Equality of Number-Theoretic Functions over Consecutive Integers

by

Eitan A. Pechenick

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Pure Mathematics

Waterloo, Ontario, Canada, 2009

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

This thesis will survey a group of problems related to certain number-theoretic functions. In particular, for said functions, these problems take the form of when and how often they are equal over consecutive integers, n and $n + 1$. The first chapter will introduce the functions and the histories of the related problems. The second chapter will take on a variant of the Ruth-Aaron pairs problem, which asks how often sums of primes of two consecutive integers are equal. The third chapter will examine, in depth, a proof by D.R. Heath-Brown of the infinitude of consecutive integer pairs with the same number of divisors—i.e. such that $d(n) = d(n + 1)$. After that we examine a similar proof of the infinitude of pairs with the same number of prime factors—$\omega(n) = \omega(n + 1)$.

Acknowledgements

I would like to thank all the people who made this possible, especially my advisor, Dr. Kevin Hare.

Dedication

This is dedicated to my parents who have always been supportive.

Contents

List of Tables

Chapter 1

Preliminaries

1.1 Introduction

The Fundamental Theorem of Arithmetic roughly states that any positive integer may be represented uniquely as a product of powers of primes. In particular, for any $n > 1$, we may write

$$n = \prod_{i=1}^{r} p_i^{a_i}$$

uniquely for some $r > 0$ and primes p_i distinct.

Example 1.1.1. Let $n = 540$. Then $n = 2^2 \cdot 3^3 \cdot 5$, uniquely.

From this representation, we may quickly deduce information about certain numbers and collections of numbers. For example, by defining the divisor function as

$$d(n) = \prod_{i=1}^{r} (a_i + 1),$$

we may determine the number of divisors of an integer n.

Example 1.1.2. Let $n = 540$ as before. Then $d(n) = (2 + 1)(3 + 1)(1 + 1) = 24$, which tells us that 540 has 24 distinct divisors. In fact, its divisors are as follows: 1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 24, 27, 30, 36, 45, 54, 60, 90, 108, 135, 180, 270, and 540.

Notice that for integers m and n such that $\gcd(m, n) = 1$, we have the *multiplicative property* which gives us:

$$d(mn) = d(m)d(n).$$

It is not trivial that the divisor function above has this property, but it will be shown in the next section. If we define the following sum:

$$N_{s,t}(n) = \sum_{i=1}^{r} a_i^s p_i^t$$

and vary the s and t, we can produce a family of number-theoretic functions, each with the *additive property*:

$$N_{s,t}(mn) = N_{s,t}(m) + N_{s,t}(n),$$

whenever $\gcd(m, n) = 1$. The simplest of these is the one for which $s = t = 0$, and it is usually denoted $\omega(n)$. It is easy to see that

$$\omega(n) = \sum_{i=1}^{r} 1 = r$$

is the number of distinct prime factors of a given integer n.

Example 1.1.3. Let $n = 540$. Then $\omega(540) = 3$, since the only prime factors of 540 are 2, 3, and 5.

If we instead set $s = 0$ and $t = 1$, we define a function which we will call $P(n)$. We can see that

$$P(n) = \sum_{i=1}^{r} p_i$$

is the sum of said prime factors of n, with each prime counting only once.

Example 1.1.4. With $n = 540$, we have $P(n) = 2 + 3 + 5 = 10$.

Similarly, if we set $s = t = 1$, and call the resulting function $S(n)$, we see that

$$S(n) = \sum_{i=1}^{r} a_i p_i$$

is the sum of the prime factors of n, where each prime is counted in the sum according to the the power of that prime represented in n.

Example 1.1.5. We continue to let $n = 540$ and see that $S(n) = 2 \cdot 2 + 3 \cdot 3 + 1 \cdot 5 = 18$.

This thesis will focus on problems concerning how often we have equality of various number-theoretic functions over consective integers. In Chapter 2, we will focus on how often we find

$$P(n) = P(n+1).$$

It is worth noticing that if we replace $P(n)$ with $S(n)$, we will find many solutions in common, but we will discuss this later.

In Chapter 3, we will examine a proof by D. R. Heath-Brown [5] which primarily states that

$$d(n) = d(n+1)$$

infinitely often.

Chapter 4 will feature a similar proof that shows the same is true in the case of $\omega(n)$.

1.2 Multiplicative Functions

Recall the function

$$d(n) = \prod_{i=1}^{r} (a_i + 1),$$

commonly known as the *divisor function* has the property $d(mn) = d(m)d(n)$ for $\gcd(m, n) = 1$. It behooves us to discuss this property in some detail and to prove that this function does, in fact, possess it. We will also discuss $\phi(n)$, the Euler-phi function, which is another common multiplicative function.

This section uses definitions and results from Rosen [11].

Definition 1.2.1. Let f be a real or complex valued function defined over all positive integers. Then f is said to be *number-theoretic* or *arithmetic*.

Definition 1.2.2. Given a number-theoretic function f, we call f *multiplicative* if $f(mn) = f(m)f(n)$ whenever $\gcd(m, n) = 1$. Moreover, we call f *completely multiplicative* if $f(mn) = f(m)f(n)$ for all positive integers m and n.

Example 1.2.3. Let $f(n) = n^k$ for some fixed k. Then $f(mn) = (mn)^k = m^k n^k = f(m)f(n)$ for all m and n. So f is completely multiplicative.

Remark 1.2.4. If f is completely multiplicative, then f is multiplicative.

Suppose that f is a multiplicative function. Notice that powers of any two distinct primes p and q must be coprime. Thus it follows that $f(p^i q^j) = f(p^i)f(q^j)$. By induction, we may make this statement, trivially, for any number of distinct primes. Namely,

Theorem 1.2.5. *Let $p_1, \ldots, p_r$ be a set of distinct primes, and let f be multiplicative. Then for positive integers $a_1, \ldots, a_r$, we have*

$$f(p_1^{a_1} \cdots p_r^{a_r}) = f(p_1^{a_1}) \cdots f(p_r^{a_r})$$

.

This is a singularly useful statement, because for any multiplicative function f and any positive integer n, it allows us to find $f(n)$ by breaking down n according to its unique prime factorization. That is to say, to define a multiplicative function, it suffices to define it on powers of primes. Moreover, for a completely multiplicative fuction, it suffices to define it on just the primes.

Although we already have a formula stated for the divisor function, $d(n)$, we have not actually proven that it holds for all positive integers n, or that it is, in fact, multiplicative. To do so, let us first properly state the definition of the divisor function.

Definition 1.2.6. For any positive integer n, denote by $d(n)$ the number of positive divisors of n. We call this the *divisor function*.

First, we will show that $d(n)$ is, in fact, multiplicative. To do this, we introduce the following general theorem for multiplicative functions.

Theorem 1.2.7. *If f is a multiplicative function, then $F(n) = \sum_{d|n} f(d)$ is also multiplicative.*

Remark 1.2.8. It is clear from the definition of the divisor function that, through some abuse of notation, $d(n) = \sum_{d|n} 1$. Since 1 is clearly multiplicative, it will follow immediately from the theorem that $d(n)$ is also multiplicative.

Proof of Theorem 1.2.7. Let $F(n) = \sum_{d|n} f(d)$ for some multiplicative function f. (For the rest of this proof, d represents individual divisors, *not* the divisor function.) Then

$$F(mn) = \sum_{d|mn} f(d).$$

Moreover, if m and n are coprime, then we may separate the divisors of mn into divisors of m and divisors of n, and products thereof. Thus, we may rewrite $F(mn)$ as follows.

$$F(mn) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2).$$

Since $\gcd(m, n) = 1$, we know $\gcd(d_1, d_2) = 1$ as well. So, since f is multiplicative,

$$\begin{aligned} F(mn) &= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1) f(d_2) \\ &= \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) \\ &= F(m)F(n) \end{aligned}$$

□

The next result follows immediately.

Corollary 1.2.9. *The divisor function, $d(n)$ is multiplicative.*

We may now construct our original formula for $d(n)$ by observing its behavior over powers of primes, as allowed by Theorem 1.2.5. It is easy to see that for any prime p, we have $d(p) = 2$. It is also apparent that for any prime p and any positive number a, we have $d(p^a) = a + 1$. Notice if $a = 1$, we still have $d(p^1) = 1 + 1 = 2$ as desired.

Example 1.2.10. Let $p = 2$. As with any prime, 2 has two divisors: 1 and itself. so $d(2) = 2$. Suppose, now, that we take some $a > 1$. For instance, take $a = 4$. Then we find the divisors of $2^4 = 16$ by considering 2^i for $0 \leq i \leq a$, which is to say for $a + 1$ values of i. In this case, we have: 2^0, 2^1, 2^2, 2^3, and 2^4. Since 1, 2, 4, 8, and 16 are indeed the complete set of divisors for 16, we see that $d(2^4) = 5 = 4 + 1$ as desired.

Indeed, since we have $d(p^a) = a+1$ for any p and a, our original formula follows immediately from Theorem 1.2.5, and we state this as follows.

Theorem 1.2.11. *Let d denote the divisor function as defined previously. Let n be some positive integer with $n = \prod_{i=1}^{r} p_i^{a_i}$ as its prime factorization. Then*

$$d(n) = \prod_{i=1}^{r} (a_i + 1).$$

Another important multiplicative function which will turn up later is the Euler-phi function, which is defined as follows.

Definition 1.2.12. The *Euler-phi function*, denoted $\phi(n)$ is defined to be the the number of positive integers up to, but not exceeding, n that are coprime with n.

