following theorem shows that $C \neq \varnothing$ iff $C_X \neq \varnothing$ for some n-appropriate set X iff $C_X \neq \varnothing$ for all n-appropriate sets X.

In particular, it follows that the question of whether there are any satisfactory colorings for n is really a question about whether there are satisfactory colorings of the n-core K_n. In fact, the theorem shows how the satisfactory colorings of the core completely determine all satisfactory colorings.

Theorem 4.6. 1. *Suppose $X \subseteq Y$ are n-appropriate. If $C_Y \neq \varnothing$, then $C_X \neq \varnothing$. In fact, $c \upharpoonright X \in C_X$ for any $c \in C_Y$.*

2. *Given $k \in A_n$, if $c \in C_{k\cdot K_n}$, let $c' : K_n \to \{1,\ldots,n\}$ be the map given by $c'(b) = c(kb)$. Then, $c' \in C_{K_n}$.*

3. *Given $k \in A_n$, if $c \in C_{K_n}$, let $\hat{c}_k : k \cdot K_n \to \{1, \ldots, n\}$ be the map given by $\hat{c}_k(m) = c(m/k)$. Then, $\hat{c}_k \in C_{k \cdot K_n}$.*

4. *Suppose that $C_{K_n} \neq \varnothing$ and X is n-appropriate. Then, $c \in C_X$ iff for each $k \in A_n \cap X$, there is a map $c^k \in C_{K_n}$ such that*

$$c = \bigcup_{k \in A_n \cap X} \widehat{c^k}_k.$$

5. *$C \neq \varnothing$ iff $C_X \neq \varnothing$ for any n-appropriate X iff $C_X \neq \varnothing$ for some n-appropriate set X. Moreover if $X \subseteq Y$ are n-appropriate, then $d \in C_X$ iff $d = c \restriction X$ for some $c \in C_Y$.*

Proof. (1) This is clear.

(2) Given $k \in A_n$ and $c \in C_{k \cdot K_n}$, if c' is defined as in item 2, then $c'(ib) = c(kib) \neq c(kjb) = c'(jb)$ for any $b \in K_n$ and $i < j \leq n$ since c is satisfactory. But, then c' is satisfactory as well.

(3) Conversely, if $c \in C_{K_n}$, $k \in A_n$, and $\hat{c}_k$ is defined as in item 3, then $\hat{c}_k(im) = c(i(m/k)) \neq c(j(m/k)) = \hat{c}_k(jm)$ for any $m \in k \cdot K_n$ and $i < j \leq n$ since c is satisfactory. But, then $\hat{c}_k$ is satisfactory as well.

(4) Suppose that $C_{K_n} \neq \varnothing$ and X is n-appropriate. For each $k \in A_n \cap X$ let $c^k \in C_{K_n}$ and define $c = \bigcup_{k \in A_n \cap X} \widehat{c^k}_k$. As shown in Lemma 4.5, $k \cdot K_n \cap l \cdot K_n = \varnothing$ whenever $k \neq l$ are in A_n. From this, and item 3, c is well defined and has domain $\bigcup_{k \in A_n \cap X} k \cdot K_n$, which equals X, again by Lemma 4.5. Suppose $m \in X$ and $i < j \leq n$. Then, there is a unique $k \in A_n \cap X$ such that mi and mj belong to $k \cdot K_n$, and by item 3 it follows that $c(mi) \neq c(mj)$. This proves that c is satisfactory.

Conversely, if $c \in C_X$, then $d = c \restriction k \cdot K_n \in C_{k \cdot K_n}$ for any $k \in A_n \cap X$, by item 1, and $c^k = d' \in C_{K_n}$ by item 2. But $d = \hat{d'}_k$, i.e., $c = \bigcup_{k \in A_n \cap X} \hat{c^k}_k$, and this completes the proof of item 4.

(5) Now, if X is n-appropriate, and $C_X \neq \varnothing$, then $C_{k \cdot K_n} \neq \varnothing$ for any k in the nonempty set $A_n \cap X$, by item 1. But then $C_{K_n} \neq \varnothing$, by item 2. It follows from item 4 that $C = C_{\mathbb{Z}^+} \neq \varnothing$. But then $C_Y \neq \varnothing$ for any n-appropriate Y, again by item 1.

Finally, if $X \subseteq Y$ are n-appropriate and $c \in C_Y$, then $d = c \restriction X \in C_X$, by item 1. Conversely, if $d \in C_X$, let $e \in C_{K_n}$, which exists as shown above. Let $c^k = e$ for $k \in A_n \cap (Y \setminus X)$. For $k \in A_n \cap X$, let $c^k = (d \restriction k \cdot K_n)'$. As in item 4, we have that $c = \bigcup_{k \in A_n \cap Y} \hat{c^k}_k \in C_Y$. And, by construction, $d = c \restriction X$. This completes the proof of item 5. □

The importance of this theorem is paramount. It provides us with the ability to restrict our attention from all of $\mathbb{Z}^+$ to a set comprised of elements with an inherent underlying structure. As such, it has played a dominant role in many of our results.

The relation between arbitrary satisfactory colorings and colorings of the core detailed in Theorem 4.6 has the following corollary:

Corollary 4.7. *For $n > 1$, with C and C_{K_n} as above, if $C_{K_n} \neq \varnothing$ then $|C| = |\mathbb{R}|$.*

Proof. As explained in Section 4.2, if there is a coloring of the core, there are at least $n! \geq 2$ such colorings (obtained by simply permuting the colors). Note that A_n is countably infinite. By item 4 of Theorem 4.6, there is a bijective correspondence between the elements of C, and the set of functions from A_n to C_{K_n}: $|C| = |C_{K_n}^{A_n}| \geq n!^{|A_n|} = |\mathbb{R}|$, by Corollary 1.25.

On the other hand, any element of C is a function from $\mathbb{Z}^+$ to $\{1, \ldots, n\}$, so $|C| \leq |\{1, \ldots, n\}^{\mathbb{Z}^+}| = n^{|\mathbb{N}|} = |\mathbb{R}|$, by Corollary 1.25.

It follows that $|C| = |\mathbb{R}|$, by the Schröder-Bernstein theorem. □

Convention 4.8. Note that we may further require that if $c \in C$, then $c(i) = i$ for $i \leq n$, without affecting the above computations, and we assume this further requirement from now on.

What Theorem 4.6 and Corollary 4.7 give us can be interpreted as follows. If there is a satisfactory coloring of K_n, then there are continuum many satisfactory colorings of $\mathbb{Z}^+$ using n colors. However, this abundance of colorings is a distraction since the underlying structure of any satisfactory coloring can be described in terms of what is happening on the core.

CHAPTER 5

STRONG REPRESENTATIONS

5.1 Strong Representatives

In this section, we present a condition on n ensuring the existence of satisfactory colorings with n colors. The construction below was suggested in MathOverflow by Victor Protsak, see [2].

From now on, we denote by $\mathbf{n}$ the set $\{1, 2, \dots, n\}$.

Theorem 5.1. *Let $n, k \in \mathbb{N}$. If $p = nk + 1$ is prime, and $1^k, 2^k, 3^k, \dots, n^k$ are distinct modulo p, then the following produces a satisfactory coloring: Let*

$$\varphi : \{i^k \pmod p : i \in \mathbf{n}\} \to \mathbf{n}$$

be the bijection given by $\varphi(i^k \pmod p) = i$. Given $m \in \mathbb{Z}^+$, write it as $m = ap^r$ where $(a, p) = 1$ and $r \in \mathbb{N}$. Now define $c(m) = \varphi(a^k \pmod p)$.

Proof. We begin noting that by Corollary 1.7 there are exactly n pairwise incongruent nonzero kth power residues modulo $nk + 1$. It follows that, for any b with $(b, p) = 1$, $b^k = j^k \pmod p$ for some $j \in \mathbf{n}$. Now let $d, e \in \mathbf{n}$. We need to argue that $c(dm) = c(em)$ if and only if $d = e$. To see this, consider $dm = adp^r$. Thus, $c(dm) = \varphi\big((ad)^k \pmod p\big)$. Similarly, we have that $c(em) = \varphi\big((ae)^k \pmod p\big)$. Since φ is a bijection,

$c(dm) = c(em)$ implies that $(ad)^k \equiv (ae)^k \pmod{p}$ and therefore $d^k \equiv e^k \pmod{p}$, so $d = e$ by assumption. □

This leads us to the following definition.

Definition 5.2. Strong Representations.
A satisfactory coloring $c : K_n \to \mathbf{n}$ admits a strong representation if and only if there exists a prime p of the form $nk+1$ such that $1^k, \dots, n^k$ are pairwise distinct modulo p and, letting

$$\varphi : \mathbf{n} \to \{a^k \pmod{p} : a \in \mathbf{n}\}$$

be the map

$$\varphi(i) = i^k \pmod{p},$$

then

$$\varphi \circ c(a) = a^k \pmod{p}$$

for all a. In this case, we call φ the strong representation of c, and p the associated prime. We also say that p is a strong representative of order n (for c).

Theorem 5.1 lends us the ability to construct a satisfactory coloring in a very simple way. However, granting the existence of such a prime has eluded us. In fact, at this time, we have only found nontrivial strong representatives of order 32 or less. Here, a prime of the form $p = nk+1$ is *nontrivial* iff $k > 2$. We call these primes trivial when $k \leq 2$, since the requirement of Theorem 5.1 is automatically satisfied in this case, see Subsection 5.1.1.

As evidence of how incredibly difficult the search for strong representatives is, we mention the following. The smallest strong representative of order 32 is $p =$

$5,209,690,063,553$. Identifying it took nearly one month of cpu time on an Intel Core™i7 machine.

Table 5.1 lists for $n \leq 33$ the smallest strong representative $p = nk + 1$ of order n.

5.1.1 Trivial Representatives

It is clear from Theorem 5.1 that if $p = n + 1$ is prime, then the coloring

$$c(m) = a \pmod{p}$$

where $m = ap^r$, $(a, p) = 1$, is a satisfactory coloring with n colors. This solves the question originally asked in KöMal [3] . From the infinitude of the primes, we have:

Corollary 5.3. *There are infinitely many values of* n *for which a satisfactory coloring exists.*

An easy observation also gives us:

Theorem 5.4. *If* $p = 2n + 1$ *is prime, then the map*

$$c(m) = a^2 \pmod{p}$$

where $m = ap^r$, $(a, p) = 1$, *induces a satisfactory coloring with* n *colors.*

Proof. We must show that if $1 \leq i < j \leq n$, then $i^2 \not\equiv j^2 \pmod{p}$, as the result then follows from Theorem 5.1. But, $i^2 \equiv j^2 \pmod{p}$ implies that $p|j - i$ or $p|j + i$. Since

$$0 < j - i < n < p$$

n	k	p
1	1	2
2	1	3
3	2	7
4	1	5
5	2	11
6	1	7
7	94	659
8	2	17
9	2	19
10	1	11
11	2	23
12	1	13
13	198364	2578733
14	2	29
15	2	31
16	1	17
17	2859480	48611161
18	1	19
19	533410	10134791
20	2	41
21	2	43
22	1	23
23	2	47
24	56610508	1358652193
25	1170546910	29263672751
26	2	53
27	6700156678	180904230307
28	1	29
29	2	59
30	1	31
31	27184496610	842719394911
32	162802814486	5209690063553
33	2	67

Table 5.1: Smallest strong representative $p = nk + 1$ of order n for $n \leq 33$.

and

$$0 < j + i \leq 2n < p,$$

both cases are impossible. □

On the other hand, the primality of $nk + 1$ for $k \geq 2$ does not automatically ensure that the hypothesis of Theorem 5.1 is satisfied, as evidenced in Table 5.1. For example, if $n = 3$, then $p = n4 + 1 = 13$ is prime. However, $2^4 = 16$, $3^4 = 81$, and $81 \equiv 16 \pmod{13}$.

We expect an affirmative answer to Question 4.1:

Conjecture 5.5. *Satisfactory colorings exist for all $n \in \mathbb{N}$.*

Question 5.6. *Do strong representatives of all orders exist?*[1]

Of course, an affirmative answer to Question 5.6 implies Conjecture 5.5, but Conjecture 5.5 may be more tractable. For example, all colorings obtained through strong representatives are *multiplicative*, and in fact are *$\mathbb{Z}_n$-colorings*, as defined below. However, there are satisfactory colorings that are non-multiplicative, multiplicative colorings that are not $\mathbb{Z}_n$-colorings, and $\mathbb{Z}_n$-colorings that do not admit a strong representation, see Sections 5.4 and 6.3.

5.2 Satisfactory Colorings with $n \leq 5$

In this section, we show that if $n \leq 4$, then there is a unique satisfactory coloring c of K_n with n colors, subject to the convention that $c(i) = i$ for $i \in \mathbf{n}$. We also show that there are precisely 2 satisfactory colorings of K_5. This is immediate if $n = 1$. For

[1] See Section 7.2.

$n = 2$, note that $K_2 = \{2^a \mid a \in \mathbb{N}\}$ and $c(a) = a + 1 \pmod 2$ is the only satisfactory coloring.

Assume $n = 3$. The result follows by generalizing a simple observation: Suppose we are trying to define a satisfactory coloring c. Since $6 = 2{\cdot}3$, we have that $c(6) \neq c(2) = 2$ and $c(6) \neq c(3) = 3$. Thus, we are forced to define $c(6) = 1$. This then forces us to choose $c(4) = 3$ and $c(9) = 2$. Also, since $c(12) \neq c(4) = 3$ and $c(12) \neq c(6) = 1$, we have that $c(12) = 2$.

Lemma 5.7. *If c is a satisfactory coloring of K_3 then, for any $x \in K_3$, we have that $c(6x) = c(x)$, $c(9x) = c(2x)$, and $c(4x) = c(3x)$.*

Proof. If $x \in K_3$, then $c(x)$, $c(2x)$, and $c(3x)$ are pairwise distinct. Note that $c(6x) \notin \{c(2x), c(3x)\}$. This it must be the case that $c(6x) = c(x)$. Similarly, $c(4x) \notin \{c(2x), c(6x)\} = \{c(x), c(2x)\}$, so $c(4x) = c(3x)$. Therefore, $c(9x) = c(3{\cdot}3x) = c(4 \cdot 3x) = c(12x) = c(6 \cdot 2x) = c(2x)$. □

Theorem 5.8. *There is a unique satisfactory coloring of K_3.*

Proof. By Theorem 5.1, we know that there is at least one satisfactory coloring, since $7 = 3 \cdot 2 + 1$ is prime. Let

$$A = \{n \in K \mid \forall c_1, c_2 \in C_K\, (c_1(in) = c_2(in) \text{ for } i \in \mathbf{3}\}.$$

Then, $1 \in A$. Moreover, by Lemma 5.7, if $n \in A$, then $2n \in A$ and $3n \in A$. But then $A = K$. □

We can easily generalize the argument above to prove the case $n = 4$:

Lemma 5.9. *If c is a satisfactory coloring of K_4, then for any $x \in K_4$, we have that $c(16x) = c(6x) = c(x)$, $c(12x) = c(2x)$, $c(8x) = c(3x)$, and $c(9x) = c(4x)$.*

Proof. If $x \in K_4$, then $c(x)$, $c(2x)$, $c(3x)$, and $c(4x)$ are pairwise distinct. Since $c(6x) \notin \{c(2x), c(3x), c(4x)\}$, we have $c(6x) = c(x)$. Therefore, $c(12x) = c(6 \cdot 2x) = c(2x)$. Since $c(8x) \notin \{c(2x), c(4x), c(6x)\}$ and $c(6x) = c(x)$, we have $c(8x) = c(3x)$. Therefore, $c(9x) = c(3 \cdot 3x) = c(8 \cdot 3x) = c(24x) = c(6 \cdot 4x) = c(4x)$. Similarly, $c(16x) = c(4 \cdot 4x) = c(9 \cdot 4x) = c(36x) = c(6 \cdot 6x) = c(6x) = c(x)$. □

Theorem 5.10. *There is a unique satisfactory coloring of K_4.*

Proof. By Theorem 5.1, we know that there is at least one satisfactory coloring, since $5 = 4 \cdot 1 + 1$ is prime. As before, let

$$A = \{n \in K \mid \forall c_1, c_2 \in C_K \, (c_1(in) = c_2(in) \text{ for } i \in \mathbf{4}\}.$$

Then, $1 \in A$. By Lemma 5.9, if $n \in A$, then $\{2n, 3n, 4n\} \subseteq A$. But then $A = K$. □

The situation with $n = 5$ is slightly more delicate. Note first that $11 = 5 \cdot 2 + 1$, so we have a satisfactory coloring c_5 given by $c_5(i) = i$ for $i \leq 5$ and $c_5(a) = c_5(b)$ iff $a^2 \equiv b^2 \pmod{11}$ for any $a, b \in K_5$. The coloring c_5 satisfies $c_5(6) = c_5(5) = 5$, since $36 \equiv 25 \pmod{11}$.