We will take for granted that the Euler-phi function is multiplicative and instead concentrate on deriving the general form. In particular, in the case of ϕ, we may define it over powers of primes by simple counting arguments.

Theorem 1.2.13. *If p is a positive integer, then p is prime if and only if $\phi(p) = p - 1$.*

Proof. If p is prime, then every positive integer k with $1 \leq k < p$ is coprime to p and so $\phi(p) = p-1$. If p is not prime, then $p = 1$ or p is composite. Since $\phi(1) = 1$, $\phi(p) \neq p - 1$ for $p = 1$. Suppose p is composite. Then there is some positive integer $1 < d < p$ with $d|p$, hence $\gcd(d, p) = d \neq 1$. So for p composite, we have $\phi(p) \leq p - 2$, which completes the proof. □

Theorem 1.2.14. *Let p be prime, and let a be a positive integer. Then $\phi(p^a) = p^a - p^{a-1}$.*

Proof. For a positive integer less than p^a to share a factor with p^a, that integer must be divisible by p. So let us count the integers kp between 1 and p^a. There

are exactly p^{a-1} of these. Thus, there are $p^a - p^{a-1}$ integers less than p^a that do not share a factor with p^a. The result follows. □

Theorem 1.2.15. *Let n be a positive integer so that $n = \prod_{i=1}^{r} p_i^{a_i}$. Then*

$$\phi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Proof. Since ϕ is multiplicative, we have

$$\phi(n) = \prod_{i=1}^{r} \phi(p_i^{a_i}).$$

By the last theorem, we have for each i

$$\phi(p_i^{a_i}) = p_i^{a_i} - p_i^{a_i - 1} = p_i^{a_i} \left(1 - \frac{1}{p_i}\right).$$

Thus we have

$$\begin{aligned} \phi(n) &= \prod_{i=1}^{r} p_i^{a_i} \left(1 - \frac{1}{p_i}\right) \\ &= \left(\prod_{i=1}^{r} p_i^{a_i}\right) \left(\prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)\right) \\ &= n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right). \end{aligned}$$

□

In addition to the divisor function and the Euler-phi function, which have been showcased above, there are a number of commonly studied multiplicative functions. One commonly discussed example is the *sum of divisors function*, denoted $\sigma(n)$, whose name is self-explanatory. A common problem for σ involves perfect numbers n, for which $\sigma(n) = 2n$. For example, 6 is a perfect number, since $\sigma(6) = 1 + 2 + 3 + 6 = 12$. However, for now we will leave the topic of multiplicative functions and move on to the history of the problems at hand.

1.3 History of the Ruth-Aaron Pairs

Recall that for $n = \prod_i p_i^{a_i}$,

$$S(n) = \sum_{i=1}^{r} a_i p_i,$$

and

$$P(n) = \sum_{i=1}^{r} p_i.$$

On April 8, 1974, Hank Aaron hit his 715th home run, thus surpassing Babe Ruth's career home run record of 714, which in turn was set in 1935, nearly 40 years earlier. With $S(n)$ defined as above, we notice:

$$S(714) = S(2 \cdot 3 \cdot 7 \cdot 17) = 2 + 3 + 7 + 17 = 29$$
$$S(715) = S(5 \cdot 11 \cdot 13) = 5 + 11 + 13 = 29$$

Thus $n = 714$ is a solution to the equality $S(n) = S(n+1)$. That is to say, the prime factors of these consecutive integers have the same sum. If we used $P(n)$ instead of $S(n)$ above, we would get the same result, since the multiplicity of each prime above is 1.

That same year, with the excitement of Hank Aaron's achievement still fresh, Carl Pomerance [9] decided to look for more of these "Ruth-Aaron Pairs." He found 26 pairs less than 20,000 with a computer search—the smallest was $(5, 6)$, and the largest $(18490, 18491)$—and conjectured these pairs to be infinite by way of a set of polynomials with appropriate solutions that satisfy Schinzel's Conjecture. Pomerance's conjecture, however, remains open to this day.

Nelson, et. al. [9] also suggested RAP's to be sparse. This was proved, moreover, by Erdös and Pomerance [3] in 1978. They also provided the following upper bound for RAP's: For large x,

$$\#\{n | n \leq x, S(n) = S(n+1)\} = O\left(\frac{x(\ln\ln x)(\ln\ln\ln x)}{\ln x}\right).$$

This bound can be improved to $O(x/\ln x)$, as with the prime numbers. However, although we know there are infinitely many primes, this bound only shows that

there *might* be infitely many RAP's.

In 1995, Aaron and Erdös received honorary degrees from Emory University for their various contributions. At the ceremony, both men signed a baseball—the same baseball—for Pomerance, thus arguably giving Aaron an Erdös number of 1. (One wonders which of the three was most amused by this fact, although it was most likely Pomerance.)

Despite having already received an autographed baseball, Pomerance continued to work on the topic and in 2002 [10] improved the bound to:

$$\#\{n|n \leq x, S(n) = S(n+1)\} = O\left(\frac{x(\ln\ln x)^4}{(\ln x)^2}\right),$$

thus establishing that the sum of the reciprocals of all RAN's is bounded, so that these numbers are sparser than the primes. In particular, we have

$$\sum_{n \text{ an RAN}} \frac{1}{n} \approx 0.4207.$$

In Chapter 2, we will examine an analogous question for Ruth-Aaron Pairs of the Second Kind (RAP2's); which is to say, we will be examining solutions to the equation $P(n) = P(n+1)$.

1.4 Of Divisors and Prime Factors

Letting $d(n)$ denote the divisor function mentioned earlier, let us note that $d(2) = d(3) = 2$ and $d(14) = d(15) = 4$. These are the first two solutions to the equality

$$d(n) = d(n+1).$$

In 1952, Erdos and Mirsky [2] asked whether there exist infinitely many integers n such that $d(n) = d(n+1)$. In the 1970's, Vaughan [14], as well as Halberstam and Richert [4], apparently linked this problem in difficulty with solving the Twin Prime Conjecture. This, fortunately, turned out not to be the case. In 1983, Spiro [13] showed that $d(n) = d(n+5040)$ occurs infinitely often; and, although the difference of 5040 arose from difficulties in dealing with powers of the first few primes, this discovery constituted significant progress toward solving the original question.

In 1984, Heath-Brown [5] adapted Spiro's argument in a journal article to deal with small primes In that article, he presented the following theorem:

Theorem. *There are infinitely many integers n such that $d(n) = d(n+1)$. Moreover, for large x, the number of such $n \leq x$ is of order at least $x(\log x)^{-7}$.*

The proof, which will be examined in Chapter 3, is essentially an application of a sieve method. Thus, although it proves existence and minimum frequency, the proof is nonconstructive. This 1984 proof, moreover, was modified in 2003 by Schlage-Puchta [12] to show that $\omega(n) = \omega(n+1)$ infinitely often. The aforementioned proof, which will be covered in Chapter 4, does not make any special statement of frequency.

Chapter 2

Ruth-Aaron Pairs of the Second Kind

2.1 Preliminaries

Let us begin by formally defining some of what was mentioned earlier.

Definition 2.1.1. For $n = \prod_{i=1}^{r} p_i^{a_i}$, we define

$$S(n) := \sum_{i=1}^{r} a_i p_i.$$

Note this is the sum of the prime factors of n, counting multiplicity.

Definition 2.1.2. For $n = \prod_{i=1}^{r} p_i^{a_i}$, we define

$$P(n) := \sum_{i=1}^{r} p_i.$$

Note this is the sum of the prime factors of n, not counting multiplicity.

Example 2.1.3. To demonstrate the difference between these two functions, let $n = 9$ which has one prime factor, namely 3, with multiplicity 2. Then $S(9) = 2 \cdot 3 = 6$, whereas $P(9) = 3$.

Definition 2.1.4. A Ruth-Aaron pair (RAP) is a pair of consecutive integers $(n, n+1)$ such that $S(n) = S(n+1)$. A Ruth-Aaron pair of the second kind (RAP2), similarly, is a pair $(n, n+1)$ such that $P(n) = P(n+1)$

Example 2.1.5. Some pairs, including $(714, 715)$, the original RAP, and $(5, 6)$ satisfy both conditions and are thus both RAPs and RAP2s. However, this usually happens in the trivial case when the prime factorizations have no repeated primes. In fact, the smallest nontrivial pair occurs at $n = 7,129,999$. On the other hand, $(24, 25)$ is an RAP2, since $P(24) = 2 + 3 = 5 = P(25)$; but it not an RAP, since $S(24) = 3 \cdot 2 + 3 = 9$, whereas $S(25) = 2 \cdot 5 = 10$.

This chapter focuses on the set of RAP2s, because they possess a distinct advantage over the standard set of RAPs in one sense. Namely, because the function $P(n)$ does not take the multiplicity of prime factors into account, one can classify certain sets of RAP2s *by prime factors alone* and then proceed to computationally determine some or all of the elements of a given class. This will be further explained later in this chapter, but first we need some tools.

2.2 Cyclotomic Polynomials

Later in this chapter, we will require certain properties of cyclotomic polynomials in order to manipulate our chosen prime factorizations for n and $n + 1$.

Definition 2.2.1. Cyclotomic polynomials, denoted $\Phi_d(x)$, where d is a positive integer, can be defined recursively as follows.

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Example 2.2.2. The first few cyclotomic polynomials are:
$\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, $\Phi_3(x) = x^2 + x + 1$, and $\Phi_4(x) = x^2 + 1$.