Similarly, $421 = 5 \cdot 84 + 1$ is prime and

$$1^{84} \equiv 1 \pmod{421},$$

$$2^{84} \equiv 279 \pmod{421},$$

$$3^{84} \equiv 252 \pmod{421},$$

$$4^{84} \equiv 377 \pmod{421},$$

$$5^{84} \equiv 354 \pmod{421},$$

$$6^{84} \equiv 1 \pmod{421},$$

so we have a satisfactory coloring c_1 given by $c_1(i) = i$ for $i \le 5$ and $c_1(a) = c_1(b)$ iff $a^{84} \equiv b^{84} \pmod{421}$ for any $a, b \in K_5$. The coloring c_1 satisfies $c_1(6) = c_1(1) = 1$.

We now proceed to show that these are the only possibilities. The following lemma follows by the same elementary reasoning as Lemmas 5.7 and 5.9 (but note the additional requirement that $c(6x) = c(x)$), we omit the details.

Lemma 5.11. *If c is a satisfactory coloring of K_5, $x \in K_5$, and $c(6x) = c(x)$, then $c(20x) = c(6x) = c(x)$, $c(25x) = c(12x) = c(2x)$, $c(18x) = c(16x) = c(10x) = c(3x)$, $c(24x) = c(15x) = c(4x)$, and $c(30x) = c(9x) = c(8x) = c(5x)$.*

Theorem 5.12. *The coloring c_1 defined above is the unique satisfactory coloring c of K_5 with $c(6) = 1$.*

Proof. Let

$$A = \{n \in K \mid \forall c \in C_K \text{ with } c(6) = 1, \text{ we have } c(in) = c_1(in) \text{ for } i \in \mathbf{5} \text{ and } c(6n) = c(n)\}.$$

We have $1 \in A$. By Lemma 5.11, if $n \in A$, then also $in \in A$ for $2 \le i \le 5$. But then $A = K$. □

Theorem 5.13. *The coloring c_5 is the unique satisfactory coloring c of K_5 with $c(6) = 5$. Moreover, the only satisfactory colorings of K_5 are c_1 and c_5.*

Proof. Let φ be the transposition (35) considered as a permutation of $\mathbf{5}$. Consider the map π that to a satisfactory coloring c of K_5 assigns the coloring $\pi(c)$ given by

$$\pi(c)(2^a 3^b 5^d) = \varphi(c(2^a 5^b 3^d)).$$

Note that $\pi(c)$ is also satisfactory, and that π is a bijection of C_{K_5} to itself, since in fact $\pi(\pi(c)) = c$ for any c.

Suppose that c is satisfactory and $c(6) = 5$. Then, $c(10) = 1$. Otherwise, since $c(10) \notin \{c(2), c(4), c(6)\} = \{2,4,5\}$, we must have $c(10) = 3$. But then $c(8) = 1$. Since $c(12) \notin \{c(3), c(4), c(6), c(8)\} = \{1,3,4,5\}$, we must have $c(12) = 2$. But then $c(20) \notin \{c(4), c(5), c(8), c(10), c(12)\} = \{1,2,3,4,5\}$, a contradiction.

It follows that $c(10) = 1$ but then $\pi(c)(6) = \varphi(c(10)) = \varphi(1) = 1$ and therefore $\pi(c) = c_1$. Since π is injective, it follows that there is a unique c with $c(6) = 5$. But then $c = c_5$.

Finally, given any satisfactory coloring c of K_5, since $c(6) \notin \{c(2), c(3), c(4)\} = \{2,3,4\}$, we must have that $c(6) \in \{1,5\}$, which implies that $c = c_1$ or $c = c_5$. □

5.2.1 Density of Strong Representatives

In Section 5.2, we identified the colorings c_5 and c_1 (with associated primes 11 and 421, respectively) as being the only satisfactory colorings for $n = 5$. Note that there are 76 primes in the interval $[12, 420]$ and none of them are strong representatives of order 5. Now, it is only natural to ask whether 11 and 421 are the only strong representatives of order 5. This is not the case:

Example 5.14. The prime $p = 701 = 5 \cdot 140 + 1$ is a strong representative of order 5. In effect,

$$1^{140} \equiv 1 \pmod{701},$$

$$2^{140} \equiv 210 \pmod{701},$$

$$3^{140} \equiv 464 \pmod{701},$$

$$4^{140} \equiv 638 \pmod{701},$$

$$5^{140} \equiv 89 \pmod{701},$$

are all distinct. Moreover, $6^{140} \equiv 1 \pmod{701}$, so p is a strong representative for c_1. Similarly, one can check that $p = 2311 = 5 \cdot 462 + 1$ is a strong representative of order 5 for c_5.

Question 5.15. *Asymptotically, how many primes are strong representatives of order 5, and are the resulting colorings equidistributed among c_5 and c_1?*

Recall that, given a real x, $\pi(x)$ denotes the number of primes $p \leq x$. Several proofs of Dirichlet's theorem (Theorem 1.8) actually establish a version of the prime number theorem for arithmetic progressions, namely, that for any $m \geq 3$, the primes are uniformly distributed among the $\phi(m)$ many congruence classes of integers relatively prime to m: For $(a, m) = 1$, denote by $\pi(x, m, a)$ the number of primes of the form $mk + a$ that are less than or equal to x. Then,

$$\pi(x, m, a) \sim \frac{1}{\phi(m)} \cdot \frac{x}{\log x}$$

as $x \to \infty$, where the notation means that the limit of the quotient of the two expressions is 1. Note that the right–hand side is independent of a. Put another way, about $1/\phi(m)$ of all primes are of the form $mk + a$. See [1] for references.

Since $1/\phi(5) = 1/4$ is a constant, it really makes no difference whether Question 5.15 is interpreted as asking for the proportion of strong representatives of order 5 among all primes, or among primes of the form $5k + 1$.

Given a real x, denote by $C_1(x)$ and $C_5(x)$, the sets of primes $p \leq x$ that are strong representatives of order 5 for c_1 and c_5, respectively, and let $C(x) = C_1(x) \cup C_2(x)$.

Conjecture 5.16. *1.* $|C_1(x)| \sim |C_5(x)|$ *as* $x \to \infty$.

2. $\displaystyle\lim_{x \to \infty} \frac{|C(x)|}{\pi(x)} > 0.$

Numerical data relevant to Conjecture 5.16 is shown in Appendix A.3. The Maple code producing the data is listed as Figure A.3.

Of course, similar questions can be asked for any n in place of 5.

Recall that Question 5.6 asks whether strong representatives of all orders exist. It is hard to imagine a scenario that would show the existence of strong representatives of a given order n without proving that there are infinitely many. For $n = 2$, we can prove that this is the case:

Theorem 5.17. *A prime p is a strong representative of order 2 iff $p \equiv \pm 3 \pmod 8$. In particular, there are infinitely many strong representatives of order 2.*

Proof. This is immediate from Theorem 1.10: If $p = 2k + 1$ is prime, then

$$2^k \equiv 1 \pmod p$$

iff $p \equiv \pm 1 \pmod 8$. It follows that if $p \equiv \pm 3 \pmod 8$, then 1 and 2^k are not congruent modulo p. □

Treating other cases seems to require a good understanding of higher order reciprocity laws. An argument that would apply to all n seems even more delicate.[2]

5.3 k-representatives

Definition 5.18. *Let $k \in \mathbb{Z}^+$. A prime p of the form $nk + 1$ is a* k-representative *if and only if p is a strong representative of order n.*

It is important to note that, in general, the roles of k and n cannot be interchanged. That is, typically, if $p = nk + 1$ is a strong representative of order n, then it is not

[2] See Section 7.2.

an n-representative, and if it is a k-representative, it is not a strong representative of order k.

The goal of this section is to show that for every $k > 2$, there are only finitely many n such that $p = nk + 1$ is a k-representative. In fact, we will show that for some values of k there are no such n.

We begin by discussing the case $k = 3$.

Theorem 5.19. *Suppose $p = n3 + 1$ is prime. Then, there is an $i \in \mathbf{n}$, $i > 2$ such that $i^3 \equiv 1 \pmod p$ or $i^3 \equiv 8 \pmod p$. In particular, p is not a 3-representative.*

Proof. Note first that -3 is a quadratic residue modulo p. This follows from Theorem 1.9:

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{3-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{n3+1}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

Work in $\mathbb{Z}_p$. Note that $x^3 = 1$ and $x \neq 1$ iff $x^2 + x + 1 = 0$ iff $4x^2 + 4x + 4 = 0$ iff $(2x + 1)^2 = -3$. Also, $x^3 = 8$ and $x \neq 2$ iff $x^2 + 2x + 4 = 0$, or $(x + 1)^2 = -3$.

We claim that for at least one $x \in \mathbf{n}$ this must happen. This is because $y^2 = -3$ has two solutions, one in the first half of the interval $[1, p - 1]$. If y is actually in the first third, we are done, we get $x = y - 1 \in \mathbf{n}$. Suppose otherwise. Note that either y or $p - y$ is odd. Call it z, and note that $z \leq 2p/3$. But then $x = (z - 1)/2$ is at most $(p - 1)/3$, so it is in $\mathbf{n}$. □

The case when k is a multiple of 4 can also be treated by elementary means. The key is the following theorem of Fermat, see Theorem 13.3 in [1]:

Theorem 5.20. (Fermat) *An odd prime p is a sum of two squares iff $p \equiv 1 \pmod 4$.*

Theorem 5.21. *If k is a multiple of 4 and $p = nk+1$ is k-representative, then $p < 2k^2$, so in particular, there are only finitely many k-representatives.*

Proof. Suppose $p = nk + 1$ is a k-representative. By Theorem 5.20, there are integers x and y with $1 \leq x < y$ such that $p = x^2 + y^2$. Fix an integer t. Then, if $p > t^2$ (which is true for all but finitely many p), then $y \leq p/t$. Otherwise, $p = x^2 + y^2 > y^2 > p^2/t^2$, a contradiction.

It follows that if $p \geq 2k^2$, then both x and y are in $\mathbf{n}$, but $x^2 \equiv -y^2 \pmod{p}$, so $x^k \equiv y^k \pmod{p}$. □

The bound on p found in Theorem 5.21 allows us for any given value of $k = 4m$ to identify all the possible values of p by a quick exhaustive search. Table 5.2 shows for $k = 4m \leq 100$ the values of n for which $p = nk + 1 = n4m + 1$ is a k-representative. If there are no such primes, we write $-N-$.

We now proceed to the general case. Letting

$$B(t, x) = \frac{te^{tx}}{e^t - 1} = \sum_{m=0}^{\infty} B_m(x) \frac{t^m}{m!},$$

then

$$B(t, x + 1) = \frac{te^{tx}e^t}{e^t - 1} = \frac{te^{tx}(e^t + 1 - 1)}{e^t - 1} = te^{xt} + B(t, x).$$

Thus

$$\sum_{m=0}^{\infty} \left(B_m(x + 1) - B_m(x) \right) \frac{t^m}{m!} = te^{xt} = \sum_{m=0}^{\infty} \frac{mx^{m-1}t^m}{m!},$$

or

$$B_m(x + 1) - B_m(x) = mx^{m-1}.$$

It follows easily that each $B_m(x)$ is a polynomial in x of degree m with rational coefficients. Moreover, we have

$k = 4m$	n	$p = nk + 1$
4	1	5
8	$-N-$	$-N-$
12	3	37
16	1	17
20	$-N-$	$-N-$
24	$-N-$	$-N-$
28	1	29
32	$-N-$	$-N-$
36	1	37
40	1	41
44	$-N-$	$-N-$
48	$-N-$	$-N-$
52	1	53
56	$-N-$	$-N-$
60	$1, 3$	$61, 181$
64	$-N-$	$-N-$
68	$-N-$	$-N-$
72	1	71
76	$-N-$	$-N-$
80	3	241
84	5	421
88	1	89
92	$-N-$	$-N-$
96	1	97
100	1	101

Table 5.2: $4m$-representatives.

$$\sum_{i=0}^{n} B_{m+1}(i+1) - B_{m+1}(i) = \sum_{i=0}^{n}(m+1)i^m,$$

or

$$\sum_{i=1}^{n} i^m = \frac{B_m(n+1) - B_{m+1}(0)}{m+1}.$$

A good reference on Bernoulli polynomials is [16]. Writing

$$B_m(x) = \sum_{k=0}^{m} \binom{m}{m-k} b_k x^{m-k},$$

the numbers $b_k = B_k(0)$ are usually called the *Bernoulli numbers*; they satisfy $b_{2k+1} = 0$ for all $k \geq 1$. In particular,

$$\sum_{i=1}^{n} i^{2m} = \frac{B_{2m+1}(n+1)}{2m+1},$$

for $m \geq 1$.

It will be important for us to know all the rational linear factors of the polynomial $B_m(x) - B_m(0)$; when n is odd this reduces to determining the rational linear factors of $B_m(x)$. A theorem of Inkeri, see Theorem 3 in [17], solves this problem.

Theorem 5.22. (Inkeri) [17]
The rational roots of a Bernoulli polynomial $B_m(x)$ can be only $0, \frac{1}{2}$, and 1. Moreover, all these are roots when $m > 1$ is odd.

With this result we are ready to prove the main result of this section.

Theorem 5.23. *If $k > 2$, then only finitely many primes are k-representatives.*

The following argument was suggested by Darij Grinberg and Gergely Harcos, see [15].

Proof. Suppose $p = nk + 1$ is a k-representative, that is, p is a strong representative of order n. We claim that

$$1^k + 2^k + \ldots + n^k \equiv 0 \pmod{p}.$$

To see this, let $S = 1^k + \ldots + (p-1)^k \pmod{p}$. Note that the map $i \mapsto 2i \pmod{p}$ is a permutation of $\mathbf{p-1}$. Therefore, $S \equiv 2^k S \pmod{p}$, so $S \equiv 0 \pmod{p}$. By Theorem 1.6, any nonzero kth power is congruent to i^k modulo p for some $i \in \mathbf{n}$, and for each such i there are precisely k integers in $\mathbf{p-1}$ realizing this congruence. But then $S \equiv k(1^k + \ldots + n^k) \pmod{p}$, and the claim follows.

Similarly,

$$\sum_{i=1}^{n} i^{2k} \equiv 0 \pmod{p}.$$

To see this, notice that, again by Theorem 1.6, there are precisely $\frac{p-1}{d} = \frac{n}{(2,n)}$ incongruent $2k$th power residues modulo p, where $d = (2k, p-1) = (2,n)k$. If n is odd, this is precisely n, which means that the numbers $1^{2k}, \ldots, n^{2k}$ are all distinct and are precisely all the nonzero $2k$th powers. If n is even, this means that each nonzero $2k$th power appears exactly twice among these numbers. In either case, it follows that the sum is zero by the same argument as in the previous paragraph.