Remark 2.2.3. If $k > 1$, notice that $\Phi_1(k) = k - 1 > 0$. It is easy to see that $\Phi_2(k)$ and $\Phi_4(k)$ are also strictly positive. Notice that $k^8 - 1 = \Phi_1(k)\Phi_2(k)\Phi_4(k)\Phi_8(k)$. Since the product is clearly positive, and since three of the terms are positive, it follows that $\Phi_8(k)$ is also strictly positive. Similarly, it can be shown by induction that for $k > 1$, we have $\Phi_m(k) > 0$ for any $m > 0$.

Having said that, it also helps to have a more direct definition.

Definition 2.2.4. The m^{th} cyclotomic polynomial, denoted $\Phi_m(x)$, is also defined

by

$$\Phi_m(x) = \prod_{\substack{k=1 \\ (k,m)=1}}^{m-1} (x - e^{2\pi ik/m}).$$

The next two lemmas are derived by Ianucci and Mintos [7], who are the authors of the source for this chapter, from theorems of Nagell [8], although we do require a definition first.

Definition 2.2.5. Let m and n be coprime integers. Then the order of m modulo n, denoted $e_n(m)$, is defined so that $m^{e_n(m)} \equiv 1 \pmod{n}$ and so that $h = e_n(m)$ is the smallest positive integer for which this happens.

Remark 2.2.6. By Fermat's Little Theorem, we know $h = e_n(m)|\phi(n)$, where ϕ is the Euler-phi function. In particular, if n is prime, then $h|n-1$.

Lemma 2.2.7. *Let p and q be odd primes, m a positive integer, $h = e_p(q)$ (order of q modulo p). Then $p|\Phi_m(q)$ if and only if $m = hp^j$ for some integer $j \geq 0$. If $j > 0$ then $p||\Phi_m(q)$.*

Example 2.2.8. Let $p = 3$ and $q = 5$, so that $h = e_3(5) = e_3(2) = 2$. This lemma implies that $3|\Phi_m(5)$ if and only m equals 2 times some nonnegative power of 3. Notice this allows for $m = 2$ as well as $m = 6, 18, \cdots$. Indeed, we have $\Phi_2(5) = 6$, $\Phi_6(5) = 21$, and $\Phi_{18}(5) = 15,501$, each of which is divisible by 3.

Lemma 2.2.9. *Let q be an odd prime and let m be a positive integer. Then $2|\Phi_m(q)$ if and only if $m = 2^j$ for some integer $j \geq 0$. If $j > 1$ then $2||\Phi_{2^j}(q)$.*

Example 2.2.10. Let $q = 3$. Here, we see that $\Phi_m(q)$ is even if and only if $m = 2^j$ is some power of 2. If $m = 4$, for instance, we have $\Phi_4(3) = 3^2 + 1 = 10$, which is indeed even. Notice also that 4 is a strictly positive power of 2 and that we also have $2||10 = \Phi_4(3)$ as per the lemma. Alternatively, suppose $m = 3$. Then we get $\Phi_3(3) = 3^2 + 3 + 1 = 13$, which is not even, as predicted by the Lemma.

Remark 2.2.11. Notice for the second lemma that the parity of $\Phi_m(q)$ does not actually depend on the choice of q.

Lemma 2.2.12. *For a prime q and an integer $m > 0$, $\Phi_m(q) \geq (q-1)^{\phi(m)}$, where ϕ is the Euler-phi function.*

Proof. Let q be prime, and let m be a nonnegative number. By the second definition for cyclotomic polynomials,

$$\Phi_m(q) = \prod_{\substack{k=1 \\ (k,m)=1}}^{m-1} (q - e^{2\pi ik/m}).$$

Since $\Phi_m(q)$ is strictly positive by our previous remark, we may write

$$\Phi_m(q) = \prod_{\substack{k=1 \\ (k,m)=1}}^{m-1} \left|q - e^{2\pi ik/m}\right|.$$

Because $|e^{2\pi ik/m}| = 1$ for all $1 \leq k \leq m-1$, it follows from the Triangle Inequality that $|q - e^{2\pi ik/m}| \geq q - 1$. Finally, since $\phi(m)$ is precisely the number of $1 \leq k \leq m-1$ for which $(k, m) = 1$, the result follows. □

We now have the tools required for the rest of the chapter, so we will proceed to the problem.

2.3 RAP2s of the form $(2^a p^b, q^c)$

As previously stated, $P(n)$ ignores multiplicies in the prime factors of a given n. As such, we can construct classes of RAP2s as follows: First, assume two numbers, n and $n+1$, to be consecutive. Next, choose prime factors for those two numbers so that their primes have the same sum–i.e. so that $P(n) = P(n+1)$. Then, if possible, *find* the powers of those primes for which the assumptions hold; and if not, determine necessary or likely properties in order to allow an efficient computer search.

In particular, since consecutive integers come in pairs of even and odd, one of the two must have 2 as a factor, and the other must not. As a result, since subtracting 2 from a sum does not affect the parity, the sum of the *odd* prime factors for n and $n+1$ must both be even or both be odd. More to the point, the numbers of odd primes dividing n and $n+1$ are both even or both odd.

Let us focus on the odd case. Better yet, let us begin with the case where both numbers have precisely 1 odd prime, and where only one of them is divisible by 2.

We have two possible forms: $(2^a p^b, q^c)$ and $(q^c, 2^a p^b)$. Notice that in each case we also have $p+2=q$, since the pair must satisfy $P(n)=P(n+1)$.

We begin with the form $(2^a p^b, q^c)$, which turns out to be the easier case to solve.

Notice that

$$2^a p^b = q^c - 1, \tag{2.1}$$

since we begin with consecutive integers. Setting $p = q-2$, we see that

$$2^a p^b \geq 2(q-2) = q + (q-4) \geq q + (5-4) > q - 1.$$

So we need $c > 1$ in (2.1). Setting $q = p+2$ in turn yields

$$\begin{aligned} 2^a p^b &= q^c - 1 \\ &= (q-1)(q^{c-1} + q^{c-2} + \cdots + q + 1) \\ &= (p+1)(q^{c-1} + q^{c-2} + \cdots + q + 1). \end{aligned}$$

Since $(p, p+1) = 1$, we must have $p+1 | 2^a$, and so $p+1 = 2^t$ for some integer $t \leq a$. Thus

$$p = 2^t - 1 \text{ and } q = 2^t + 1,$$

and it follows immediately that $t = 2$, $p = 3$, and $q = 5$. To see this, note that the powers of 2 modulo 3 are limited to 1 and 2, which means that one of p and q must be divisible by 3.

So now we have

$$2^a 3^b = 5^c - 1,$$

with $c > 1$. Powers of 5 alternate between 1 and 2 modulo 3 for odd and even powers, respectively. Since $5^c \equiv 1 \pmod 3$, we know $2|c$ which we denote by $c = 2\gamma$. Hence,

$$2^a 3^b = (5^\gamma + 1)(5^\gamma - 1).$$

Trivially, $5^\gamma + 1 \equiv 2 \pmod 4$, so we know $2 || 5^\gamma + 1$. Moreover, $5^\gamma + 1 \geq 6 > 2$, so we also have $3 | 5^\gamma + 1$. Furthermore, since $(5^\gamma + 1, 5^\gamma - 1) = 2$, we also know that $3 \nmid 5^\gamma - 1$. With these observations, we can completely factor the right-hand side of the equation above.

$$5^\gamma - 1 = 2^{a-1}.$$
$$5^\gamma + 1 = 2 \cdot 3^b.$$

We also notice that γ is odd (otherwise, we would have $3|5^\gamma - 1$). Suppose moreover that $\gamma > 1$. Then

$$5^\gamma - 1 = (5-1)(5^{\gamma-1} + 5^{\gamma-2} + \cdots + 5 + 1).$$

The second factor on the right is both odd and greater than 1. This contradicts the observation that $5^\gamma - 1 = 2^{a-1}$. Therefore, $\gamma = 1$ and $c = 2$. It immediately follows that $a = 3$ and $b = 2$, yielding the identity $2^3 \cdot 3 = 5^2 - 1$.

We now summarize this section by the following theorem.

Theorem 2.3.1. *If for some positive integer n, $(n, n+1)$ is an RAP2 with the form $(2^a p^b, q^c)$, then n and $n+1$ must be equal to 24 and 25, respectively. That is to say, $(24, 25)$ is the only RAP2 of this form.*

2.4 RAP2s of the form $(q^c, 2^a p^b)$

We now examine the second case. Again we note that these are consecutive integers. So,

$$2^a p^b = q^c + 1 \tag{2.2}$$

Moreover, according to the recursive definition of cyclotomic polynomials, we may write

$$2^a p^b = q^c + 1 = \frac{q^{2c} - 1}{q^c - 1} = \prod_{d|2c,\ d\nmid c} \Phi_d(q). \tag{2.3}$$

2.4.1 Proving $c = 2^m$

As with the previous section, we want to determine possible values for the exponents a, b, and c. We begin by looking at all possibilities for c. Write $c = 2^m s$, where s

is odd. We have three cases for s: Either $s = 1$, s is prime, or s is composite. We shall examine each case.