Since

$$\sum_{i=0}^{n} i^{2k} = \frac{B_{2k+1}(n+1)}{2k+1},$$

it must be the case that $(nk+1) | B_{2k+1}(n+1)$. By Inkeri's Theorem 5.22, since $k > 2$, the polynomial $kx + 1$ is relatively prime to the polynomial $B_{2k+1}(x+1)$. But then there must be polynomials $u, v \in \mathbb{Q}[x]$ such that

$$(kx+1)\cdot u(x) + B_{2k+1}(x+1)\cdot v(x) = 1.$$

(In fact, v is a constant.)

Multiplying this identity by an appropriate integer constant $L = L_1 L_2$, it follows that there are polynomials $u' = Lu, B'_{2k+1} = L_1 B_{2k+1}, v' = L_2 v \in \mathbb{Z}[x]$ such that

$$(kx+1)\cdot u'(x) + B'_{2k+1}(x+1)\cdot v'(x) = L.$$

Since $B_{2k+1}(n+1) \equiv 0 \pmod{nk+1}$, evaluating the last displayed equation at $x = n$ gives us that $p = nk+1|L$. But there are only finitely many such p. □

Note that this argument does not supersede Theorems 5.19 or 5.21. For Theorem 5.21 in particular, note that the bound obtained there is in general much smaller than the bound L found in the proof of Theorem 5.23, which depends on the size of the denominator of $B_{2k+1}(x+1)$. Let us illustrate this result with some examples.

Example 5.24.

$$\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}.$$

Clearly, if $n3+1$ is prime, it does not divide $n^2(n+1)^2$. Thus, it follows that no prime is a 3-representative.

Example 5.25.

$$\sum_{i=1}^{n} i^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}.$$

If $n4+1$ is a 4-representative, then it must divide $(3n^2+3n-1)$. But

$$16(3n^2+3n-1) = (9+12n)(n4+1) - 25,$$

so $n4+1$ must divide 25, so $n=1$, and $p=5$ is the only 4-representative.

Example 5.26.

$$\sum_{i=1}^{n} i^5 = \frac{n^2(n+1)^2(2n+1)(2n^2+2n-1)}{12}.$$

If $n5+1$ is a 5-representative, then it must divide $(2n^2+2n-1)$. But

$$25(2n^2+2n-1) = (10n+8)(n5+1) - 33,$$

so $n5+1$ must divide 33, so $n=2$. Since

$$2^5 = 32 \equiv -1 \not\equiv 1 \pmod{11},$$

it follows that $p=11$ is indeed the only 5-representative.

Example 5.27.

$$\sum_{i=1}^{n} i^6 = \frac{n(n+1)(2n+1)(3n^4+6n^3-3n+1)}{42}.$$

If $n6+1$ is a 6-representative, then it must divide $(3n^4+6n^3-3n+1)$. But

$$432(3n^4+6n^3-3n+1) = (216n^3+396n^2-66n-205)(n6+1)+637,$$

so $n6+1$ must divide $637 = 7^2 \cdot 13$, so $n=1$ or $n=2$. Since

$$2^6 = 64 \equiv -1 \not\equiv 1 \pmod{13},$$

it follows that $p=7$ and $p=13$ are the only 6-representatives.

Example 5.28.

$$\sum_{i=1}^{n} i^7 = \frac{n^2(n+1)^2(3n^4+6n^3-n^2-4n+2)}{24}.$$

If $n7+1$ is a 7-representative, then it must divide $(3n^4+6n^3-n^2-4n+2)$. But

$$2401(3n^4+6n^3-n^2-4n+2) = (1029n^3+1911n^2-616n-1284)(n7+1)+6086,$$

so $n7+1$ must divide $6086 = 2\cdot 17\cdot 179$. However, since none of these are congruent to 1 modulo 7, it follows that there are no 7-representatives.

Example 5.29.

$$\sum_{i=1}^{n} i^8 = \frac{n(n+1)(2n+1)(5n^6+15n^5+5n^4-15n^3-n^2+9n-3)}{90}.$$

If $n8+1$ is a 8-representative, then it must divide $(5n^6+15n^5+5n^4-15n^3-n^2+9n-3)$. But

$$262144(5n^6+15n^5+5n^4-15n^3-n^2+9n-3) =$$
$$(163840n^5+471040n^4+104960n^3-504640n^2+30312n291123)(n8+1)-1077555,$$

so $n8+1$ must divide

$$1077555 = 3\cdot 5\cdot 71837.$$

However, since none of these are congruent to 1 modulo 8, it follows that there are no 8-representatives.

Note that using Theorem 5.21 instead, we only had to consider those primes not exceeding 128.

Example 5.30.

$$\sum_{i=1}^{n} i^9 = \frac{n^2(n+1)^2(n^2+n-1)(2n^4+4n^3-n^2-3n+3)}{20}.$$

If $n9+1$ is a 9-representative, then it must divide (n^2+n-1) or $(2n^4+4n^3-n^2-3n+3)$. But

$$81(n^2 = n-1) = (9n+8)(n9+1) - 89,$$

so $n9+1$ must divide $89 \not\equiv 1 \pmod 9$. Now, since

$$6561(2n^4+4n^3-n^2-3n+3) = (1458n^3+2754n^2-1035n-2072)(n9+1)+21755,$$

$n9+1$ must divide $21755 = 5 \cdot 19 \cdot 229$. So the only possibility is $n = 2$. Since

$$2^9 = 512 \equiv -1 \not\equiv 1 \pmod{19},$$

it follows that $p = 19$ is indeed the only 9-representative.

Example 5.31.

$$\sum_{i=1}^{n} i^{10} = \frac{n(n+1)(2n+1)(n^2+n-1)(3n^6+9n^5+2n^4-11n^3+3n^2+10n-5)}{66}.$$

If $n10+1$ is a 10-representative, then it must divide

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

or

$$(3n^6+9n^5+2n^4-11n^3+3n^2+10n-5).$$

But

$$100(n^2 + n - 1) = (10n + 9)(n10 + 1) - 109,$$

and

$$10^6(3n^6 + 9n^5 + 2n^4 - 11n^3 + 3n^2 + 10n - 5) =$$
$$(3 \cdot 10^5 n^5 + 87 \cdot 10^4 + 113000n^3 - 111300n^2 + 411130n + 958887)(n10 + 1) - 5958887,$$

so $n10 + 1$ must divide 109, or $5958887 = 11^5 \cdot 37$, so $n = 1$. It follows that $p = 11$ is the only 10-representative.

5.3.1 k_n-densities

Definition 5.32. *Let $p = nk + 1$ be a prime that is* not *a strong representative of order n. The k_n*-density*, denoted k_n, is given by*

$$k_n = \left|\{i^i : i \neq j,\ i^k \not\equiv j^k \pmod p), i, j \in \mathbf{n}\}\right|/n.$$

We conclude this section with some remarks on k_n-densities. As illustrated in Appendix A.4, the numbers 3_n stay rather close to 2/3 while the numbers 5_n are very close to 84/125. In [15], Noam D. Elkies discusses the k_n-densities and confirms these observations. We include his argument verbatim:

> [The proof of Theorem 5.23] yields the existence of one coincidence $a^k \equiv b^k$ with $0 < a < b < p/k$; but in fact the number of coincidences is asymptotically proportional to p: the count is $C_k\, p + O_k(p^{1-\epsilon(k)})$, where $C_k = (k-1)/(2k^2)$ or $(k-2)/(2k^2)$ according as k is odd or even, and $\epsilon(k) = 1/\phi(k) \geq 1/(k-1)$. Extending the analysis to triple and higher-order

coincidences also yields the asymptotic proportion of k-th powers that arise in $\{a^k \pmod p) : a < p/k\}$. For example, when k is an odd prime, the proportion of k-th powers that do not have a kth root in $(0, p/k)$ is asymptotic to $((k-1)^k + 1)/k^k$; for $k = 5$ that's 41/125, so the proportion with such a kth root is 84/125, which matches A.Caicedo's observed 0.672 exactly. It also gives $1 - \frac{8+1}{27} = 2/3$ for $k = 3$, matching the proportion of cubes reported by Greg Martin in comments below; as $k \to \infty$ the proportion of k-th powers with small k-th roots approaches $1 - (1/e)$.

Here's how to estimate the number of pairs. Begin with the observation that $a^k = b^k$ iff $b \equiv ma \pmod p$ where m is one of the $k-1$ solutions of $m^k \equiv 1 \pmod p$ other than $m = 1$. If k is even, we exclude also $m = -1$, which is impossible with $0 < a, b < p/k$. Then $b \equiv ma \pmod p$ defines a lattice of index p in $\mathbb{Z}^2$ all of whose nonzero vectors have length $\gg p^{\epsilon(k)}$, because for such a vector p divides the nonzero number $a^k - b^k$, which factors into homogeneous polynomials in a, b each of degree at most $\phi(k)$. [This is where we use $m \neq -1$: if $a = -b$ then $a^k - b^k = 0$.] Thus the solutions of $b \equiv ma \pmod p$ with $a, b \in (0, p/k)$ are the lattice points in a square of area $(p/k)^2$, and their number is estimated by $p^{-1}(p/k)^2 = p/k^2$, with an error bound proportional to (perimeter)/(length of shortest nonzero vector), i.e. proportional to $p^{1-\epsilon(k)}$. The total of $C_k\, p + O_k(p^{1-\epsilon(k)})$ then follows by summing over all $k-1$ or $k-2$ solutions of $m^k = 1 \pmod p$ other than $m = \pm 1$, and dividing by 2 because we've counted each coincidence twice, as (a, b) and (b, a).

Likewise one can estimate the counts of triples etc. One must be careful

> with subsets of the kth roots of unity that have integer dependencies, but at least when k is prime there are no dependencies except that all k of them sum to zero. If I did this right, the result for $j < k$ is that the number of j-element subsets of $\{1, 2, \ldots, (p-1)/k\}$ with the same kth power is asymptotic to $\binom{k}{j} p/k^{j+1}$, while there are no such subsets with $j = k$ because the sum of all k solutions of $a^k \equiv c \pmod{p}$ vanishes. An exercise in generatingfunctionological inclusion-exclusion then produces the formula $((k-1)^k + 1)/k^k$ for the asymptotic proportion of kth powers that have no kth roots at all in $(0, p/k)$.
>
> The same technique also works for $0 < a < b < M$ with M considerably smaller than p/k; and the resulting coincidences, when they exist, can be calculated efficiently using lattice basis reduction (which as it happens I mentioned on this forum [*http://mathoverflow.net/questions/77986*] a few days ago).

5.4 Multiplicative Colorings

As shown in Section 5.2, if $n \leq 5$, then any satisfactory coloring of K_n admits a strong representation. These colorings are very special: Fix some n, and suppose that c is a satisfactory coloring of K_n admitting a strong representation φ associated to the prime $p = nk + 1$. Let $G = \{a^k \pmod{p} \mid a \in \mathbf{n}\}$. Then, as pointed out in Corollary 1.7, $G \leq \mathbb{Z}_p^*$ is a group isomorphic to $\mathbb{Z}_n$. Let $h = \varphi \circ c$, so

$$h : K_n \to G.$$

Since $h(a) = a^k \pmod{p}$ for any $a \in K_n$, the map h satisfies

$$h(ab) = h(a) \cdot h(b)$$

for any $a, b \in K_n$, where ab is the usual product of a and b and $h(a) \cdot h(b)$ is the product in G. Note that the bijection φ coincides with the restriction of h to $\mathbf{n}$.

Definition 5.33. *A satisfactory coloring c of K_n is* multiplicative *iff there exists a group $(G, \cdot)$ of order n and a bijection $\varphi : \mathbf{n} \to G$ such that, letting $h = \varphi \circ c$, we have that*

$$h(ab) = h(a) \cdot h(b)$$

*for any $a, b \in K_n$. In this case, we say that c is a G-*coloring.

Lemma 5.34. *If a satisfactory coloring of K_n is both a G_1-coloring and a G_2-coloring, then $G_1 \cong G_2$.*

Proof. If $\varphi_1 : \mathbf{n} \to G_1$ and $\varphi_2 : \mathbf{n} \to G_2$ witness that c is both a G_1-coloring and a G_2-coloring, then $\varphi_1 \circ \varphi_2^{-1} : G_2 \to G_1$ is an isomorphism. □

Note that if G is as in Definition 5.33, then G is abelian, and consequently we adopt additive notation in what follows, so h is a kind of *discrete logarithm.* Rather than adopting this notation, we also say that h is multiplicative:

Definition 5.35. *If $(G, +)$ is an abelian group and the map $h : K_n \to G$ satisfies that $h(ab) = h(a) + h(b)$ for any $a, b \in K_n$, we say that h is* multiplicative.

Since there are only finitely many groups of any given order, there are only finitely many possibilities for G. In fact, we can easily list all the possibilities, thanks to the classification theorem for finite abelian groups, Theorem 4.3 in [1]:

Theorem 5.36. *Any finite abelian group is isomorphic to a direct sum of the form $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ where each n_i is a power of a prime number.*

Corollary 5.37. *For any n, there are only finitely many multiplicative colorings of K_n.*

Proof. Suppose c is multiplicative as witnessed by $(G,+)$, φ. Let $h = \varphi \circ c$, so $h(ab) = h(a)+h(b)$ for all $a, b \in K_n$. Note that this induces a group structure $\oplus$ on $\mathbf{n}$ isomorphic to G because c is the identity on $\mathbf{n}$, so if $a \in \mathbf{n}$, then $h(a) = \varphi(c(a)) = \varphi(a)$. So we are setting $a \oplus b = d$ for $a, b, d \in \mathbf{n}$, if and only if $\varphi(d) = \varphi(a) + \varphi(b)$. By identifying $(G,+)$ with $(\mathbf{n}, \oplus)$, it follows that we may assume that φ is the identity so $h = c$. But then $(\mathbf{n}, \oplus)$ completely determines c. In effect, if $p_1, \ldots, p_k$ are the primes less than or equal to n, then the multiplicity requirement gives us

$$c(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \alpha_1 c(p_1) \oplus \ldots \oplus \alpha_k c(p_k),$$

where

$$\alpha_i c(p_i) = \underbrace{c(p_i) \oplus \ldots \oplus c(p_i)}_{\alpha_i \text{ times}}.$$

Since there are only finitely many group structures on $\mathbf{n}$, we are done. □

In what follows, given an abelian group $(G, \oplus)$, we will denote α-fold sums of the form

$$\underbrace{g \oplus \cdots \oplus g}_{\alpha \text{ times}}$$

by $g^{\oplus \alpha}$.

Remark 5.38. Note that not every abelian group structure of $\mathbf{n}$ gives rise to a multiplicative coloring. For example, by Theorem 5.10, if $n = 4$, then $\oplus$ is given by $a \oplus b = ab \pmod 5$ and in particular $\oplus$ is isomorphic to $\mathbb{Z}_4$ and not to $\mathbb{Z}_2 \times \mathbb{Z}_2$. We further discuss this in the next chapter.

The case when $G \cong \mathbb{Z}_n$, as in the case of a strong representation, deserves special attention.

Question 5.39. *Does every $\mathbb{Z}_n$-coloring admit a strong representation?*

Perhaps surprisingly, the answer to Question 5.39 is negative, as we show in the next chapter. Nevertheless, we can answer Question 5.39 affirmatively at the cost of replacing strong representations with a weak variant, see Remark 5.46.

Although so far our examples and results have only exhibited multiplicative colorings, it should be pointed out that not every satisfactory coloring is multiplicative. For example, in personal communication, Caicedo has found a non-multiplicative satisfactory coloring of K_6. We state the result without proof.

Theorem 5.40. (Caicedo)
There is a unique satisfactory coloring c of K_6 such that $c(2^3) = 5$, $c(2^4) = 2$, $c(2^5) = 4$, $c(3^2) = 9$, $c(2^6 n) = c(n)$, $c(12n) = c(27n)$, and $c(20n) = c(45n)$ for any $n \in K_6$. This coloring satisfies that $c(3^7 n) = c(3n)$ and $c(5^7 n) = c(5n)$ for any $n \in K_6$.

Note that if c is as in Theorem 5.40, then it is non-multiplicative. For example, if c is multiplicative, then $c(18) = c(9 \times 2) = c(9) + c(2) = c(2) + c(2) = c(2 \times 2) = c(4) = 4$. Instead, $c(18) = 5$.