Let $h = e_p(q)$ be the order of q modulo p so that $q^h \equiv 1 \pmod{p}$. Since $q = p+2$, $h = e_p(2)$. Since the left-hand side of (2.3) has only 2 and p as prime factors, we have for $\Phi_d(q)$ in the product on the right-hand side either $2|\Phi_d(q)$ or $p|\Phi_d(q)$. If $2|\Phi_d(q)$ then $d = 2^k$ for $k \geq 0$ by Lemma 2.2.9. In particular, for this case, since $d|2c$ and $d \nmid c$, we have $d = 2^{m+1}$. If $p|\Phi_d(q)$, then $d = hp^{j_d}$ for some $j_d \geq 0$. Since we only consider d for which $d \nmid c$ and $d|2c$, we have $2^{m+1}||d$, and hence $2^{m+1}||h$.

Proposition 2.4.1. *Set $c = 2^m s$ as above and assume that $s > 1$. Then s is not prime.*

Proof. Suppose by way of contradiction that s is prime. Since $2c = 2^{m+1}s = hp^j$ from before (and because $s \neq 1$), we know that either $j = 0$ or $j = 1$. In the second case, we get $h = 2^{m+1}$ and $s = p$. Since $j > 0$, we have $2 \nmid \Phi_{2c}(q)$ by Lemma 2.2.9 and $p||\Phi_{2c}(q)$ by Lemma 2.2.7, which implies that $\Phi_{2c}(q) = p$ by (2.3). However, according to Lemma 2.2.12, $\Phi_{2c}(q) > q - 1 > p$, so that case fails.

Trying the first case ($j = 0$), we have $h = 2c = 2^{m+1}s$. Given $h = 2^{m+1}s$, it follows from (2.3) that

$$2^a p^b = \Phi_{2^{m+1}s}(q)\Phi_{2^{m+1}}(q). \tag{2.4}$$

If $m > 0$, then we have $p \nmid \Phi_{2^{m+1}}(q)$ by Lemma 2.2.7, $2||\Phi_{2^{m+1}}(q)$ by Lemma 2.2.9, and $\Phi_{2^{m+1}}(q) > 2$ by Lemma 2.2.12, which is simply impossible. Hence, (2.4) is only possible if $m = 0$, and thus $h = 2s$, which turns (2.4) into

$$2^a p^b = \Phi_2(q)\Phi_{2s}(q).$$

This in turn implies $2^a = \Phi_2(q) = q + 1$, hence $q = 2^a - 1$. Otherwise, $2|\Phi_{2s}(q)$, which contradicts Lemma 2.2.9. This gives us $p = q - 2 = 2^a - 3$. Since $a > 2$ (otherwise $p < 2$), we have $p \equiv 5 \pmod{8}$, which means 2 is not a quadratic residue of p. This in turn yields $2^{(p-1)/2} \equiv -1 \pmod{p}$ by Euler's criterion.

This implies that $h = e_p(2) = p - 1$, and since $p - 1 = 2^a - 4$, which is divisible by 2^2 (since $a > 2$), we have $2^2|e_p(2) = h$. However, since $h = 2s$, where s is odd, it follows that $2||h$, which is a contradiction. □

Having shown s is not prime, we proceed to show that s is not composite, which will leave only $s = 1$.

Proposition 2.4.2. *Set $c = 2^m s$ as before. If s is composite, then $s = p^k$ for some $k > 1$.*

Proof. First notice that equation (2.3) can be rewritten as

$$2^a p^b = \prod_{d|s} \Phi_{2^{m+1}d}(q). \tag{2.5}$$

Let $h = e_p(q) = e_p(2)$. Since the left-hand side of (2.5) has only 2 and p as prime factors, we have in the product on the right-hand side that either $2|\Phi_{2^{m+1}d}(q)$ or $p|\Phi_{2^{m+1}d}(q)$. In particular, $2|\Phi_{2^{m+1}d}(q)$ if and only if $d = 1$. Moreover, by Lemma 2.2.7 we have for each integer $d|s$ with $d > 1$ that $2^{m+1}d = hp^{j_d}$.

Since for $d \neq 1$, we have $2^{m+1}d = hp^{j_d}$ for some $j_d \geq 0$, and since s is assumed to be composite, there is some t such that $1 < t < s$ and $t|s$. So we have

$$2^{m+1}t = hp^{j_t}, \text{ and}$$
$$2^{m+1}s = hp^{j_s}.$$

In particular, this shows that $s/t = p^{j_s - j_t}$ for all such t, which shows that s must be some power of p. □

Having better defined the cases for which s is composite, we may now discount all of them in one fell swoop.

Proposition 2.4.3. *Set $c = 2^m s$ as before. Then s is not composite.*

Proof. Recall that if s is composite, then $s = p^k$ for some $k > 1$ so that $c = 2^m p^k$. Since $2|\Phi_{2^{m+1}p^j}(q)$ if and only if $j = 0$, it follows that $2^a||\Phi_{2^{m+1}}(q)$ and that $\Phi_{2^{m+1}p^j}(q)|p^b$ for $j > 1$. However, by Lemma 2.2.12, we see that $\Phi_{2^{m+1}p^j}(q) > 1$, which means that $p|\Phi_{2^{m+1}p^j}(q)$ whenever $j > 0$. By Lemma 2.2.7, if $j > 0$, then $p||\Phi_{2^{m+1}p^j}(q)$, hence $\Phi_{2^{m+1}p^j}(q) = p$. However, since $q = p + 2$, we know that $\Phi_{2^{m+1}p^j}(q) > p$ by Lemma 2.2.12, which is a contradiction. □

Therefore, with s neither composite nor prime, we are left with one choice.

Proposition 2.4.4. *Set $c = 2^m s$ as before. Then $s = 1$ and $c = 2^m$.*

As a result of this last statement, we may rewrite Equation (2.2.12) as follows.

$$2^a p^b = q^{2^m} + 1. \tag{2.6}$$

2.4.2 Finding m

We must now determine the possibilities for m.

Claim 2.4.5. *With $c = 2^m$ as shown above, $m \in \{0, 1\}$.*

Not surprisingly, the aim of this part of the section is to eliminate all cases $m > 1$, and so we begin by supposing $m > 1$. Then $q^{2^m} \equiv 1 \pmod 4$ since q is odd and $m \geq 1$. This implies $a = 1$, since $q^{2^m} \equiv 3 \pmod 4$ otherwise. Now we have

$$2p^b = q^{2^m} + 1. \tag{2.7}$$

Since $q^{2^m} + 1 = \Phi_{2^{m+1}}(q)$ by nature of Φ, we have $p | \Phi_{2^{m+1}}(q)$. Thus $h = 2^{m+1}$ according to Lemma 2.2.7. Noting that $h = e_p(2)$ is defined to be the order of 2 modulo p, we see that $h | \phi(p)$; in particular, $2^{m+1} | p - 1$. Trivially, we have $p \equiv 1 \pmod{2^{m+1}}$. Also, since $e_p(2) = 2^{m+1}$ and $\Phi_{2^{m+1}}(2) = 2^{2^m} + 1$, we know from Lemma 2.2.7 that

$$p | 2^{2^m} + 1. \tag{2.8}$$

Since $p \equiv 1 \pmod{2^{m+1}}$, we can write $p = 2^{m+1}t + 1$ for some t. Suppose t is odd. Since $2^{2^m} \equiv -1 \pmod p$ by (2.8),

$$2^{(p-1)/2} = 2^{2^m t} = (2^{2^m})^t \equiv (-1)^t \equiv -1 \pmod p.$$

Therefore, $\left(\frac{2}{p}\right) = -1$—namely, 2 is not a quadratic residue modulo p—by Euler's criterion. However, $\left(\frac{2}{p}\right) = 1$ on account of the observation that $m > 1$ implies $p \equiv 1 \pmod 8$. This is a contradiction, and so we must choose t to be even instead, which means that

$$p \equiv 1 \pmod{2^{m+2}}. \tag{2.9}$$

To finish off the case $m > 1$, let us consider the options for b. First, let us suppose $b > 2^m$. Then (2.7) implies

$$\begin{aligned} 2p^{b-2^m} = \frac{2p^b}{p^{2^m}} &= \frac{q^{2^m}}{p^{2^m}} + \frac{1}{p^{2^m}} \\ &= \frac{(p+2)^{2^m}}{p^{2^m}} + \frac{1}{p^{2^m}} \\ &= \left(1 + \frac{2}{p}\right)^{2^m} + \frac{1}{p^{2^m}}. \end{aligned}$$

However, by (2.9), $p > 2^{m+2}$, so that

$$2p^{b-2^m} < \left(1 + \frac{1}{2^m}\right)^{2^m} + 1 < e + 1 < 4.$$

This follows on account of the the fact that the sequence $\{(1 + 1/n)^n\}$, which of course converges to e as $n \to \infty$, is increasing. However, this implies that $2p < 4$, which is clearly a contradiction.