Similarly, not every multiplicative coloring is a $\mathbb{Z}_n$-coloring. Examples are presented in the next chapter. Non-multiplicative colorings seem more difficult to analyze, and we do not understand them well. For example, the coloring c from Theorem 5.40 is *periodic*, in the sense that $c(p^7 n) = c(pn)$ for $p = 2, 3, 5$ and $n \in K_6$; we do not know whether there are non-periodic non-multiplicative colorings as well. In what follows, we restrict our attention to the multiplicative case.

5.5 Partial G-Homomorphisms

The following extends a notion due independently to Caicedo and Ewan Delanoy, see [2], where only the case $G = \mathbb{Z}_n$ was considered. Though not identical, it is closely related to the concept of *Freiman homomorphism* in additive combinatorics, see [5].

Definition 5.41. *Let $(G, +)$ be an abelian group of order n. A map $h : \mathbf{n} \to G$ is a* partial G-homomorphism *if and only if h is a bijection and, whenever $a, b \in \mathbf{n}$, if $ab \leq n$, then $h(ab) = h(a) + h(b)$. If $G = \mathbb{Z}_n$, we simply call h a partial homomorphism.*

Remark 5.42. We require G to be abelian as our goal is to relate partial G-homomorphisms to satisfactory colorings, cf. Theorem 5.43 below, and the natural argument, requires that G is abelian. But the question of whether there are partial G-homomorphisms where G is not abelian is interesting in its own right. This seems to be open in general, but for n odd the answer is negative, as shown by K.A. Chandler, see [24].

Since h is a bijection, it induces a group operation $\oplus$ on $\mathbf{n}$ such that $(\mathbf{n}, \oplus) \cong (G, +)$ and $\oplus$ extends the partial graph of multiplication on $\mathbf{n}$. Our use of the phrase homomorphism here is based on the following observation: For any partial G-homomorphism h, we have that $h(1) = h(1 \cdot 1) = h(1) + h(1) = h(1)^{\oplus 2}$. It follows that $h(1) = 0_G$. In other words, h maps the multiplicative identity in $\mathbf{n}$ to the additive identity in G, and embeds a multiplicative structure into an additive one.

Theorem 5.43. *If $h : \mathbf{n} \to G$ is a partial G-homomorphism, then h can be uniquely extended to a multiplicative map $\hat{h} : K_n \to G$. Moreover, $h^{-1} \circ \hat{h} : K_n \to \mathbf{n}$ is a G-coloring of K_n.*

Proof. Let $h : \mathbf{n} \to G$ be a partial G-homomorphism. Let $p_1, \dots, p_s$ be the primes less than or equal to n. Then, $\hat{h} : K_n \to G$ extends h and is multiplicative iff for any $a_1, \dots, a_s \in \mathbb{N}$, we have

$$\hat{h}(p_1^{a_1} \dots p_s^{a_s}) = \bigoplus_i h(p_i)^{\oplus_i a_i}.$$

This proves the existence and uniqueness of the extension $\hat{h}$. Moreover, if $1 \leq i < j \leq n$ and $a \in K_n$, then

$$\hat{h}(ia) = \hat{h}(i) + \hat{h}(a) \neq \hat{h}(j) + \hat{h}(a) = \hat{h}(ja)$$

because $\hat{h} \restriction_{\mathbf{n}} = h$ is a bijection.

But then, letting $c = h^{-1} \circ \hat{h}$, we have that $c : K_n \to \mathbf{n}$ is a G-coloring.

□

Remark 5.44. Note the similarity between this argument and the proof of Corollary 5.37.

Obviously, if $\hat{h} : K_n \to G$ is multiplicative and $h = \hat{h} \restriction_{\mathbf{n}}$ is a bijection, then h is a partial G-homomorphism. Therefore, if $c : K_n \to \mathbf{n}$ is a G-coloring as witnessed by the bijection $\varphi : \mathbf{n} \to G$, then φ is a partial G-homomorphism as, by definition, $h = \varphi \circ c$ is multiplicative, and $\varphi = h \restriction_{\mathbf{n}}$.

This shows that the problem of building G-colorings of K_n is equivalent to the problem of building partial G-homomorphisms or, equivalently, G-satisfactory groups:

Definition 5.45. *Given an abelian group $(G, +)$ of order n, we say that an abelian group structure on $\mathbf{n}$, $(\mathbf{n}, \oplus)$, is a G-*satisfactory group *iff $(\mathbf{n}, \oplus) \cong (G, +)$ and $a \oplus b = ab$ whenever $a, b, ab \in \mathbf{n}$.*

We say that the G-coloring resulting from extending $\oplus$ as in Theorem 5.43 is associated *to $(\mathbf{n}, \oplus)$.*

There is a two-fold advantage on building G-satisfactory groups rather than partial G-homomorphisms: First, the extension to a G-coloring is immediate. Second, and more significantly, different partial G-homomorphisms may give rise to the same G-coloring, as the notion is only uniquely determined up to automorphisms of G.

For example, if $h_1 : \mathbf{6} \to \mathbb{Z}_6$ and $h_2 : \mathbf{6} \to \mathbb{Z}_6$ are the maps

$$\begin{array}{llllll} h_1(1) = 0, & h_1(2) = 2, & h_1(3) = 1, & h_1(4) = 4, & h_1(5) = 5, & h_1(6) = 3, \\ h_2(1) = 0, & h_2(2) = 4, & h_2(3) = 5, & h_2(4) = 2, & h_2(5) = 1, & h_2(6) = 3 \end{array}$$

then both give rise to the $\mathbb{Z}_6$-coloring strongly represented by $7 = 6 \cdot 1 + 1$ (this is explained in more detail in Subsection 5.5.1 with a different example), and this coloring is associated to the G-satisfactory group shown below:

⊕	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Table 5.3: A $\mathbb{Z}_6$-satisfactory group.

In the next chapter, we use systematically the notation of G-satisfactory groups to identify all multiplicative colorings with at most 8 elements.

Remark 5.46. We are now in a position to explain how $\mathbb{Z}_n$-colorings or, equivalently, partial homomorphisms are closely related to strong representations. In fact, we can prove that any $\mathbb{Z}_n$-coloring admits a "weak" representation.

Let $h : \mathbf{n} \to \mathbb{Z}_n$ be a partial homomorphism. As before, let $p_1, \ldots, p_s$ be the primes less than or equal to n. Extend h to a map from K_n to $\mathbb{Z}_n$ as in the proof of Theorem 5.43. Denote the extension again by h.

By Dirichlet's theorem, there are primes P of the form $nk+1$. For any such P, let g be a primitive root modulo P, i.e., a generator of $\mathbb{Z}_P^*$. In other words, the powers g^{ki} are precisely the kth power residues modulo P. Invoking again Dirichlet's theorem, for each p_i, we can find a prime q_i such that $q_i \equiv g^{h(p_i)} \pmod{P}$. Now for $x \in K_n$ define $d : K_n \to \mathbb{Z}_P^*$ by $d(x) = g^{kh(x)}$.

Suppose $x = \prod_{i=1}^{s} p_i^{a_i}$. Then, $h(x) = \sum_i a_i h(p_i)$ and

$$d(x) = \prod_i (g^{h(p_i)})^{ka_i} = \left(\prod_i q_i^{a_i}\right)^k \tag{5.1}$$

where of course the products are computed modulo P.

The point is that if $i, j \in \mathbf{n}$, then $d(i) \neq d(j)$ because $h(i) \neq h(j)$, h being a bijection. Say $0 \leq h(i) < h(j) < n$, then $0 \leq kh(i) < kh(j) < kn$, and $g^{kh(i)} \neq g^{kh(j)}$, since g is a primitive root. It follows that $d(ix) = d(i)d(x) \neq d(j)d(x) = d(jx)$ and, after precomposing with an appropriate permutation, d becomes a $\mathbb{Z}_n$-coloring.

Note how close the coloring given by Equation 5.1 is to the colorings described in Definition 5.2. Strong representations are the particular case where we can choose P for which we can take $q_i = p_i$ for all i.

Partial homomorphisms are easy to construct "by hand." For instance, it is a matter of at most a couple of hours to construct partial homomorphisms for all $n \leq 32$, essentially by what amounts to following a greedy algorithm. Examples of partial homomorphisms for all $n \leq 54$ are shown in Appendix B.[3]

Given n, define M and M_{K_n} as the sets of multiplicative colorings of $\mathbb{Z}^+$ and of K_n, respectively. In Corollary 5.37, we showed that M_{K_n} is finite. We now show that

[3] See Section 7.2.

restricting attention to colorings in M does not affect the computation of the number of satisfactory colorings, Corollary 4.7.

Theorem 5.47. *If $n > 1$ and $M_K \neq \varnothing$, then $|M| = |\mathbb{R}|$.*

Proof. As in Corollary 4.7, it is enough to show that $n^{|\mathbb{N}|} \leq |M|$. Let $c : K_n \to \mathbf{n}$ be a multiplicative coloring associated to the G-satisfactory group $(\mathbf{n}, \oplus)$. To each prime p assign a number $a_p \in \mathbf{n}$ with the only restriction that $a_p = p$ if $p \in \mathbf{n}$. Now define $c' : \mathbb{Z}^+ \to \mathbf{n}$ as follows: If $m \in \mathbb{Z}^+$, let $\prod_i p_i^{b_i}$ be its prime factorization, and set

$$c'(m) = \bigoplus_i a_{p_i}^{\oplus b_i}.$$

It is immediate that any c' defined this way is multiplicative and extends c, and that different sequences $(a_p \mid p \text{ prime})$ give rise to different c'. But then we have associated $n^{|\mathbb{N}|}$ colorings in M to each $c \in M_K$, so $n^{|\mathbb{N}|} \leq |M|$. □

5.5.1 An Example

Here we illustrate how to construct a satisfactory coloring of K_5 by making use of a partial homomorphism. To do so, we will again make use of the table described in Chapter 4, but limited to columns in K_5. However, in this case we will not view the choices for first column as completely arbitrary. Instead, the first column will be formed by creating a partial homomorphism.

Thus, we begin by forming a partial homomorphism $h : \mathbf{5} \to \mathbb{Z}_5$. As we stated above, $h(1) = 0$. Next, we will choose $h(2) = 1$. By choosing $h(2) = 1$, since $h(4) = h(2 \cdot 2) = h(2) + h(2)$, we must define $h(4) = 1 + 1 = 2$. This leaves us to define $h(3)$ and $h(5)$. Since $3 \cdot 2 = 6 > 5 = n$ and $5 \cdot 2 = 10 > 5 = n$, we are free to choose any of the remaining values as the image of 3 and 5. For simplicity, we will choose $h(3) = 3$

and $h(5) = 4$. Now, we have the following initial table: Next we will complete each column in the following manner. For the ith column, we define the coloring as

1	0	2	1	3	3	4	2	5	4	6		8		9	
2	1	4	2	6		8		10		12		16		18	
3	3	6		9		12		15		18		24		27	
4	2	8		12		16		20		24		32		36	
5	4	10		15		20		25		30		40		45	

$$h(2i) = 1 + h(i)$$

$$h(3i) = 3 + h(i)$$

$$h(4i) = 2 + h(i)$$

$$h(5i) = 4 + h(i)$$

Inductively, this completely determines the table:

1	0	2	1	3	3	4	2	5	4	6	4	8	3	9	1
2	1	4	2	6	4	8	3	10	0	12	0	16	4	18	2
3	3	6	4	9	1	12	0	15	2	18	2	24	1	27	4
4	2	8	3	12	0	16	4	20	1	24	1	32	0	36	3
5	4	10	0	15	2	20	1	25	3	30	3	40	2	45	0

Looking at the table, we obtain verification that $c(6) = c(5)$. In fact, the coloring we have created is just a relabeling of the coloring c_5.

CHAPTER 6

MULTIPLICATIVE COLORINGS WITH AT MOST 8 COLORS

6.1 Six Colors

In this chapter, we build all G-satisfactory groups for $6 \leq |G| \leq 8$, thus determining all multiplicative colorings with at most 8 colors. See Section 5.5 for details on how a G-satisfactory group $(\mathbf{n}, \oplus)$ uniquely determines a G-coloring of K_n.

Note that the only abelian group of order 6 is $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ by Theorem 5.36, so all the groups $(\mathbf{6}, \oplus)$ we build here are $\mathbb{Z}_6$-satisfactory.

In the task of constructing the group operations $\oplus$ (extending the graph of multiplication on $\mathbf{6}$), the following immediate fact proves useful:

Fact 6.1. *If $(\mathbf{n}, \oplus)$ is G-satisfactory for some G, then $\{2 \oplus a \mid a \in \mathbf{n}, 2a > n\}$ coincides with the set of odd integers in $\mathbf{n}$.*

Before we do anything, note the following *base operation table* for $n = 6$ (Table 6.1) is already determined, and our task is to fill out its blank spots.

It is also useful to keep in mind the following observations:

a. $\oplus$ must be associative and commutative.

$\oplus$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6			
3	3	6				
4	4					
5	5					
6	6					

Table 6.1: The base operation table for $n = 6$.

b. Each column and each row on the table must be a permutation of $\mathbf{n}$.

c. (Lagrange's theorem) The *order* in $(\mathbf{n}, \oplus)$ of any element a must divide n.

As the readers may verify by themselves, completing Table 6.1 is not unlike solving an easy Sudoku puzzle. Start by noting from Fact 6.1, that 1 must be one of $2 \oplus 4$, $2 \oplus 5$, or $2 \oplus 6$.

1. Suppose first that $2 \oplus 4 = 1$. Then, $4 \oplus 4 = 2$. By observation b, $2 \oplus 5 = 3$, so $4 \oplus 5 = 6$, $2 \oplus 6 = 5$, $4 \oplus 6 = 3$, and $4 \oplus 3 = 5$. At this point, our table is given by:

$\oplus$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6		5		
4	4	1	5	2	6	3
5	5	3		6		
6	6	5		3		

We are left with 3 possibilities for $3 \oplus 3$.

(a) If $3 \oplus 3 = 1$, then $3 \oplus 6 = 2$ and, by observations a and b, these choices completely determine $\oplus$. It is easy to see that $(\mathbf{6}, \oplus)$ is indeed an abelian group. In fact, its associated coloring is strongly representable. Recall from

Chapter 5 that if $p = nk + 1$ is prime and $1^k, \ldots, n^k$ are distinct modulo p, the $\mathbb{Z}_n$-coloring $c : K_n \to \mathbf{n}$ strongly represented by p is given by $c(i) = i$ for $i \in \mathbf{n}$, and $c(a) = c(b)$ iff $a^k \equiv b^k \pmod{p}$.

$\oplus$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	1	5	4	2
4	4	1	5	2	6	3
5	5	3	4	6	2	1
6	6	5	2	3	1	4

Table 6.2: The associated $\mathbb{Z}_6$-coloring is strongly represented by $103 = 6 \cdot 17 + 1$.

(b) If $3 \oplus 3 = 2$, the operation $\oplus$ is again completely determined:

$\oplus$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Table 6.3: The associated $\mathbb{Z}_6$-coloring is strongly represented by $7 = 6 \cdot 1 + 1$.

(c) Finally, if $3 \oplus 3 = 4$, we obtain the group from Table 6.4:

2. If $2 \oplus 5 = 1$, then $4 \oplus 5 = 2$. By observations a and b, this completely determines $\oplus$, see Table 6.5:

3. Finally, if $2 \oplus 6 = 1$, we obtain the group from Table 6.6:

$\oplus$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	4	5	2	1
4	4	1	5	2	6	3
5	5	3	2	6	1	4
6	6	5	1	3	4	2

Table 6.4: The associated $\mathbb{Z}_6$-coloring is strongly represented by $487 = 6 \cdot 81 + 1$.

$\oplus$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	3	1	5
3	3	6	1	5	4	2
4	4	3	5	6	2	1
5	5	1	4	2	6	3
6	6	5	2	1	3	4

Table 6.5: The associated $\mathbb{Z}_6$-coloring is strongly represented by $547 = 6 \cdot 91 + 1$.

6.2 Seven Colors

The only abelian group of order 7 is $\mathbb{Z}_7$, so all groups we build here are $\mathbb{Z}_7$-satisfactory. The base operation table for $n = 7$ is shown in Table 6.7.

Note that $2 \oplus 4 \neq 1$ by observation c, as 1 is the identity of $(\mathbf{7}, \oplus)$ and every member of $\mathbb{Z}_7$ other than 0 has order 7. Also, $2 \oplus 6 = 4 \oplus 3 \neq 3$. By observation b, $2 \oplus a \neq a$ for $a = 5, 7$. Hence, the sequence $(2 \oplus a \mid 4 \leq a \leq 7)$ is a permutation of the numbers 1,3,5,7 that does not begin with 1, does not have 5 as its second element, does not have 3 as its third element, and does not end with 7.

This means it must be one of the following sequences: $(3,1,7,5)$, $(3,7,1,5)$, $(3,7,5,1)$, $(5,1,7,3)$, $(5,3,7,1)$, $(5,7,1,3)$, $(7,1,5,3)$, $(7,3,1,5)$, or $(7,3,5,1)$.

However, $(3,7,1,5)$, $(5,1,7,3)$, and $(7,3,5,1)$ are not possible.

$\oplus$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	5	3	1
3	3	6	4	1	2	5
4	4	5	1	3	6	2
5	5	3	2	6	1	4
6	6	1	5	2	4	3

Table 6.6: The associated $\mathbb{Z}_6$-coloring is strongly represented by $13 = 6 \cdot 2 + 1$.

$\oplus$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6				
3	3	6					
4	4						
5	5						
6	6						
7	7						

Table 6.7: Base operation table for $n = 7$.

a. Consider $(3, 7, 1, 5)$: if $4 \oplus 2 = 3$ and $6 \oplus 2 = 1$, then $4 \oplus 4 = 6$ and $6 \oplus 2 = 2^{\oplus 5}$, so 2 would have order 5.

b. Consider $(5, 1, 7, 3)$: If $4 \oplus 2 = 5$ and $5 \oplus 2 = 1$, then $2^{\oplus 4} = 1$.

c. Finally, consider $(7, 3, 5, 1)$: if $4 \oplus 2 = 7$ and $7 \oplus 2 = 1$, then again $2^{\oplus 4} = 1$.

Each of the remaining 6 sequences uniquely determines $\oplus$ as listed below. This was to be expected; after all, the column for $2 \oplus a$ in particular determines the subgroup generated by 2, which is $(\mathbf{7}, \oplus)$, as this group is isomorphic to $\mathbb{Z}_7$, that has no non-trivial subgroups.

1. $(3, 1, 7, 5)$: see Table 6.8.

$\oplus$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	3	1	7	5
3	3	6	5	7	4	1	2
4	4	3	7	6	2	5	1
5	5	1	4	2	7	3	6
6	6	7	1	5	3	2	4
7	7	5	2	1	6	4	3

Table 6.8: The associated $\mathbb{Z}_7$-coloring is strongly represented by $2087 = 7 \cdot 298 + 1$.

2. $(3, 7, 5, 1)$: see Table 6.9.

$\oplus$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	3	7	5	1
3	3	6	7	5	2	1	4
4	4	3	5	6	1	7	2
5	5	7	2	1	3	4	6
6	6	5	1	7	4	2	3
7	7	1	4	2	6	3	5

Table 6.9: The associated $\mathbb{Z}_7$-coloring is strongly represented by $1429 = 7 \cdot 204 + 1$.

3. $(5, 3, 7, 1)$: see Table 6.10.

4. $(5, 7, 1, 3)$: see Table 6.11.

5. $(7, 1, 5, 3)$: see Table 6.12.

6. $(7, 3, 1, 5)$: see Table 6.13.

$\oplus$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	5	3	7	1
3	3	6	2	7	1	4	5
4	4	5	7	3	6	1	2
5	5	3	1	6	7	2	4
6	6	7	4	1	2	5	3
7	7	1	5	2	4	3	6

Table 6.10: The associated $\mathbb{Z}_7$-coloring is strongly represented by $659 = 7 \cdot 94 + 1$.

$\oplus$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	5	7	1	3
3	3	6	5	1	2	7	4
4	4	5	1	7	3	2	6
5	5	7	2	3	6	4	1
6	6	1	7	2	4	3	5
7	7	3	4	6	1	5	2

Table 6.11: The associated $\mathbb{Z}_7$-coloring is strongly represented by $21911 = 7 \cdot 3130 + 1$.

6.3 Eight Colors

There are three abelian groups of order 8, namely $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. The base operation table for $n = 8$ is given by Table 6.14.

Since $2 \oplus 2 = 4 \neq 1$, the number 2 does not have order 2, and it follows that there are no $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$-satisfactory groups (and the same simple argument rules out several other possible groups for larger values of n). We will see that the other two cases do occur.

As before, we consider the sequence $(2 \oplus a \mid 5 \leq a \leq 8)$, noting that it must be a permutation of the numbers $1, 3, 5, 7$ that does not begin with 5 and does

$\oplus$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	7	1	5	3
3	3	6	2	5	7	4	1
4	4	7	5	3	2	1	6
5	5	1	7	2	6	3	4
6	6	5	4	1	3	7	2
7	7	3	1	6	4	2	5

Table 6.12: The associated $\mathbb{Z}_7$-coloring is strongly represented by $3557 = 7 \cdot 508 + 1$.

$\oplus$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	7	3	1	5
3	3	6	7	1	4	5	2
4	4	7	1	5	6	2	3
5	5	3	4	6	2	7	1
6	6	1	5	2	7	3	4
7	7	5	2	3	1	4	6

Table 6.13: The associated $\mathbb{Z}_7$-coloring is strongly represented by $17431 = 7 \cdot 2490 + 1$.

not have 7 as a third element. Moreover, 3 cannot be the second element, or $2 \oplus 6 = 3$, but then $3 \oplus 4 = 3$ and $4 = 1$. This means that the sequence must be one of the following: $(1,5,3,7)$, $(1,7,3,5)$, $(1,7,5,3)$, $(3,1,5,7)$, $(3,5,1,7)$, $(3,7,1,5)$, $(3,7,5,1)$, $(7,1,3,5)$, $(7,1,5,3)$, $(7,5,1,3)$, or $(7,5,3,1)$.

However, $(1,7,3,5)$, $(3,5,1,7)$, and $(7,1,5,3)$ are not possible:

a. Consider $(1,7,3,5)$: If $2 \oplus 6 = 7$ and $2 \oplus 7 = 3$, then $3 \oplus 8 = 6 \oplus 4 = 3$, or $8 = 1$.

b. Consider $(3,5,1,7)$: If $2 \oplus 5 = 3$ and $2 \oplus 6 = 5$, then again $3 \oplus 8 = 6 \oplus 4 = 3$.

c. Consider $(7,1,5,3)$: If $2 \oplus 6 = 1$ and $2 \oplus 8 = 3 = 4 \oplus 4$, then $4^{\oplus 3} = 3 \oplus 4 = 1$, against Lagrange's theorem.

$\oplus$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	8				
3	3	6						
4	4	8						
5	5							
6	6							
7	7							
8	8							

Table 6.14: The base operation table for $n = 8$.

Of the remaining 8 sequences, 6 of them determine $\oplus$ uniquely as shown below. In all cases, the resulting group is $\mathbb{Z}_8$-satisfactory and 2 is a generator. As we will see below, none of associated colorings is strongly representable, which solves Question 5.39 negatively.

1. $(1,5,3,7):$ see Table 6.15.

2. $(1,7,5,3):$ see Table 6.16.

3. $(3,1,5,7):$ see Table 6.17.

4. $(3,7,1,5):$ see Table 6.18.

5. $(7,1,3,5):$ see Table 6.19.

6. $(7,5,1,3):$ see Table 6.20.

The remaining two sequences do not contain sufficient information to determine $\oplus$, but we can partially fill out the base operation table as follows:

1. $(3,7,5,1)$: see Table 6.21.

2. $(7,5,3,1)$: see Table 6.22.

$\oplus$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	8	1	5	3	7
3	3	6	4	5	7	8	2	1
4	4	8	5	7	2	1	6	3
5	5	1	7	2	6	3	8	4
6	6	5	8	1	3	7	4	2
7	7	3	2	6	8	4	1	5
8	8	7	1	3	4	2	5	6

Table 6.15: $\mathbb{Z}_8$-coloring corresponding to the sequence $(1, 5, 3, 7)$.

$\oplus$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	8	1	7	5	3
3	3	6	1	7	8	2	4	5
4	4	8	7	3	2	5	1	6
5	5	1	8	2	7	3	6	4
6	6	7	2	5	3	4	8	1
7	7	5	4	1	6	8	3	2
8	8	3	5	6	4	1	2	7

Table 6.16: $\mathbb{Z}_8$-coloring corresponding to the sequence $(1, 7, 5, 3)$.

$\oplus$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	8	3	1	5	7
3	3	6	7	1	8	5	4	2
4	4	8	1	7	6	2	3	5
5	5	3	8	6	4	7	2	1
6	6	1	5	2	7	3	8	4
7	7	5	4	3	2	8	1	6
8	8	7	2	5	1	4	6	3

Table 6.17: $\mathbb{Z}_8$-coloring corresponding to the sequence $(3, 1, 5, 7)$.

$\oplus$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	8	3	7	1	5
3	3	6	4	7	2	8	5	1
4	4	8	7	5	6	1	2	3
5	5	3	2	6	1	4	8	7
6	6	7	8	1	4	5	3	2
7	7	1	5	2	8	3	6	4
8	8	5	1	3	7	2	4	6

Table 6.18: $\mathbb{Z}_8$-coloring corresponding to the sequence $(3, 7, 1, 5)$.

$\oplus$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	8	7	1	3	5
3	3	6	5	1	4	7	8	2
4	4	8	1	5	3	2	6	7
5	5	7	4	3	1	8	2	6
6	6	1	7	2	8	3	5	4
7	7	3	8	6	2	5	4	1
8	8	5	2	7	6	4	1	3

Table 6.19: $\mathbb{Z}_8$-coloring corresponding to the sequence $(7, 1, 3, 5)$.

$\oplus$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	8	7	5	1	3
3	3	6	1	5	4	2	8	7
4	4	8	5	3	1	7	2	6
5	5	7	4	1	3	8	6	2
6	6	5	2	7	8	4	3	1
7	7	1	8	2	6	3	5	4
8	8	3	7	6	2	1	4	5

Table 6.20: $\mathbb{Z}_8$-coloring corresponding to the sequence $(7, 5, 1, 3)$.

$\oplus$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	8	3	7	5	1
3	3	6		7				5
4	4	8	7	1	6	5	3	2
5	5	3		6				7
6	6	7		5				3
7	7	5		3				6
8	8	1	5	2	7	3	6	4

Table 6.21: Partial group operation corresponding to the sequence $(3,7,5,1)$.

$\oplus$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	8	7	5	3	1
3	3	6		5				7
4	4	8	5	1	3	7	6	2
5	5	7		3				6
6	6	5		7				3
7	7	3		6				5
8	8	1	7	2	6	3	5	4

Table 6.22: Partial group operation corresponding to the sequence $(7,5,3,1)$.

Note that in both cases we have $2^{\oplus 4} = 1$. We conclude by observing that the value of $3 \oplus 3 = a$ completely determines the tables, and any of the 4 options for a (namely, 1, 2, 4, or 8) is possible, see Tables 6.23 and 6.24.

In both cases, we obtain $\mathbb{Z}_8$-satisfactory groups iff $a = 2$ or 8. The associated colorings admit strong representatives, as follows: For the sequence $(3,7,5,1)$, if $a = 2$, take $5417 = 8 \cdot 677 + 1$, and if $a = 8$, take $117017 = 8 \cdot 14627 + 1$. For the sequence $(7,5,3,1)$, if $a = 2$, take $3617 = 8 \cdot 452 + 1$, and if $a = 8$, take $17 = 8 \cdot 2 + 1$.

If instead we let $a = 1$ or 4, we obtain $\mathbb{Z}_2 \times \mathbb{Z}_4$-satisfactory groups. If $a = 1$, in both cases, the unique group homomorphism that maps 2 to $(0,1)$ and 3 to $(1,0)$ is an

$\oplus$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	8	3	7	5	1
3	3	6	a	7	$8 \oplus a$	$2 \oplus a$	$4 \oplus a$	5
4	4	8	7	1	6	5	3	2
5	5	3	$8 \oplus a$	6	$4 \oplus a$	a	$2 \oplus a$	7
6	6	7	$2 \oplus a$	5	a	$4 \oplus a$	$8 \oplus a$	3
7	7	5	$4 \oplus a$	3	$2 \oplus a$	$8 \oplus a$	a	6
8	8	1	5	2	7	3	6	4

Table 6.23: Group corresponding to the sequence $(3, 7, 5, 1) : a = 1$, 2, 4, or 8.

$\oplus$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	8	7	5	3	1
3	3	6	a	5	$4 \oplus a$	$2 \oplus a$	$8 \oplus a$	7
4	4	8	5	1	3	7	6	2
5	5	7	$4 \oplus a$	3	a	$8 \oplus a$	$2 \oplus a$	6
6	6	5	$2 \oplus a$	7	$8 \oplus a$	$4 \oplus a$	a	3
7	7	3	$8 \oplus a$	6	$2 \oplus a$	a	$4 \oplus a$	5
8	8	1	7	2	6	3	5	4

Table 6.24: Group corresponding to the sequence $(7, 5, 3, 1) : a = 1$, 2, 4, or 8.

isomorphism between $(\mathbf{8}, \oplus)$ and $\mathbb{Z}_2 \times \mathbb{Z}_4$. If $a = 4$ and the sequence is $(3, 7, 5, 1)$, the corresponding isomorphism is obtained by considering the homomorphism that maps 2 to $(0, 1)$ and 5 to $(1, 0)$. If $a = 4$ and the sequence is $(7, 5, 3, 1)$, consider instead the homomorphism that maps 2 to $(0, 1)$ and 7 to $(1, 0)$.

Finally, we argue that the colorings associated with the first six $\mathbb{Z}_8$-satisfactory groups we listed are not strongly representable. For this, simply note that if they were, any strong representative must be of the form $p = 8k + 1$, so (by Theorem 1.10)

$$2^{4k} \equiv 1 \pmod{p}.$$

But $2^{4k} = (2^4)^k$, so the corresponding coloring c must satisfy $c(2 \oplus 8) = c(2^4) = 1 = c(1)$, that is, we must have $2 \oplus 8 = 1$. For a high–level explanation of why some of these $\mathbb{Z}_8$-colorings are strongly representable while others are not, see Theorem 7.18.

CHAPTER 7

FINAL REMARKS

7.1 A Conjecture of R.L. Graham

Theorem 7.1. (Balasubramanian–Soundararajan, 1996)
Let $n \geq 1$, and $0 < a_1 < a_2 < \ldots < a_n$ be integers. Then $\max_{i,j}\left\{\dfrac{a_i}{(a_i, a_j)}\right\} \geq n$.

Theorem 7.1 originated as a conjecture of R.L. Graham of 1970, see [**?**]. An affirmative answer was published in 1996 by Balasubramanian and Soundararajan, see [7]. Interestingly an affirmative answer to the question of whether there are satisfactory colorings for all n implies Theorem 7.1.