Now we suppose $b < 2^m$. Then applying (2.7) again gives us

$$2 = \frac{(p+2)^{2^m}}{p^b} + \frac{1}{p^b}.$$

The right-hand side can be rewritten so that

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

Hence,

$$2 > (p+2)^{2^m - b} \geq p + 2 > 2.$$

This is also a clear contradiction. Thus we must assume $b = 2^m$, and applying (2.7) yet again yields

$$2p^{2^m} = q^{2^m} + 1. \tag{2.10}$$

Substituting $q = p + 2$ yields

$$p^{2^m} = -p^{2^m} + (p+2)^{2^m} + 1.$$
$$= \sum_{k=1}^{2^m} \binom{2^m}{k} p^{2^m-k} 2^k + 1. \tag{2.11}$$

Recall that $p > 2^{m+2}$ by (2.9). Thus, for each $1 \leq k \leq 2^m$, we have $p^{-k} < 2^{-k(m+2)} \leq 2^{-mk-2}$. Therefore

$$\begin{aligned}
\binom{2^m}{k} p^{2^m-k} 2^k &= \frac{2^m(2^m-1)\cdots(2^m-k+1)}{k!} \cdot p^{2^m-k} 2^k \\
&< \frac{2^{mk}}{k!} \cdot p^{2^m-k} 2^k \\
&= \frac{2^{mk}}{k!} \cdot p^{-k} p^{2^m} 2^k \\
&\leq \frac{2^{mk}}{k!} \cdot 2^{-mk-1} p^{2^m} 2^k \\
&= \frac{1}{2^k} \cdot \frac{1}{k!} \cdot p^{2^m}.
\end{aligned}$$

It follows from (2.11) and by the series expansion for $e^{1/2}$ that

$$p^{2^m} < \sum_{k=1}^{2^m} \frac{1}{2^k} \cdot \frac{1}{k!} \cdot p^{2^m} < p^{2^m}(\sqrt{e} - 1 + \frac{1}{p^{2^m}}) < 0.8 p^{2^m},$$

and now we have our final contradiction in the case of $m > 1$.

2.4.3 Determining the pairs

We now return to (2.6) in the knowledge that $m = 0$ or $m = 1$. If $m = 0$, this becomes

$$2^a p^b = q + 1 = p + 3,$$

which implies $p|3$, forcing $p = 3$ and $q = 5$. This in turn yields $2^a 3^b = 6$ with $a = b = 1$, which gives us the RAP2 $(5, 6)$.

If $m = 1$, on the other hand, we have

$$2^a p^b = q^2 + 1,$$

by (2.6), which implies $a = 1$ since $q^2 \equiv 1 \pmod 4$—again, because q is odd. Hence,

$$2p^b = q^2 + 1 = (p+2)^2 + 1 = p^2 + 4p + 5,$$

which forces $p|5$, hence $p = 5$ and $q = 7$. So we have $2 \cdot 5^b = 50$, and thus $b = 2$, giving us the RAP2 $(49, 50)$.

The method applied in this section was exhaustive; therefore, $(5, 6)$ and $(49, 50)$ are the only RAP2s of the form $(q^c, 2^a p^b)$. By this section and the last, we now have the following theorem:

Theorem 2.4.6. *The only RAP2s* $(n, n+1)$ *with* $\{\omega(n), \omega(n+1)\} = \{1, 2\}$ *are* $(5, 6)$, $(24, 25)$ *and* $(49, 50)$.

2.5 RAP2s of form $(2^{2n}pq, rs)$

In this section, we consider a specific class of RAP2s–namely, RAP2s $(N, N+1)$ with $\omega(N) = 2$ and $\omega(N+1) = 3$. The first three pairs are listed below.

$$(492, 493) = (2^2 \cdot 3 \cdot 41, 17 \cdot 29)$$
$$(2600, 2601) = (2^3 \cdot 5^2 \cdot 13, 3^2 \cdot 17^2)$$
$$(6556, 6557) = (2^2 \cdot 11 \cdot 149, 79 \cdot 2)$$

Notice how wide the spread is between these. In fact, there are only 88 RAP2s of this form for which N is less than 10^9. (Only 18 of these are less than 10^7.) Of these 88, 41–or nearly half, including the first–are of the form $(4pq, rs)$ for odd primes $p < q, r < s$. Another six have the form $(16pq, rs)$, the first of which occurs at $N = 24432$. Three more have the form $(64pq, rs)$.

To summarize, the case $(N, N+1) = (2^a q^b, r^c s^d)$ yields many more solutions than either of the simplest two cases for RAP2s, but those solutions appear to be incredibly sparse. As a result, we cannot tell at a glance whether the number of such solutions is finite or infinite. The author conjectures, much like in the normal RAP case, that the larger problem $P(N) = P(N+1)$ has infinitely many solutions; however, this remains conjecture, as with the original RAP problem.

Nevertheless, since $(N, N+1) = (2^a q^b, r^c s^d)$ yields the first set of RAP2s which *could* be infinite, it is worth paramatrizing these particular solutions for further examination. In particular, since most of the solutions mentioned before have the simpler form $(2^{2n}pq, rs)$, where $n \geq 1$, it is prudent to work with this subset.

For pairs of the form $(2^{2n}pq, rs)$, we have

$$2 + p + q = r + s, \tag{2.12}$$
$$2^{2n}pq + 1 = rs. \tag{2.13}$$

By (2.12), there are integers x, y, and z so that

$$\begin{aligned} r &= x - y, & s &= x + y, \\ p &= x - 1 - z, & q &= x - 1 + z. \end{aligned} \tag{2.14}$$

As a result, we can now work with 3 variables instead of 4. If we substitute (2.14) into (2.13) and simplify, we end up with

$$((2^{2n} - 1)x - (2^{2n} + 1))(x - 1) = (2^n z - y)(2^n z + y).$$

At this point, we would like to find a way to determine which of x, y, z are free variables. Dividing through by $(x - 1)$ gives the following.

$$\frac{(2^{2n} - 1)x - (2^{2n} + 1)}{2^n z - y} = \frac{2^n z + y}{x - 1} = \frac{a}{b}. \tag{2.15}$$

Since a/b represents the fractions above in their lowest terms, $(a, b) = 1$. We cross multiply and rearrange the terms to get

$$\begin{gathered} (2^{2n} - 1)bx + ay - 2^n az = (2^{2n} + 1)b, \\ ax - by - 2^n bz = a. \end{gathered}$$

We then solve for x, y in terms of z, which we may now consider the only free variable, to get:

$$(a^2 + (2^{2n} - 1)b^2)x = 2^{n+1}abz + a^2 + (2^{2n} + 1)b^2, \tag{2.16}$$
$$(a^2 + (2^{2n} - 1)b^2)y = 2^n(a^2 - (2^{2n} - 1)b^2)z + 2ab. \tag{2.17}$$

The authors discovered many possible quotients a/b satisfying (2.15) but noticed that some were especially common. These included $2/1$ and $7/4$ when $n = 1$ is fixed. These turn out to be solutions to the Pell equation $a^2 - 3b^2 = 1$, thus the search was focused on pairs a, b that solve the more general Pell equation

$$a^2 - (2^{2n} - 1)b^2 = 1, \tag{2.18}$$

where $n \geq 1$. Since

$$\begin{aligned} 2a^2 &= a^2 + (2^{2n} - 1)b^2 + a^2 - (2^{2n} - 1)b^2 \\ &= a^2 + (2^{2n} - 1)b^2 + 1, \end{aligned}$$

We know that $a^2 + (2^{2n} - 1)b^2 = 2a^2 - 1$. And since

$$\begin{aligned} a^2 + (2^{2n} + 1)b^2 - 2b^2 &= a^2 + (2^{2n} - 1)b^2 \\ &= 2a^2 - 1, \end{aligned}$$

we know $a^2 + (2^{2n} + 1)b^2 = 2a^2 + 2b^2 - 1$. We may use these observations to simplify (2.16) and (2.17) to

$$\begin{aligned} (2a^2 - 1)x &= 2^{n+1}abz + 2a^2 + 2b^2 - 1, \\ (2a^2 - 1)y &= 2^n z + 2ab. \end{aligned} \tag{2.19}$$

All positive solutions to (2.18) are given by

$$\begin{aligned} a_1 &= 2^n, & b_1 &= 1, \\ a_{j+1} &= 2^n a_j + (2^{2n} - 1)b_j & (j &\geq 1), \\ b_{j+1} &= a_j + 2^n b_j & (j &\geq 1). \end{aligned} \tag{2.20}$$

One can show by induction that $2^n | a_j b_j$ for all $j \geq 1$. So we parametrize z in (2.19). Since y is an integer, we know that $2a^2 - 1 | 2^n z + 2ab$. Also, $2a^2 - 1$ is odd. So we have

$$z \equiv -\frac{2ab}{2^n} \pmod{2a^2-1},$$

which gives us the following form for z for integers $k \geq 0$:

$$z = (2a^2-1)k + 2a^2 - 1 - \frac{2ab}{2^n}$$

Substituting this into (2.16) and (2.17) yields.

$$x = 2^{n+1}abk + 2^{n+1}ab - 2b^2 + 1, \tag{2.21}$$
$$y = 2^n k + 2^n \tag{2.22}$$

and if we substitute these last three equations into (2.14), we derive the following theorem:

Theorem 2.5.1. *Let some $n \geq 1$ be an integer and let a, b be solutions to* (2.18)*, the more general Pell equation used earlier. Then $(2^{2n}pq, rs)$ is a RAP2 if, for an integer $k \geq 0$, the following four quantities are all prime:*

$$\begin{aligned}
p &= 2(2^{n+1}ab - 2a^2 + 1)k + \left(2^{n+1} - 2b^2 - 2a^2 + 1 + \frac{2ab}{2^n}\right), \\
q &= 2(2^{n+1}ab + 2a^2 - 1)k + \left(2^{n+1} - 2b^2 + 2a^2 - 1 - \frac{2ab}{2^n}\right), \\
r &= 2^{n+1}(2ab-1)k + 2^n(2ab-1) - 2b^2 + 1, \\
s &= 2^{n+1}(2ab+1)k + 2^n(2ab+1) - 2b^2 + 1.
\end{aligned}$$

Remark 2.5.2. Notice that $2ab/2^n$ is always an integer as a result of (2.20). Furthermore, the authors substituted $2k$ instead of k to ensure the p, q from the theorem are odd. The numerators retain the term $2ab$, because the Pell sequences have the property $b_{2j} = 2a_j b_j$. One shows by induction that for all n, k, if a_{3j}, b_{3j} are used in Theorem 2.5.1, then at least one of the four values is divisible by 3 (resulting in no RAP2).