Theorem 7.2. *Conjecture 5.5 implies Theorem 7.1. In fact, if there are satisfactory colorings with $m-1$ colors, then Theorem 7.1 holds for $n = m$.*

Proof. Suppose that there exists some m and a set $B = \{b_1, \ldots, b_m\}$ with $0 < b_1 < \ldots < b_m$ such that $\max_{i,j}\left\{\dfrac{b_i}{(b_i, b_j)}\right\} < m$. Suppose $i \neq j$ and let $M = (b_i, b_j)$. Let $\frac{b_i}{M} = a_i$ and $\frac{b_j}{M} = a_j$. By our hypothesis, we have that $a_i < m$, $a_j < m$, and $a_i \neq a_j$. Since $b_i = a_i M$, $b_j = a_j M$, in any satisfactory coloring with at least $m-1$ colors, we must have that b_i is colored differently than b_j. But $|B| = m$ so we need, at least, m colors. □

The proof of Theorem 7.1 in [7] requires careful analytic estimates of average values of number theoretic functions associated with the distribution of primes. This may say something about the inherent difficulty of Conjecture 5.5. Using purely elementary arguments, Vélez [8] established a particular case of Theorem 7.1. We present the argument in hope that a suitable adaptation may establish Conjecture 5.5 for n colors, when $n = p$ is a prime.

The remainder of the section follows [8] closely.

Theorem 7.3. (Vélez, 1977) [8]
Theorem 7.1 is true for $n = p + 1$, with p prime.

Before proving this theorem, we begin with some remarks and preliminary results.

1. If we multiply a sequence by a constant, we obtain the same set of ratios, so we may assume $(a_1, a_2, \ldots, a_n) = 1$.

2. Given a sequence $Q = \{a_1 < a_2 < \cdots < a_n\}$, let $A = \operatorname{lcm}(a_1, a_2, \ldots, a_n)$ and form

$$Q^{-1} = \left\{ \frac{A}{a_n} < \frac{A}{a_{n-1}} < \cdots < \frac{A}{a_1} \right\}.$$

   It is easily seen that Q and Q^{-1} yield the same set of ratios.

Define $M_n = \operatorname{lcm}(1, 2, \ldots, n)$ and $b_i^{(n)} = \frac{M_n}{n-i+1}$, so $\frac{M_n}{n} < \frac{M_n}{n-1} < \cdots < \frac{M_n}{2} < \frac{M_n}{1}$ is the *pseudo-inverse* of $\mathbf{n}$. We are now ready to begin the proof.

Definition 7.4. *Given a sequence $a_1 < a_2 < \ldots < a_n$, call it a* standard sequence *if it is a multiple of $\mathbf{n}$ or of $\{b_1^{(n)} < b_2^{(n)} < \ldots < b_n^{(n)}\}$. That is, either*

$$a_i = ki \quad \textit{for all } i,$$

or

$$a_i = kb_i^{(n)} \quad \textit{for all } i.$$

In fact, Balasubramanian–Soundararajan [7] established a strong form of Graham's conjecture, where they determine the circumstances under which equality holds:

Theorem 7.5. (Balasubramanian–Soundararajan, 1996) [7]
Assume $(a_1, a_2, \ldots, a_n) = 1$ *and* $\max_{i,j}\left\{\frac{a_i}{(a_i, a_j)}\right\} = n$. *Then, the sequence is a standard sequence except for* $n = 4$, *where we have the additional sequence* $\{2, 3, 4, 6\}$.

Following Vélez [8], we prove in Theorem 7.7 that Theorem 7.5 is indeed a strengthening of Theorem 7.1. We now begin the argument towards Theorem 7.3. We do not assume either Theorem 7.1 or 7.5.

Theorem 7.6. *Let* $q = \{a_1 < a_2 < \ldots < a_n\}$ *be a standard sequence and* b *be any integer such that* $b \neq a_i$ *for any* i *and* $(a_1, a_2, \ldots, a_n, b) = 1$. *Form the new sequence* $Q' = \{a_1 < a_2 < \ldots < a_n, b\}$ *(where* b *is inserted in the appropriate place). Then, if* Q' *is not a standard sequence, we have*

$$\max_{i,j}\left\{\frac{a_i}{(a_i, a_j)}, \frac{b}{(a_i, b)}, \frac{a_i}{(a_i, b)}\right\} > n + 1,$$

except possibly when $n = 4$.

Proof. Note that $(a_1, a_2, \ldots, a_n, b) = 1$ is not a restriction. To see this, assume $a_i = k'b_i^{(n)}$. Let $a = \operatorname{lcm}(a_1, a_2, \ldots, a_n, b)$ and form the new sequence

$$\left\{\frac{a}{a_n} < \frac{a}{a_{n-1}} < \ldots < \frac{a}{a_1}, \frac{a}{b}\right\}.$$

Hence, we have the new sequence

$$Q' = \{k < 2k < \ldots < nk, b'\} \text{ with } (b', k) = 1.$$

We will prove the theorem for this sequence.

Assume Q' is not a standard sequence. If $k = 1$, then $b' \neq n+1$, since Q' is not a standard sequence. Hence, $b' > n+1$, but then $\frac{b'}{(k,b')} = b' > n+1$. Hence, we may assume that $k > 1$. If $b' > n+1$, then $\frac{b'}{(k,b')} = b' > n+1$. If $b' = n+1$, then $\frac{kn}{(kn,b')} = kn > n+1$. If $b' = n$, then $\frac{k(n-1)}{(k(n-1),b')} = k(n-1) > n+1$ for $k > 2$ or $n > 3$. If $k = 2$ and $n = 3$, then $2(3-1) = 3+1$ and this gives the sequence $\{2 < 4 < 6, b' = 3\}$. If $b' = n-1$, then $\frac{kn}{(b',kn)} = kn > n = 1$. Hence, we may assume that $b' < n-1$, so $b'+1 < n$ and $k(b'+1)$ appears somewhere in the sequence Q' and

$$\frac{k(b'+1)}{(k(b'+1),b')} = k(b'+1).$$

If $k(b'+1) > n+1$, then we are done. If not, then $kb'+1 < kb'+k \leq n+1$. Define l by

$$k(k^{l+1}b'+1) > n = 1,$$

$$k(k^{l}b'+1) \leq n+1.$$

Then, $l \geq 0$ and we have that $k^{l+1}b'+1 < k^{l+1}b'+k \leq n+1$, so $k^{l+1}b'+1 \leq n$; $k(k^{l+1}b'+1)$ appears somewhere in the sequence Q', and

$$\frac{k(k^{l+1}b'+1)}{(k(k^{l+1}b'+1),b')} = k(k^{l+1}b'+1) > n+1.$$

□

Theorem 7.7. *Theorem 7.5 implies Theorem 7.1. In fact, if Theorems 7.1 and 7.5 hold for n, then Theorem 7.1 holds for $n+1$.*

Proof. We proceed by induction on n. Assume that Theorem 7.1 is true for n and consider

$$0 < a_1 < \ldots < a_n < a_{n+1}.$$

Then, by induction, we know that

$$\max_{1\le i,j\le n}\left\{\frac{a_i}{(a_i,a_j)}\right\} \ge n.$$

If $\max_{1\le i,j\le n}\left\{\frac{a_i}{(a_i,a_j)}\right\} > n$, then

$$\max_{1\le i,j\le n+1}\left\{\frac{a_i}{(a_i,a_j)}\right\} \ge n+1.$$

Hence, we may assume that

$$\max_{1\le i,j\le n}\left\{\frac{a_i}{(a_i,a_j)}\right\} = n.$$

By Theorem 7.5, the sequence is standard, i.e., $a_1 < a_2 < \ldots < a_n$ is a standard sequence. Now by Theorem 7.6 we have

$$\max_{1\le i,j\le n+1}\left\{\frac{a_i}{(a_i,a_j)}\right\} \ge n+1.$$

□

Theorem 7.8. (Szemerédi) [8]

Theorem 7.1 is true for $n = p$, where p is prime.

Proof. This follows immediately from Theorem 7.2, since Conjecture 5.5 holds with $p-1$ colors, by Theorem 5.1. □

Lemma 7.9. *If* $(a_i, a_2, \ldots, a_n) = 1$, $\max_{i,j}\left\{\dfrac{a_i}{(a_i, a_j)}\right\} \le n$ *and* p *is a prime with* $p|a_i$, *for some* i, *then* $p \le n$.

Proof. Since $(a_i, a_2, \ldots, a_n) = 1$ and $p|a_i$, there exists an a_j such that $p \nmid a_j$. Hence, $\frac{a_i}{(a_i,a_j)} \ge p$. However, by our hypothesis $\max_{i,j}\left\{\dfrac{a_i}{(a_i, a_j)}\right\} \le n$, hence we have $p \le n$. □

Lemma 7.10. *If* $(a_1, a_2, \ldots, a_n) = 1$ *and* $\max_{i,j}\left\{\dfrac{a_i}{(a_i, a_j)}\right\} \le n$, *then* $a_i|M_n$ *for all* i.

Proof. Let $M_n = p_1^{l_1} \cdots p_s^{l_s}$ and assume $p_i^{l_i+1}|a_k$. Then, there exists a_j such that $(a_j, p_i) = 1$. Hence,

$$p_i^{l_i+1}|\frac{a_k}{(a_j, a_k)}.$$

But this says that the ratio is larger than n. We now see that if the maximum of the ratios is $\le n$, then each element of the sequence divides M_n. □

Lemma 7.11. *If* $a_1 = b_1^{(n)} = \frac{M_n}{n}$ *and* $\max_{i,j}\left\{\dfrac{a_i}{(a_i, a_j)}\right\} \le n$ *with* $(a_1, \ldots, a_n) = 1$, *then* $a_i = b_i^{(n)}$ *for all* i.

Proof. We have $a_1 = \frac{M_n}{n}$, $a_k = \frac{j_k a_1}{i_k}$, $(i_k, j_k) = 1$, $i_k \le j_k \le n$. Assume $(j_k, n) = d \ne j_k$. Then, there exists a prime $p = p_1$ such that $p_1|j_k$, $p_1 \nmid n$. Thus, since $p_1^{l_1}|a_1$ and $(i_k, j_k) = 1$, we have $p_1^{l_1+1}|a_k$, which contradicts Lemma 7.10. Hence, $j_k|n$ so that

$$a_k = \frac{na_1}{d_k}, \quad 1 \le d_k \le n.$$

But the a_k are increasing and there are exactly n of them; hence, this says $d_1 = n, d_2 = n-1, \ldots, d_n = 1$, i.e.,

$$a_k = \frac{na_1}{n-k+1} = \frac{M_n}{n-k+1}.$$

□

Corollary 7.12. *If* $(a_1, \ldots, a_n) = 1$ *and* $\max\limits_{i,j}\left\{\dfrac{a_i}{(a_i, a_j)}\right\} \le n$*, then* $a_i \le b_i^{(n)}$*, for all* i*.*

Proof. Since $\max\limits_{i,j}\left\{\dfrac{a_i}{(a_i, a_j)}\right\} \le n$, we have that $a_i = \frac{M_n}{c_i}$, where $c_1 > c_2 > \ldots > c_n$. If $a_i > b_i^{(n)}$, then $\frac{M_n}{c_i} > \frac{M_n}{n-i+1}$, so $n-i+1 > c_i$. So we have that $n-i+1 > c_i > c_{i+1} > \ldots > c_n$. Hence,

$$\{c_i, c_{i+1}, \ldots, c_n\} \subset \{1, 2, \ldots, n-i\}.$$

But $|\{c_i, c_{i+1}, \ldots, c_n\}| = n-i+1 > n-i = |\{1, 2, \ldots, n-i\}|$, and we have a contradiction.

□

Theorem 7.13. *Theorem 7.5 is true for* $n = p$*,* p *a prime.*

Proof. We may assume that $(a_1, \ldots, a_n) = 1$. Since $\frac{a_i}{(a_i, a_j)} \le p$, we have that $a_i \le pa_j$. If $a_i \ne pa_j$, for all i, j, consider $a_i^{'} = \frac{a_i}{(a_i, p)}$. Then, $|\{a_1^{'}, \ldots, a_p^{'}\}| = p$. Furthermore, since $p^2 \nmid M_p$, where M_p is the least common multiple of $\mathbf{p}$, we have that$(a_i^{'}, p) = 1$, so $\max\limits_{i,j}\left\{\dfrac{a_i}{(a_i, a_j)}\right\} < p$, which contradicts Theorem 7.8. Hence, for some i, j, we must have $a_i = pa_j$. But this implies that $i = 1$, $j = p$ and $a_p = pa_1$. Furthermore, since $p^2 \nmid M_p$, $p \nmid a_1$. If $p | a_i$ for all $i > 1$, then $a_i = \frac{pa_1}{c_i}$, with $c_1 = p > c_2 > \ldots > c_p = 1$. Hence, $a_i = b_i^{(n)}$ and $a_1 < \ldots < a_n$ is a standard sequence. Assume that $(a_i, p) = 1$ for some $i > 1$. Then, $a_i = \frac{k_1 a_1}{k_2}$, $(k_1, k_2) = 1$,$k_2 | a_1$, $k_2 < k_1 < p$. Then $(a_p, a_i) = (pa_1, \frac{k_1 a_1}{k_2}) = \frac{a_1}{k_2}$, so $\frac{a_p}{(a_i, a_p)} = pk_2 \le p$, which implies $k_2 = 1$. So we have that if $(a_i, p) = 1$, then $a_i = k_i a_1$. If $a_j = \frac{pa_1}{c}$, $(c, p) = 1$, then $(a_i, a_j) = (\frac{pa_1}{c}, \frac{k_i c a_1}{c}) = \frac{a_1}{c}$. Hence, $\frac{a_i}{(a_i, a_j)} = \frac{k_i a_1}{\frac{a_1}{c}} = k_i c \le p$, so $k_i < \frac{p}{c}$, since $(k_i c, p) = 1$. Hence, $k_i a_1 < \frac{pa_1}{c}$, so $a_i < a_j$. That is, the sequence $a_1 < \ldots < a_p$ takes the form

$$a_1 < a_1 k_1 < \ldots < a_1 k_l < \frac{pa_1}{c_1} < \ldots < \frac{pa_1}{c_r} < \frac{pa_1}{1}. \tag{7.1}$$

If $k_l > \frac{p}{2}$, then $\frac{p}{c_1} > k_l > \frac{p}{2}$, so $c_1 < 2$, that is $c_1 = 1$ and (7.1) becomes

$$a_1 < 2a_1 < 3a_1 < \ldots < (p-1)a_1 < pa_1, \tag{7.2}$$

so $a_1 = 1$, since $(a_1, \ldots, a_p) = 1$, and (7.2) is a standard sequence. Assume that $k_l < \frac{p}{2}$, that is, $|\{a_i : (a_i, p) = 1\}| < \frac{p}{2}$. Since there is at least one a_i, $i > 1$, such that $(a_i, p) = 1$, we have that $\frac{p}{c_1} > k_l \geq 2$, so $c_1 < \frac{p}{2}$, that is, the c_i must assume fewer than $\frac{p}{2}$ values. Hence, $|\{a_i : p|a_i\}| < \frac{p}{2}$. But

$$\{a_1, a_2, \ldots, a_p\} = \{a_i : p|a_i\} \cup \{a_i : (a_i, p) = 1\}$$

and this implies that

$$|\{a_1, a_2, \ldots, a_p\}| = p < \frac{p}{2} + \frac{p}{2} < p,$$

so $p < p$. Hence, $k_l \nleq \frac{p}{2}$. □

Corollary 7.14. *Theorem 7.1 is true for $n = p + 1$, p a prime.*

Proof. Since Theorems 7.1 and 7.7 are true for $n = p$, p a prime, Theorem 7.6 readily gives us the desired result. □

In our attempts to provide proof of the existence of partial homomorphisms of arbitrary order, we turned to trying to find a way in which a given partial homomorphism can be extended or truncated. It is in this light that the result of Vélez may prove useful.

Question 7.15. *Given any prime p, is there at least one partial homomorphism of order $p-1$ that can be extended to produce a partial homomorphism of order p?*[1]

[1] The answer is no in general. See Section 7.2 and Appendix C.

A natural attempt towards solving Question 7.15 affirmatively would be to show that there is a partial homomorphism $h : \mathbf{p-1} \to \mathbb{Z}_{p-1}$ such that, defining $h(p) = p-1$, the resulting extension is a partial homomorphism. This would be the case if we could ensure that there is at least one such h that does not require any "carrying," i.e., such that if $a, b, ab \in \mathbf{p-1}$, then $h(a) + h(b) = h(ab)$ in $\mathbb{Z}$, not just in $\mathbb{Z}_{p-1}$.

7.2 A Late Conclusion

Four days after the defense of this thesis, Zack Teitler informed us of a series of articles that allow us to answer the question of whether multiplicative colorings exist for all n. The motivation for the research done in the articles was the conjecture of Graham, which resulted in the Balasubramanian–Soundararajan Theorem of the previous section.

Without further ado, let us first state the following theorem concerning the existence of multiplicative colorings.

Theorem 7.16. *There exist $n \in \mathbb{Z}^+$ for which no multiplicative coloring exists. In fact, the smallest such n is $n = 195$.*

This refutes what seemed to be the prevailing opinion, that a careful probabilistic argument would prove the existence of multiplicative colorings for all n, see for example Greg Kuperberg's suggestion in [2].

The proof follows from the work initiated by Rodney Forcade, Jack Lamoreaux, and Andrew Pollington when they posed the following question in 1986, see [18].

Question 7.17. *Is it possible, changing only those products that exceed n, to make the set $\mathbf{n}$ into a multiplicative group?*

Note that, in our terminology, the question corresponds to asking whether G-satisfactory groups exist for all values of n. In the article, they conjecture that the answer to Question 7.17 is affirmative. In their discussion, they also ask (in different terms) whether strong representatives exist for all values of n.

In 1990, perhaps surprisingly, Forcade and Pollington answered Question 7.17 negatively, see [19]. To do so they employed an exhaustive search algorithm that, in the case of $n = 195$, did not produce a G-satisfactory group.

We refer to those values of n for which no G-satisfactory group exist as *groupless* n. We included in Appendix C a list of all groupless $n \leq 500$.

Additionally, the work of Simon Blackburn and James McKee, in [21], is particularly relevant. In their paper, partial $\mathbb{Z}_n$-homomorphisms are referred to as "bijective logarithms of length n," or, simply, "logarithms of length n". Several references where they are studied are provided in their Section 5.1. Using our terminology, we now state their Theorem 5.1. For proof, see [20].[2]

Theorem 7.18. (Kummer, Mills)
Let h be a partial $\mathbb{Z}_n$-homomorphism.

(a) If n is odd, then the associated $\mathbb{Z}_n$-coloring is strongly representable.

(b) If $n \equiv 2 \mod 4$, then the associated $\mathbb{Z}_n$-coloring is strongly representable iff $h(m)$ is even whenever m divides n and $m \equiv 1 \pmod 4$.

(c) If $n \equiv 0 \mod 4$, then the associated $\mathbb{Z}_n$-coloring is strongly representable iff $h(m)$ is even whenever m divides $n/4$.

[2] It is noteworthy to mention that the argument makes essential use of Chebotarev's density theorem, a subtle generalization of Dirichlet's theorem.

(d) *If there is one strong representative of order n, then there are in fact infinitely many.*

Also, in Blackburn–McKee, [21] Section 5.2, Dömötör's coloring question, Question 4.1 of this thesis, is considered (independently), in the language of tilings of powers of $\mathbb{Z}$. In [21] Section 9.2, they discuss the number of partial homomorphisms for a given n and present a table of values of $n \leq 300$ that do not admit partial $\mathbb{Z}_n$-homomorphisms.[3] Blackburn-McKee [21] suggest, based on numerical evidence, that if n is large enough, then there is a partial $\mathbb{Z}_n$-homomorphism iff $n+1$ or $n2+1$ is prime. Perhaps, in fact, for n large enough, there is a G-satisfactory group (even without the restriction of G being abelian) iff the same restriction on n holds: $n+1$ or $n2+1$ is prime so, in fact, there is a $\mathbb{Z}_n$-satisfactory group.[4]

In closing, we mention the following: Although it is known that multiplicative colorings do not exist for all values of n, the question of whether satisfactory colorings exist for all values of n remains open. As evidenced by Theorem 5.40, non-multiplicative satisfactory colorings do in fact exist. Thus, if one is to make progress in solving the problem, then it will require a better understanding of non-multiplicative colorings. Perhaps a good place to start this analysis would be the case of $n = 195$.

[3] The table they present coincides with our Table C.1.

[4] See Remark 5.42.

REFERENCES

[1] Melvin B. Nathanson. *Elementary Methods in Number Theory.* Springer-Verlag, New York, 2000.

[2] Palvolgyi Dömötör. *http://mathoverflow.net/questions/26358/can-we-color-z-with-n-colors-such-that-a-2a-na-all-have-different-colors*

[3] KöMaL. *http://www.komal.hu/verseny/feladat.cgi?a=honaph=201004t=matl=en*

[4] Alexander Soifer. *The Mathematical Coloring Book, Mathematics of Coloring and the Colorful Life of Its Creators.* Springer, New York, 2009.

[5] Terence Tao and Van Vu. *Additive Combinatorics.* Cambridge University Press, Cambridge, 2006.

[6] Eric W. Weisstein. "Graph Coloring." From MathWorld–A Wolfram Web Resource. *http://mathworld.wolfram.com/GraphColoring.html*

[7] Ramachandran Balasubramanian and Kannan Soundararajan. *On a conjecture of R. L. Graham.* Acta Arithmetica, LXXV.1 (1996), pp. 1–38.

[8] William Yslas Vélez. *Some Remarks On a Number Theoretic Problem of Graham.* Acta Arithmetica, XXXII (1977), pp. 232–238.

[9] Andrés E. Caicedo. *Regressive functions on pairs.* European Journal of Combinatorics (2009), doi:10.1016/j.ejc.2009.07.010

[10] Ronald Graham, Bruce Rothschild, Joel Spencer. *Ramsey Theory*, second edition. John Wiley and sons, New York, N.Y., 1990.

[11] András Hajnal. *Infinitary combinatorics*, in *Handbook of Combinatorics*, Vol. II, Ronald Graham, Martin Grötschel, László Lovász, eds., Elsevier, The MIT Press, 1995, 2085–2116.

[12] Markus Meringer, Eric W. Weisstein. "Regular Graph." From MathWorld–A Wolfram Web Resource. *http://mathworld.wolfram.com/RegularGraph.html*

[13] Kenneth Falconer. *The realization of distances in measurable subsets covering* $\mathbb{R}^n$. Journal of Combinatorial Theory Series A, vol 31 (2), (1981), 184–189.

[14] Dan Pritkin. *All unit-distance graphs of order 6197 are 6-colorable.* Journal of Combinatorial Theory Series B, vol 73 (2) (1998), 159–163.

[15] Andrés E. Caicedo (mathoverflow.net/users/6085), Fifth powers modulo a prime, http://mathoverflow.net/questions/78270 (version: 2011-10-16).

[16] Lawrence C. Washington. *Introduction to Cyclotomic Fields*, second edition. Springer-Verlag, New York, 1997.

[17] Kustaa Inkeri. *The Real Roots of Bernoulli Polynomials.* Ann. Univ. Turku. Ser. A I 37 1959 20.

[18] Rodney Forcade, Jack Lomoreaux and Andrew Pollington. *A Group of Two Problems in Groups.* The American Mathematical Monthly, vol 93, No 2 (Feb., 1986), pp. 119-121.

[19] Rodney Forcade, Andrew Pollington. *What is special about 195? Groups, nth power maps and a problem of Graham.* Proceddings of the First Conference of the Canadian Number Theory Association, Banff, 1988, R.A. Mollin, ed., Walter de Gruyter, Belin, 1990.

[20] W.H. Mills. *Characters with preassigned values.* Canad. J. Math., 15 (1963), pp. 169–171.

[21] Simon Blackburn, James McKee. *Constructing k-radius Sequences.* (Mathematics of computation, to appear.)

[22] Bronislaw Knaster. *Un théorème sur les fonctions d'ensenmbles.* Ann. Soc. Polon. Math, vol 6 (1928), pp. 133–134.

[23] Alfred Tarski. *A lattice-theoretical fixpoint theorem and its applications.* Pacific Journal of Mathematics, vol 5, No 2 (1955), pp. 285–309.

[24] Karen Chandler. *Groups formed by redefining multiplication.* Canad. Math. Bull. vol 31, No 4 (1988), pp. 419–423.

[25] Ronald Graham. *Advanced Problem 5749.* The American Mathematical Monthly, vol 77, No 7 (Aug. - Sep., 1970), p. 775.

APPENDIX A

CODE

A.1 Matlab Code for *g*(4,4)

```
%Function to find miniumum
%homogeneous sets of size 4
%input value m is the minimum
%value at which the search starts.
%The function is currently only
%written for the case m=4.
%Any value other than 4 will
%produce nonsense. The input variable
%n determines the level to
%which the search for homogenous sets
%will occur. This function produces no
%min homog sets of size 4 for values
%of n less than 85
function MinH4(m,n)

%initializing matrix
A=zeros(85);


% filling matrix with values determined by g3
```

```
A(2:37,2:37)=MinH3(3);

% Sentinal values
A(1:85,1:3)=-1;
A(1:4,1:85)=-1;

    for i=1:85

        for j=1:85

                if i<=j
                    A(i,j)=-1;
                end

        end

     end

 % for loop extending g3
    for i = 38:85
        % for loop for 4-36 (non-injective part)
        for j =4:36
            if i>=j
            A(i,j)=j-1;
            end
        end % end for loop for 4-36

        % for loop for 37-85 (injective part)
        for k =37:85
            if i>k
            A(i,k)=mod(i-k-1,k);
            end
        end %end loop for 37-85

    end %end loop to extend g3

    A(8,6)=2;
    A(17,4)=1;
    A(17,9)=7;
    A(17,10)=6;
    A(17,11)=9;
    A(17,13)=11;
    A(17,15)=13;
    A(17,5)=2;
    A(17,8)=6;
    A(17,11)=5;
    A(17,13)=3;
    A(17,15)=1;
    A(18,9)=8;
    A(19,4)=0;
    A(19,5)=3;
    A(19,8)=4;
    A(20,8)=3;
    A(20,9)=0;
    A(21,9)=2;
    A(21,8)=2;
    A(21,12)=8;
    A(22,13)=3;
    A(23,8)=0;
    A(23,13)=4;
```

```
A(24,13)=5;
A(25,13)=6;
A(26,13)=7;
A(27,13)=8;
A(28,13)=9;
A(29,13)=10;
A(32,12)=0;
A(33,12)=1;
A(34,12)=2;
A(35,12)=3;
A(36,12)=4;
A(37,12)=5;
A(38,4)=2;
A(38,20)=17;
A(38,5)=1;
A(38,6)=0;
A(38,7)=0;
A(38,8)=2;
A(38,9)=1;
A(38,10)=6;
A(38,12)=6;
A(38,14)=3;
A(38,15)=3;
A(38,16)=3;
A(38,17)=3;
A(38,19)=5;
A(39,4)=2;
A(39,5)=0;
A(39,6)=3;
A(39,7)=4;
```

```
A(39,8)=5;
A(39,9)=2;
A(39,11)=6;
A(39,13)=4;
A(39,14)=4;
A(39,15)=4;
A(39,16)=4;
A(39,17)=4;
A(39,19)=6;
A(39,20)=18;
A(39,21)=16;
A(40,4)=2;
A(40,5)=1;
A(40,6)=2;
A(40,7)=3;
A(40,8)=6;
A(40,9)=2;
A(40,10)=0;
A(40,12)=7;
A(40,13)=5;
A(40,14)=5;
A(40,15)=5;
A(40,16)=5;
A(40,17)=5;
A(40,19)=7;
A(40,20)=19;
A(40,21)=17;
A(40,22)=17;
A(40,23)=18;
A(40,24)=19;
```

```
A(40,25)=20;
A(40,26)=21;
A(40,27)=22;
A(40,28)=21;
A(40,29)=22;
A(40,30)=21;
A(40,31)=22;
A(40,32)=21;
A(40,33)=22;
A(40,34)=21;
A(40,35)=22;
A(40,36)=22;
A(41,4)=0;
A(41,6)=4;
A(41,7)=2;
A(41,8)=0;
A(41,9)=0;
A(41,10)=1;
A(41,12)=8;
A(41,13)=6;
A(41,14)=6;
A(41,15)=6;
A(41,16)=6;
A(41,19)=0;
A(41,20)=18;
A(41,21)=18;
A(41,22)=18;
A(41,23)=19;
A(41,24)=20;
A(41,25)=21;
```

```
    A(41,26)=22;
    A(41,27)=23;
    A(41,28)=22;
    A(41,29)=23;
    A(41,30)=22;
    A(41,31)=23;
    A(41,32)=22;
    A(41,33)=23;
    A(41,34)=22;
    A(41,35)=23;
    A(41,36)=23;
    A(42,5)=3;
    A(42,10)=2;
    A(42,12)=0;
    A(42,13)=0;
    A(42,14)=0;
    A(42,15)=0;
    A(42,16)=0;
    A(42,17)=0;
    A(42,20)=17;
    A(43,5)=0;
    A(43,10)=3;
    A(43,11)=6;
    A(43,12)=1;
    A(43,13)=1;
    A(43,14)=1;
    A(43,15)=1;
    A(43,16)=1;
    A(43,17)=1;
    A(43,20)=16;
```

```
A(44,10)=4;
A(44,12)=2;
A(44,13)=2;
A(44,14)=2;
A(44,15)=2;
A(44,16)=2;
A(44,17)=2;
A(44,20)=14;
A(45,10)=5;
A(45,12)=3;
A(45,13)=3;
A(45,14)=3;
A(45,15)=3;
A(45,17)=3;
A(46,13)=4;
A(46,14)=4;
A(46,15)=4;
A(46,16)=4;
A(46,17)=4;
A(49,14)=2;
A(49,32)=0;
A(50,14)=3;
A(50,33)=0;
A(51,14)=4;
A(51,34)=0;
A(52,14)=5;
A(52,35)=0;
A(53,14)=6;
A(54,14)=7;
A(54,19)=0;
```

```
A(54,36)=0;
A(55,14)=8;
A(55,20)=0;
A(56,14)=9;
A(56,21)=0;
A(57,22)=0;
A(58,15)=2;
A(58,23)=0;
A(59,15)=3;
A(59,24)=0;
A(60,15)=4;
A(60,25)=0;
A(61,15)=5;
A(61,26)=0;
A(62,15)=6;
A(62,27)=0;
A(63,15)=7;
A(63,28)=0;
A(64,15)=8;
A(64,29)=0;
A(65,15)=9;
A(65,30)=0;
A(66,15)=10;
A(66,31)=0;
A(77,24)=1;
A(78,25)=1;
A(79,26)=1;
A(80,27)=1;
A(81,28)=1;
A(82,29)=1;
```

```
    A(83,30)=1;
    A(84,31)=1;

    A(22:30,9)=3;
    A(31:39,9)=2;
    A(40:48,9)=1;
    A(49:57,9)=4;
    A(58:66,9)=5;

    for i=21:36
        A(38,i)=A(38,i)-1;
    end
    for i=22:36
        A(39,i)=A(39,i)-5;
    end
    for i=41:84
        A(i,18)=mod(i,18);
    end
    for i=40:42
        A(i,11)=mod(i,11);
    end

    for i=44:48
        A(i,11)=mod(i,11);
    end
%%%%%%%%%%%%%%%%%%%%%%%end g4
%%%%%%%%%%%%%%%%%%%%%%%modifications
%%%%%%%%%%%%%%%%%%%%%%

    %begin search for min homog sets of size 4
    for a = m:n

        for b=5:n

            for c=6:n

                for d=6:n

                    if (A(b,a)==A(c,a)
                        && A(b,a)==A(d,a)
                        && A(c,b)==A(d,b)
                        && c<d && a<b
                        && b<c && A(b,a)>=0
                        && A(c,a)>=0 && A(d,a)>=0
                        && A(c,b)>=0 && A(d,b)>=0)

                    H=[a,b,c,d]

                    end %end if

                end %end d

            end %end c

        end %end b

    end %end a
    A;
end %end function
```

Figure A.1: A Matlab function witnessing a regressive function with no min-homogeneous set of size 4

A.2 The Search for Strong Representatives

Recall that a strong representative of order n for a coloring c is a prime

$$p = nk + 1$$

such that

$$i^k \pmod{p}$$

are pairwise distinct for $i \in \mathbf{n}$. Thus to find a strong representative of order n is to define a satisfactory coloring using n colors.