The authors found by way of a computer search that 149 RAP2s of the form $(2^{2n}pq, rs)$ less than 2^{34} exist, and of these 116 correspond to $n = 1$. Of these, 16 correspond to $a_1 = 2, b_1 = 1$. Further statistics are available in the original article.

Chapter 3

Solutions to $d(z) = d(z+1)$

3.1 Outline

Recall the divisor function, $d(z)$, which is defined to be the number of divisors of z, a positive integer. This chapter will focus on a proof by Heath-Brown [5] of the following theorem, which he presented in 1984.

Theorem 3.1.1. *There are infinitely many integers z such that $d(z) = d(z+1)$. Moreover, for large x, the number of such $z \leq x$ is of order at least $x(\log x)^{-7}$.*

The proof uses the following sieve, which is a weak version of a result by Halberstam and Richert [4].

Lemma 3.1.2. *Let N be a natural number greater than 1, and let $a_i, b_i, 1 \leq i \leq N$ be integers satisfying*

$$\prod_{i=1}^{N} a_i \prod_{1 \leq t < s \leq N} (a_t b_s - a_s b_t) \neq 0. \tag{3.1}$$

Suppose also that

$$\prod_{i=1}^{N} (a_i n + b_i) \tag{3.2}$$

has no fixed prime factor—that is to say: no prime divides the product above for all integers n. Then, for any natural number r sufficiently large, and depending only on N, there is a positive number δ such that, as $x \to \infty$,

$$\#\left\{n; 1 \leq n \leq x, \prod_{i=1}^{N}(a_i n + b_i) = P_r\right\} \geq \delta \frac{x}{(\log x)^N}\left(1 + O((\log x)^{-1/2})\right), \quad (3.3)$$

where P_r is some p_r-smooth number, and where δ and the O constant depend only on r, N and on the a_i's and b_i's.

Remark 3.1.3. The weakening in the lemma involves weakening the condition for the lower bound of r. However, for small N, an improvement by Xie [15] leads to a stronger set of bounds on r than does the original lemma. In particular, for $N = 7$, we may take $r = 27$. This pair will eventually be used both to prove the main theorem and to give us the lower bound of order $x(\log x)^{-7}$ for the frequency.

By using the pair $(N, r) = (2, 14)$—also from Xie—we may construct a relatively simple example for $N = 2$.

Example 3.1.4. Let $a_1 = a_2 = 1$, and let $b_1 = -1$ and $b_2 = 1$. Clearly this satisfies Property (3.1), since the product is 2. It follows from the lemma and the value of r given by Xie that the number of positive integers n no larger than x as $x \to \infty$ for which $n^2 - 1$ is $p_{14}-$smooth, where $p_{14} = 43$ is the 14^{th} prime, is of order at least $O(x(\log x)^{-2})$.

Given this sieve, what remains for the proof is to find a set of linear equations that will satisfy the sieve and also satisfy $d(z) = d(z + 1)$, and also to confirm the result $N = 7$ above. In order to achieve this, we require the following "Key Lemma" from Heath-Brown's proof.

Lemma 3.1.5. *For any positive integer N there exist N distinct natural numbers a_n with the following properties. If $m \neq n$ and $d_{mn} = a_m - a_n$, then*

$$d_{mn} = \gcd(a_m, a_n) \quad (3.4)$$

Moreover,

$$d(a_m)d\left(\frac{a_n}{|d_{mn}|}\right) = d(a_n)d\left(\frac{a_m}{|d_{mn}|}\right). \quad (3.5)$$

This key lemma takes care of small primes and allows adaptation of the sieve method employed by Spiro, which gave the result for $d(z) = d(z + 5040)$. The lemma will be proven in later sections so as not to distract the reader from the

main problem. In the following section, we will outline the proof of the theorem. In particular, we will use the Key Lemma to construct a set of linear functions which not only allow us to create instances of $d(z) = d(z+1)$, but which satisfy the sieve and thereby allow us to create these instances infinitely often.

3.2 Proof of the Theorem

Let a_n, d_{mn} be as in Lemma 3.1.5, and let $A = N! \prod a_n$. Let $p_1, \ldots, p_N$ be distict primes, none of which divides A. We define

$$r_n = p_n^{d(a_n)-1},$$

so that

$$d(a_n) = d(r_n), \tag{3.6}$$

whenever $1 \leq n \leq N$.

We may illustrate this construction with a trivial case.

Example 3.2.1. Let $N = 2$, and set

$$a_1 = 2$$
$$a_2 = 3.$$

It is clear that 2 and 3 satisfy the properties (3.4) and (3.5). So we set $A = N! \prod a_n = 2 \cdot 2 \cdot 3 = 12$ and choose $p_1 = 5$ and $p_2 = 7$ so that our chosen primes do not divide $N!$ or either a_n, and thus do not divide A. Since $d(2) = d(3) = 2$, we set

$$r_1 = p_1^{2-1} = 5,$$
$$r_2 = p_2^{4-1} = 7,$$

and we note that $d(a_n) = d(r_n)$ for each n.

By the Chinese Remainder Theorem, the system of simultaneous congruences

$$a_n A x + 1 \equiv r_n \pmod{r_n^2},$$

has a solution with $1 \leq n \leq N$. Noting that $(a_n A, r_n^2) = 1$, let X be any fixed solution. We set Y_n so that

$$a_n AX + 1 = r_n Y_n, \tag{3.7}$$

with

$$(Y_n, Ar_n) = 1. \tag{3.8}$$

Writing $R = \prod r_n$ and $R_n = R/r_n$, we define

$$F_n(x) = a_n AR_n Rx + Y_n. \tag{3.9}$$

Remark 3.2.2. Note that the coefficients of $F_n(x)$ will correspond with the coefficients in (3.1), and in particular, the N from the statements of both lemmas will correspond.

Example 3.2.3. Continuing with the a_n and r_n defined in the previous example, we begin by solving the congruences

$$\begin{aligned} 2 \cdot 12x + 1 &\equiv 5 \pmod{5^2}, \\ 3 \cdot 12x + 1 &\equiv 7 \pmod{7^2}. \end{aligned}$$

The smallest positive solution to this system is $x = 1021$, and so we set $X = 1021$, although X need not be positive. Now we want to find Y_1 and Y_2 so that

$$\begin{aligned} 24 \cdot 1021 + 1 &= 5Y_1, \\ 36 \cdot 1021 + 1 &= 7Y_2. \end{aligned}$$

Clearly, $Y_1 = 4901$ and $Y_2 = 5251$, and we see that neither of these is divisible by 2 or 3, so (3.8) holds. We set $R = r_1 r_2 = 35$ and in this instance, $R_n = R/r_n$ simply yields $R_1 = r_2 = 7$ and $R_2 = r_1 = 5$. Thus, we have our linear functions defined according to (3.9) as follows.

$$\begin{aligned} F_1(x) &= 5880x + 4901, \\ F_2(x) &= 6300x + 5251. \end{aligned}$$

In particular, note that $(5880 \cdot 5251 - 4901 \cdot 6300) = -420 \neq 0$. Hence, the coefficients

of $F_1(x)$ and $F_2(x)$ do indeed satisfy (3.1).

Proposition 3.2.4. *For F_n, A, and R as defined above,*

$$(F_n(x), AR) = 1. \tag{3.10}$$

Proof. If $p|A$ then by (3.8) $p \nmid Y_n$, hence by (3.9) $p \nmid F_n(x)$. Similary, since $p_n|r_n$, (3.8) and (3.9) also show that $p_n \nmid F_n(x)$. If $m \neq n$ and $p_m|F_n(x)$, then $p_m|Y_n$ by (3.9), since $p_m|R$. However, (3.7) now gives us

$$a_n AX + 1 = r_n Y_n \equiv 0 \pmod{p_m},$$

since $p_m|Y_n$, and

$$a_m AX + 1 = r_m Y_m \equiv 0 \pmod{p_m},$$

since $p_m|r_m$. Putting these together yields

$$a_n AX + 1 \equiv a_m AX + 1 \equiv 0 \pmod{p_m}.$$

Since $p_m|AX$, it follows that $p_m|(a_m - a_n) = d_{mn}$, which implies $p_m|a_m$ by Lemma 3.1.5. However, this contradicts our choice of p_m, which completes the proof. □

Proposition 3.2.5. *If $a_m > a_n$,*

$$\frac{a_m}{d_{mn}} r_n F_n(x) = 1 + \frac{a_n}{d_{mn}} r_m F_m(x).$$

Proof. This can be verified from (3.7) and (3.9) as follows.