As discussed in subsection 5.1.1, in two specific cases (when n+1 or 2n+1 is prime), we are guaranteed the existence of a strong representative of order n. However, outside these two cases it is an arduous task to find a strong representative of order n. Figure A.2 gives the Maple code we used to find a strong representatives of order n. Although the code evolved over time to what is seen below the general search algorithm has remained unchanged.

A.3 Density Data Collection Code for Strong Representatives of Order 5

Figure A.3 gives the Maple code that was utilized to collect data concerning the density of primes associated with strong representatives in the case of 5 colors.

Table A.1 represents data collected on the density of satisfactory 5-colorings.

```
f := proc (n, crem, lil, big)
 #n is the number of colors being used
 #crem is the increment. crem is 1 if n is even and 2 if n is odd
 #lil is the lower bound for where the search starts
 #big is the upper bound for the search
 #The purpose for using big and lil is
 #to search over an interval
 #so the worksheet can be started at a different
 #lower bound if no positive result is attained
 #on the interval

#begin main loop for k ‘
 for k from lil by crem to big do

#Statement to keep track of
#how far along the process
#is in case the kernel collapses
if 0 = ‘mod‘(k, 1000000) then print(k)
end if; #End tracking

  #Begin primary search loop
  if isprime(n*k+1) then #Check if nk+1 is prime

P := n*k+1; #Assigning prime

#Creating se using Maple’s seq function
S := {seq(‘mod‘(‘&^‘(i, k), P), i = 1 .. n)};

#Checking the cardinality of the set
if evalb(nops(S) = n) then
return [k, P]
end if  #End cardinality check

end if #End primary search loop

end do; #End main loop for k

#Returns a statement if there is no positive result on
#the interval
return "No positive result on this interval";

end proc; #End procedure
```

Figure A.2: Maple code used in the search for strong representatives

```
f := proc (m, n)
P1 := 0; P5 := 0; PT := 0;
M := Matrix(25, 9);
M[1, 1] := "5k"; M[1, 2] := "P1";
M[1, 3] := "P5"; M[1, 4] := "PT";
M[1, 5] := "P1+P5"; M[1, 6] := "pi(5k)";
M[1, 7] := "P_1 / P_5"; M[1, 8] := "(P_1+P_5)/PT";
M[1, 9] := "(P1+P5)/pi(5k)";
j := 2;

for k from m by 2 to n do
if 0 = ‘mod‘(k, 200000) then
M[j, 1] := 5*k;
M[j, 2] := P1;
M[j, 3] := P5;
M[j, 4] := PT;
M[j, 5] := P1+P5;
M[j, 6] := Pi(5*k);
M[j, 7] := P1/P5;
M[j, 8] := (P1+P5)/PT;
M[j, 9] := (P1+P5)/Pi(5*k);
j := j+1 end if;
if isprime(5*k+1) then
P := 5*k+1;
PT := PT+1;
S := {seq(‘mod‘(‘&^‘(i, k), P), i = 1 .. 5)};
if evalb(nops(S) = 5) then
a6 := ‘mod‘(‘&^‘(6, k), P);
a5 := ‘mod‘(‘&^‘(5, k), P);
if evalb(1 = a6) then
P1 := P1+1 end if;
if evalb(a5 = a6) then
P5 := P5+1 end if
end if
end if
end do;
Export(M, "n_5_density_data.xls") end proc;
proc(m, n)  ...  end;
```

Figure A.3: Maple code used for data acquisition in the case of 5 colors

Recall that c_1 denotes a satisfactory coloring using 5 colors which has $c(6) = c(1)$ and c_5 denotes a satisfactory coloring using 5 colors which has $c(6) = c(5)$. Define the following sets:

$$P_1(m) = \left|\{p : p = 5k + 1 \leq m, p \text{ is } prime, p \text{ is a strong representative for } c_1\}\right|,$$

$$P_5(m) = \left|\{p : p = 5k + 1 \leq m, p \text{ is } prime, p \text{ is a strong representative for } c_5\}\right|,$$

$$P_T(m) = \left|\{p : p = 5k + 1 \leq m,\ p \text{ is prime}\}\right|,$$

$$\pi(m) = \left|\{p : p \text{ is prime}, p \leq m\}\right|.$$

A.4 Density Data Collection Code for 3-representatives

Figure A.5 gives the Sage code which was utilized to collect data concerning the size of the set of distinct cubes among the first n cubes modulo a prime $p = n3 + 1$. No such p is a strong representative of order n. The following is a sample of the output which the code produced: Similarly, we may consider the 5-densities using the code in Figure A.5 (replacing $k = 3$ by $k = 5$ and initializing $p = 11$). In this case, the following is a sample of the output which the code produced:

```
For k = 5, n = 35738, and p = 178691  do not work:
|{i^k mod p: i=1,...,n}| = 24001 and m/n = 0.6715820695
For k = 5, n = 35756, and p = 178781  do not work:
|{i^k mod p: i=1,...,n}| = 24029 and m/n = 0.6720270724
For k = 5, n = 35766, and p = 178831  do not work:
```

```
For k = 3, n = 387562, and  p = 1162687  do not work:
|{i^k mod p: i=1,...,n}| = 258374  and m/n = 0.6666649465
For k = 3, n = 387576, and  p = 1162729  do not work:
|{i^k mod p: i=1,...,n}| = 258387  and m/n = 0.6666744071
For k = 3, n = 387580, and  p = 1162741  do not work:
|{i^k mod p: i=1,...,n}| = 258387  and m/n = 0.6666675267
For k = 3, n = 387584, and  p = 1162753  do not work:
|{i^k mod p: i=1,...,n}| = 258390  and m/n = 0.6666683867
For k = 3, n = 387590, and  p = 1162771  do not work:
|{i^k mod p : i=1,...,n}| = 258393  and m/n = 0.6666658067
For k = 3, n = 387596, and  p = 1162789  do not work:
|{i^k mod p: i=1,...,n}| = 258400  and m/n = 0.6666735467
For k = 3, n = 387602, and  p = 1162807  do not work:
|{i^k mod p: i=1,...,n}| = 258401  and m/n = 0.6666658067
For k = 3, n = 387622, and  p = 1162867  do not work:
|{i^k mod p: i=1,...,n}| = 258414  and m/n = 0.6666649468
For k = 3, n = 387626, and  p = 1162879  do not work:
|{i^k mod p: i=1,...,n}| = 258390  and m/n = 0.6665961520
For k = 3, n = 387632, and  p = 1162897  do not work:
|{i^k mod p: i=1,...,n}| = 258422  and m/n = 0.6666683865
For k = 3, n = 387642, and  p = 11629274 do not work:
|{i^k mod p: i=1,...,n}| = 258429  and m/n = 0.6666692464
```

Figure A.4: Sample of the output produced by the code found in Figure A.5 when $k = 3$.

```
|{i^k mod p: i=1,...,n}| = 24017 and m/n = 0.6715036627

For k = 5, n = 35784, and p = 178921  do not work:

|{i^k mod p: i=1,...,n}| = 24052 and m/n = 0.6721439750

For k = 5, n = 35786, and p = 178931  do not work:

|{i^k mod p: i=1,...,n}| = 24027 and m/n = 0.6714078131

For k = 5, n = 35790, and p = 178951  do not work:

|{i^k mod p: i=1,...,n}| = 24051 and m/n = 0.6720033529

For k = 5, n = 35804, and p = 179021  do not work:

|{i^k mod p: i=1,...,n}| = 24065 and m/n = 0.6721316054
```

Sample of the output produced by the code found in Figure A.5 when $k = 5$.

```
k=3
s=0
p=k
while s==0:
   p=next_prime(p)
   while not((p-1)%k==0):
       p=next_prime(p)
   R=IntegerModRing(p)
   n=(p-1)/k
   s=1
   m=Set([R(i)^k for i in range(1,n+1)]).cardinality()
   if not(m==n):
       s=0
       t=(m/n).n(digits=10)
       print "For k =",k,", n =",n,", and p =",p," do not work:
       |{i^k mod p: i=1,...,n}| =",m," and m/n =",t
```

Figure A.5: Sage code used in the density analysis of k-representatives

m	10^6	$2 \cdot 10^6$	$3 \cdot 10^6$	$4 \cdot 10^6$	$5 \cdot 10^6$	$6 \cdot 10^6$	$7 \cdot 10^6$	$8 \cdot 10^6$	$9 \cdot 10^6$	10^7
$P_1(m)$	626	1203	1757	2314	2838	3376	3873	4386	4886	5358
$P_5(m)$	626	1210	1783	2291	2822	3309	3843	4302	4772	5265
$P_T(m)$	19617	37188	54175	70779	87062	103153	119109	134912	150604	166104
$P_1(m) + P_5(m)$	1252	2413	3540	4605	5660	6685	7716	8688	9658	10623
$\pi(m)$	78498	148933	216816	283146	348513	412849	476648	539777	602489	664579
$\frac{P_1(m)}{P_5(m)}$	1	0.994215	0.985418	1.010039	1.005670	1.020248	1.007806	1.019526	1.023889	1.017664
$\frac{P_1(m)+P_5(m)}{P_T(m)}$	0.063822	0.064887	0.065344	0.065062	0.065011	0.064807	0.064781	0.064398	0.064128	0.063954
$\frac{P_1(m)+P_5(m)}{\pi(m)}$	0.015949	0.016202	0.016327	0.016264	0.016240	0.016192	0.016188	0.016096	0.016030	0.015985

Table A.1: Density data for satisfactory 5-colorings

APPENDIX B

PARTIAL HOMOMORPHISM TABLES

The following tables represent explicit constructions of partial homomorphisms for $n \leq 54$. The tables are interpreted as follows. The first column represents the domain of the partial homomorphisms. The column whose first entry is $h_n(a)$ has as its row entries the image of a partial homomorphism on a set of size n. For example, in Table B.1, $h_8(3) = 4$. Note that in Tables B.2, B.4, B.3, and B.5 we list only the values for the primes less than or equal to $\frac{n}{2}$ since having these values allows one to complete the table.

a	$h_1(a)$	$h_2(a)$	$h_3(a)$	$h_4(a)$	$h_5(a)$	$h_6(a)$	$h_7(a)$	$h_8(a)$	$h_9(a)$	$h_{10}(a)$	$h_{11}(a)$	$h_{12}(a)$	$h_{13}(a)$	$h_{14}(a)$	$h_{15}(a)$	$h_{16}(a)$
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	-	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	-	-	2	3	3	3	3	4	4	4	4	4	4	4	4	5
4	-	-	-	2	2	2	2	2	2	2	2	2	2	2	2	2
5	-	-	-	-	4	5	5	6	6	6	6	9	9	9	9	8
6	-	-	-	-	-	4	4	5	5	5	5	5	5	5	5	6
7	-	-	-	-	-	-	6	7	7	9	9	7	7	11	11	11
8	-	-	-	-	-	-	-	3	3	3	3	3	3	3	3	3
9	-	-	-	-	-	-	-	-	8	8	8	8	8	8	8	10
10	-	-	-	-	-	-	-	-	-	7	7	10	10	10	10	9
11	-	-	-	-	-	-	-	-	-	-	10	11	11	7	7	14
12	-	-	-	-	-	-	-	-	-	-	-	6	6	6	6	7
13	-	-	-	-	-	-	-	-	-	-	-	-	12	13	14	15
14	-	-	-	-	-	-	-	-	-	-	-	-	-	12	12	12
15	-	-	-	-	-	-	-	-	-	-	-	-	-	-	13	13
16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	4

Table B.1: Partial Homomorphism table for $n \in [1, 16]$.

a	$h_{17}(a)$	$h_{18}(a)$	$h_{19}(a)$	$h_{20}(a)$	$h_{21}(a)$	$h_{22}(a)$	$h_{23}(a)$	$h_{24}(a)$	$h_{25}(a)$	$h_{26}(a)$	$h_{27}(a)$	$h_{28}(a)$	$h_{29}(a)$	$h_{30}(a)$	$h_{31}(a)$	$h_{32}(a)$
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	6
5	8	8	8	12	12	12	12	12	12	12	12	12	12	12	12	14
7	11	14	14	18	15	15	15	15	15	15	18	18	18	20	20	23
11	14	12	12	9	9	8	8	18	18	18	21	21	21	26	26	30
13	15	17	17	8	8	21	21	21	21	21	25	25	25	28	28	26

Table B.2: Partial Homomorphism table for $n \in [17, 32]$.

a	$h_{33}(a)$	$h_{34}(a)$	$h_{35}(a)$	$h_{36}(a)$	$h_{37}(a)$	$h_{38}(a)$	$h_{39}(a)$
1	0	0	0	0	0	0	0
2	1	1	1	1	1	1	1
3	6	6	7	7	7	7	7
5	14	14	11	11	11	11	11
7	23	23	23	23	23	23	23
11	26	26	26	26	26	26	28
13	10	10	28	28	28	28	26
17	-	30	31	31	31	31	31
19	-	-	-	-	-	35	36

Table B.3: Partial Homomorphism table for $n \in [33, 39]$.

a	$h_{40}(a)$	$h_{41}(a)$	$h_{42}(a)$	$h_{43}(a)$	$h_{44}(a)$	$h_{45}(a)$	$h_{46}(a)$	$h_{47}(a)$	$h_{48}(a)$
1	0	0	0	0	0	0	0	0	0
2	1	1	1	1	1	1	1	1	1
3	6	6	6	6	6	6	6	6	6
5	32	32	19	19	19	20	20	20	21
7	19	19	33	33	35	35	36	36	38
11	16	16	23	23	23	28	29	29	29
13	30	30	30	30	27	32	33	33	19
17	26	26	15	15	15	15	15	15	15
19	28	28	27	27	30	24	24	24	36
23	-	-	-	-	-	-	44	44	46

Table B.4: Partial Homomorphism table for $n \in [40, 48]$.

a	$h_{49}(a)$	$h_{50}(a)$	$h_{51}(a)$	h_{52}	h_{53}	h_{54}
1	0	0	0	0	0	0
2	1	1	1	1	1	3
3	6	6	6	17	17	52
5	21	23	35	47	47	22
7	39	42	15	14	43	40
11	30	31	23	6	22	29
13	19	16	36	24	14	13
17	15	19	33	10	29	39
19	34	27	43	37	25	21
23	37	38	45	39	9	33

Table B.5: Partial Homomorphism table for $n \in [49, 54]$.

APPENDIX C

GROUPLESS n

The data found in Table C.1 was supplied by Rodney Forcade. The table lists all groupless values of $n \leq 500$. The data was obtained via an exhaustive search algorithm implemented by a computer. Note that for all values of $n \leq 500$ not listed in the table, at least one of the following is true:

1. $n + 1$ is prime,

2. $2n + 1$ is prime,

3. The existence of a G-satisfactory group has been verified.

195
205
208
211
212
214
217
218
220
227
229
235
242
244
246
247
248
252
253
255
257
258
259
263
264
265
266
267
269
271
274
275
279
283
286
287
289
290
291
294
295
297
298
301
302
304
305
307
311
313
314
317
318
319
322
324
325
327
328
331
332
333
334
335
337
339
340
343
344
347
349
351
353
355
356
357
361
362
364
365
367
368
370
373
374
376
377
379
381
383
385
387
389
390
391
392
394
395
397
399
401
402
403
406
407
409
412
415
416
417
421
422
423
424
425
427
433
434
435
436
437
439
444
445
446
447
449
450
451
452
454
457
458
461
463
465
467
469
471
472
474
475
477
479
480
481
482
484
487
489
492
493
494
496
497
499
500

Table C.1: A list of all groupless n for $n \leq 500$.