$$\begin{aligned}
\frac{a_m}{d_{mn}} r_n F_n(x) &= \frac{a_m}{d_{mn}} r_n (a_n A R_n R x + Y_n) \\
&= \frac{a_m}{d_{mn}} (a_n A R^2 x + r_n Y_n) \\
&= \frac{a_m}{d_{mn}} (a_n A R^2 x + a_n A X + 1) \\
&= \frac{a_n}{d_{mn}} \left(a_m A R^2 x + a_m A X + \frac{a_m}{a_n} \right) \\
&= \frac{a_n}{d_{mn}} \left(a_m A R^2 x + a_m A X + 1 + \frac{a_m}{a_n} - 1 \right) \\
&= \frac{a_n}{d_{mn}} \left(a_m A R^2 x + r_m Y_m + \frac{a_m}{a_n} - 1 \right) \\
&= \frac{a_n}{d_{mn}} r_m \left(a_m A R_m R x + Y_m + \frac{\frac{a_m}{a_n} - 1}{r_m} \right) \\
&= \frac{a_n}{d_{mn}} r_m \left(F_m(x) + \frac{a_m - a_n}{a_n r_m} \right) \\
&= 1 + \frac{a_n}{d_{mn}} r_m F_m(x).
\end{aligned}$$

Moreover, by (3.10) (and the definition of r_n), $a_n/d_{mn}, r_n$, and $F_n(x)$ are pairwise coprime. Therefore, by (3.6),

$$\begin{aligned}
d\left(\frac{a_n}{d_{mn}} r_m F_m(x) \right) &= d\left(\frac{a_n}{d_{mn}} \right) d(a_m) d(F_m(x)), \text{ and} \\
d\left(1 + \frac{a_n}{d_{mn}} r_m F_m(x) \right) &= d\left(\frac{a_m}{d_{mn}} r_n F_n(x) \right) \\
&= d\left(\frac{a_m}{d_{mn}} \right) d(a_n) d(F_n(x)).
\end{aligned}$$

□

Example 3.2.6. It can be difficult to visualize these properties for arbitrary x. For fixed x, however, this is fairly straight-forward. Let $F_1(x) = 5880x + 4901$ and $F_2(x) = 6300x + 5251$ as before. Set $d_{12} = |a_1 - a_2| = 1$. Fix $X = 0$ so that $F_1(X) = 4901$ and $F_2(X) = 5251$. We now have

$$\begin{aligned}
\frac{a_1}{d_{12}} r_2 F_2(X) &= 2 \cdot 7 \cdot 5251 = 73,514, \\
\frac{a_2}{d_{12}} r_1 F_1(X) &= 3 \cdot 5 \cdot 4901 = 73,515,
\end{aligned}$$

and the difference is 1, as predicted.

An immediate result of Lemma 3.1.5 follows:

Corollary 3.2.7. *For $m \neq n$,*

$$d\left(\frac{a_n}{d_{mn}} r_m F_m(x)\right) = d\left(1 + \frac{a_n}{d_{mn}} r_m F_m(x)\right),$$

whenever

$$d(F_m(x)) = d(F_n(x)). \tag{3.11}$$

To prove the main theorem, all that remains is to find solutions to (3.11) by way of the sieve method.

Proposition 3.2.8. *Requiring that each factor $a_i n + b_i$ be square-free does not affect the lower bound in* (3.3).

Proof. According to the proof of Lemma 3.1.2 [4], there exists a constant $\eta > 0$ such that every prime factor of $a_i n + b_i$ satisfies $p \geq x^\eta$. Define K_s to be the the number of n for which $a_i n + b_i$ contains a square. Since $p^2 | a_i n + b_i$ implies $p \ll x^{1/2}$, it follows that

$$K_s \ll \sum_{x^\eta \leq p \leq x^{1/2}} x p^{-2} \ll x^{1-\eta}.$$

Thus the instances of such n are sufficiently few. □

Proving the main theorem requires the application of Lemma 3.1.2 to the functions $F_n(x)$ for $1 \leq n \leq N$. So first we show that the coefficients of $F_n(x)$ satisfy the conditions of the lemma. We begin with condition (3.2) that $\prod F_n(x)$ has no fixed prime factor.

Proposition 3.2.9. *The product of the $F_n(x)$ for $1 \leq n \leq N$ has no fixed prime factor.*

Proof. If $p | AR$, then by (3.10) p cannot divide $F_n(x)$. If $p \nmid AR$, then there exists precisely one solution to the congruence $F_n(x) \equiv 0 \pmod{p}$, which we denote $x \equiv x_{n,p} \pmod{p}$. Since $N!$ divides A, p must be greater than N. By the Pigeon Hole Principle, there exists some x_0 such that $x_0 \not\equiv x_{n,p} \pmod{p}$ for all n. Thus, $p \nmid \prod F_n(x)$. □

Proposition 3.2.10. *Condition* (3.1) *holds for the coefficients of* $F_n(x)$. *Namely,*

$$\prod_{i=1}^{N} a_i A R_i R \prod_{1\le t<s\le N} (a_t A R_t R Y_s - a_s A R_s R Y_t) \neq 0.$$

Proof. Trivially, $a_i A R_i R \neq 0$. By way of contradiction, suppose $a_t A R_t R Y_s = a_s A R_s R Y_t$. Since $a_s, a_t | A$ with $(A, R) = (A, Y_n) = 1$, the only way to account for the factors of A is to force $a_s = a_t$. However, since the a_n are derived from Lemma 3.1.5, they must be distinct. Therefore the condition holds. □

To complete the proof of the main theorem, that there exist infinitely many integers z such that $d(z) = d(z+1)$, we must only satisfy (3.11).

Proof of Theorem 3.1.1. First, we note that since all the $F_n(x)$ are square-free, we may use the functions d and Ω, with the usual definitions, interchangeably. Adding the condition that the $a_i n + b_i$ be square-free to Lemma 3.1.2 and applying the lemma to the functions $F_n(x)$ yields a sequence of integers x such that $\Omega(\prod F_n(x)) \le r$. If $\Omega(F_m(x)) \neq \Omega(F_n(x))$ for all $m \neq n$, then we must have

$$r \ge \Omega\left(\prod F_n(x)\right) = \sum_n \Omega(F_n(x)) \ge \sum_{i=1}^{N} i = \frac{1}{2} N(N+1).$$

In other words, if we can find some N for which the associated r is strictly less than $N(N+1)/2$, there exists some pair m, n with $m < n \le N$ such that $\Omega(F_m(x)) = \Omega(F_n(x))$, which in turn implies $d(F_m(x)) = d(F_n(x))$, and thus (3.11) is satisfied. As remarked previously, for $N = 7$, we may take $r = 27 < N(N+1)/2 = 28$. Moreover, by (3.3), the frequency of $x \le X$ for which this occurs is at least $O(X(\log X)^{-7})$, which completes the proof. □

Remark 3.2.11. Although the conditions on the a_i in Lemma 3.1.5 are fairly simple, finding suitable sets for arbitrary N is not simple at all. For $N = 2$, it is clear that any two consecutive integers will do. For $N = 3$, there are only 22 examples for which the a_n are less than 1000. The smallest are $\{84, 85, 90\}$ and $\{84, 90, 91\}$. For $N = 4$, there is no suitable set for which the a_n are less than 25,000. The difficulty arises from the fact that the divisor function is multiplicative but not *completely* multiplicative. As a result, the symmetry property, namely (3.5), tends to fail.

Moreover, even using the smallest possible case for $N = 2$—$(2, 3)$—we end up with 4-digit coefficients in the F_n generated during the proof. For $N = 3$, where the smallest case is $\{84, 85, 90\}$, the coefficients will already be massive. As a result of this, even if we could find such a set for $N = 7$, using it to generate the functions in the proof of the main theorem would prove far too unwieldy for any practical benefit.

3.3 Key Lemma

We now return to Heath-Brown's key lemma (Lemma 3.1.5). It should at this point be noted that by the summary of the proof in the last section, if we can find a set of values satisfying the sieve and the properties of the lemma for $N = 7$, then we can be done with the proof. Nevertheless, the key lemma, in spite of the fact that it proves existence of such values for *all* positive N, but does not provide for their construction, is worth examining for its own sake. So we will do so.

The method of proving this lemma is mainly pairing powers of primes. In other words: If for some prime p, $p^e||a_m$ and $p^f||a_n$, with $e > f \geq 1$, then we want another prime q such that $q^e||a_n$ and $q^f||a_n$. Then the left-hand side of (3.5) will give us $(e + 1)$ for factors of p, plus $(f + 1)(e - f + 1)$ for factors of q. Similarly, the right-hand side will give us $(f + 1)(e - f + 1)$ for factors of p, plus $(e + 1)$ for factors of q. Hence, p and q combined will produce the same number of factors on both sides. If this can be done simultaneously for all pairs m, n, then we will have proven the lemma.

One might ask whether it is possible to balance both sides of (3.5) without the constraint $e \neq f$. Let us consider what happens when $2^e||a_m, a_n$. Then $2^{(e+1)}|a_m - a_n = d_{mn}$. This contradicts (3.4), and similar problems arise for other small primes.

Heath-Brown achieves the goal of pairing up primes by choosing $N = 2^k$ for arbitrary k and using the convenient symmetry of the additive group $G = \mathbb{Z}_2^k$, which can easily be equated with the set $\{0, 1, 2, \ldots, N-1\}$ by way of the following bijection.

Definition 3.3.1. For $\sigma = (\sigma_1, \ldots, \sigma_k) \in G = \mathbb{Z}_2^k$, with $\sigma_i \in \{0, 1\}$, set

$$n(\sigma) = \sum_{\ell=1}^{k} 2^{(\ell-1)}\sigma_\ell.$$

Definition 3.3.2. We define $A_\sigma = a_{1+n(\sigma)}$ and $D_{\sigma\tau} = A_\sigma - A_\tau$.

By way of said notation, we rewrite the conditions of Lemma 3.1.5 as

$$D_{\sigma\tau} | A_\sigma \tag{3.12}$$

and

$$d(A_\sigma)d\left(\frac{A_\tau}{|D_{\sigma\tau}|}\right) = d(A_\tau)d\left(\frac{A_\sigma}{|D_{\sigma\tau}|}\right) \tag{3.13}$$

for all $\sigma \neq \tau$.

Definition 3.3.3. Using the 1-1 correspondence between the set 0 through $N-1$ and $G = \mathbb{Z}_2^k$, we define $\{p_\sigma | \sigma \in G\}$ to be the first N primes.

Definition 3.3.4. With the p_σ defined as above, we write

$$P = \prod_{\sigma \in G} p_\sigma.$$

Definition 3.3.5. We write $D_{\sigma\tau} = E_{\sigma\tau}F_{\sigma\tau}$, where $E_{\sigma\tau}$ is a product of powers of the first N primes p_π, and

$$(F_{\sigma\tau}, P) = 1.$$

Remark 3.3.6. The main purpose of this distinction between the $E_{\sigma\tau}$ and the $F_{\sigma\tau}$ is to deal with the smaller primes (factors of $E_{\sigma\tau}$) separately in order to avoid the problems encountered by Spiro.

Proposition 3.3.7. *If we can arrange the p_σ so that*

$$p_\sigma^{n(\sigma+\tau)} || A_\tau \tag{3.14}$$

and

$$p | F_{\sigma\tau} \implies p || F_{\sigma\tau},\ p || A_\sigma, \tag{3.15}$$

for all $\sigma \in G$, then for every $\sigma \in G$, A_σ satisfies the revised conditions, (3.12) *and* (3.13)*, for Lemma 3.1.5.*

Proof. If $\sigma \neq \tau$, then $\pi+\sigma \neq \pi+\tau$, and thus $n(\pi+\sigma) \neq n(\pi+\tau)$. Since $p_\pi^{n(\pi+\sigma)}||A_\sigma$ and $p_\pi^{n(\pi+\tau)}||A_\tau$, we have

$$p_\pi^{\min(n(\pi+\sigma),n(\pi+\tau))}||A_\sigma - A_\tau = D_{\sigma\tau} = E_{\sigma\tau}F_{\sigma\tau},$$

so that

$$p_\pi^{\min(n(\pi+\sigma),n(\pi+\tau))}||E_{\sigma\tau}.$$

Thus, if $\sigma \neq \tau$,

$$E_{\sigma\tau} = \prod_{\pi\in G} p_\pi^{\min(n(\pi+\sigma),n(\pi+\tau))}, \tag{3.16}$$

so that

$$E_{\sigma\tau}|A_\sigma \tag{3.17}$$

by (3.14). This agrees with (3.12). Now consider the number of factors contributed by all the primes p_π corresponding with the left-hand side of (3.13). By way of (3.14) and (3.16), we get

$$\prod_{\pi\in G}(1+n(\pi+\sigma))\prod_{\pi\in G}(1+n(\pi+\tau)-\min\{n(\pi+\sigma),n(\sigma+\tau)\}).$$

We substitute $\rho = \pi+\sigma$ to get

$$\prod_{\rho\in G}(1+n(\rho))\prod_{\rho\in G}(1+n(\rho+\sigma+\tau)-\min\{n(\rho),n(\rho+\sigma+\tau)\}).$$

This is symmetric in σ and τ and thus agrees with (3.13). For the remaining (larger) primes, it follows trivially from (3.15) that $F_{\sigma\tau}|A_\sigma$. This in conjunction with (3.17) is enough to satisfy (3.12). Moreover, $p|A_\sigma, A_\tau \implies p|D_{\sigma\tau} \implies p|F_{\sigma\tau}$. The first implication follows from the definition of $D_{\sigma\tau}$; the second because p is a large prime. By (3.15), we have $p||A_\sigma, A_\tau, D_{\sigma\tau}$. It follows that

$$p||A_\sigma, \qquad p\nmid \frac{A_\tau}{|D_{\sigma\tau}|}, \qquad p||A_\tau, \qquad p\nmid \frac{A_\sigma}{|D_{\sigma\tau}|},$$

and the corresponding factors of p in (3.13) match. If, alternatively, $p\nmid A_\sigma$ and $p^e||A_\tau$ ($e\geq 1$), then $p\nmid D_{\sigma\tau}$, thus

$$p\nmid A_\sigma, \qquad p^e||\frac{A_\tau}{|D_{\sigma\tau}|}, \qquad p^e||A_\tau, \qquad p\nmid \frac{A_\sigma}{|D_{\sigma\tau}|},$$

and the corresponding factors of p still match up on both sides. This suffices for (3.13). $\square$

We must still show how (3.14) and (3.15) can be satisfied. For ease of notation, set $J = (1, 1, \ldots, 1) \in G$ so that $n(J) = N - 1$. We also assign

$$E^*_{\sigma\tau} = \prod_{\pi \in G} p_\pi^{\min(n(\pi+\sigma), n(\pi+\tau))}. \tag{3.18}$$

Proposition 3.3.8. *Let δ_σ ($\sigma \in G$) be distinct integers with $\delta_I = 0$ and such that the following property holds for $\sigma \neq \tau$.*

For $E^*_{\sigma\tau}$ as defined above, $\delta_\sigma - \delta_\tau = E^*_{\sigma\tau} F^*_{\sigma\tau}$, where

$$F^*_{\sigma\tau} \text{ is square-free,} \tag{3.19}$$

$$(F^*_{\sigma\tau}, P) = 1, \tag{3.20}$$

and

$$(F^*_{\sigma\tau}, F^*_{\pi\rho}) = 1, \qquad \{\sigma, \tau\} \neq \{\pi, \rho\}. \tag{3.21}$$

Then there exists a constant that, when added to each δ_σ, yields a set of A_σ that satisfy (3.14) *and* (3.15).

Proof. Consider the system of simultaneous congruences

$$x \equiv -\delta_\sigma + p_{J+\sigma}^{N-1} \pmod{p_{J+\sigma}^N}, \qquad \sigma \in G, \tag{3.22}$$

$$x \equiv -\delta_\sigma - E^*_{\sigma\tau} F^*_{\sigma\tau} \pmod{F^{*2}_{\sigma\tau}}, \qquad \sigma, \tau \in G, \qquad n(\sigma) < n(\tau). \tag{3.23}$$

The $p_{J+\sigma}^N$ and $F^{*2}_{\sigma\tau}$ are all pairwise coprime by (3.20) and (3.21). Therefore, by the Chinese Remainder Theorem, solutions to the system exist. Let x be a solution sufficiently large so that $x + \delta_\sigma$ is positive for all σ, and set $A_\sigma = x + \delta_\sigma$. Since the δ_σ are distinct, so are the A_σ. From (3.22), it follows that

$$p_{J+\sigma}^{N-1} || A_\sigma.$$

Letting $\pi = J + \sigma$ (also, $\sigma = \pi + J$) gives us

$$p_\pi^{N-1} || A_{\pi+J}. \tag{3.24}$$

If $\sigma \neq \pi + J$, then $n(\sigma+\pi) < N-1 = n((\pi+J)+\pi) = n(J)$. Hence, $p_\pi^{n(\sigma+\pi)} || E^*_{\sigma\tau}$ by (3.18). Since $A_\sigma = A_{\pi+J} + (\delta_\sigma - \delta_{\pi+J})$ and $\delta_\sigma - \delta_{\pi+J} = E^*_{\sigma,\pi+J} F^*_{\sigma,\pi+J}$, we have $p_\pi^{n(\sigma+\pi)} || A_\sigma - A_{\pi+J}$. So it follows from (3.24) that

$$p_\pi^{n(\sigma+\pi)} || A_\sigma$$

for all $\sigma, \pi \in G$. This satisfies (3.14), which only leaves (3.15). Since this construction of the A_σ yields $F_{\sigma\tau} = F^*_{\sigma\tau}$ and, similarly, $E_{\sigma\tau} = E^*_{\sigma\tau}$, we have $p | F^*_{\sigma\tau} \implies p || F^*_{\sigma\tau}$ by (3.19). Moreover, $p \nmid E^*_{\sigma\tau}$, so by (3.23) we have $p || A_\sigma$ whenever $n(\sigma) < n(\tau)$. If, on the other hand, $n(\sigma) > n(\tau)$, then we have $A_\tau - A_\sigma = D_{\tau\sigma} \implies A_\sigma = A_\tau - D_{\tau\sigma}$, which gives us

$$A_\sigma = A_\tau - E^*_{\tau\sigma} F^*_{\tau\sigma} = x + \delta_\tau - E^*_{\tau\sigma} F^*_{\tau\sigma} \equiv -2 E^*_{\tau\sigma} F^*_{\tau\sigma} \pmod{F^{*2}_{\tau\sigma}}.$$

Since $E^*_{\tau\sigma} = E^*_{\sigma\tau}$ and $F^*_{\tau\sigma} = -F^*_{\sigma\tau}$, we have

$$A_\sigma \equiv 2 E^*_{\sigma\tau} F^*_{\sigma\tau} \pmod{F^{*2}_{\sigma\tau}}.$$

Since $p | F^*_{\sigma\tau}$ implies $p \nmid P$, which in turn means that $p > 2$, we conclude that $p || A_\sigma$ in both cases. Thus (3.15) is satisfied as well. □

All that remains for the lemma is to find suitable integers δ_σ.

3.4 Key Lemma: Finding the Integers δ_σ

Set

$$\alpha_\sigma = \prod_\pi p_\pi^{n(\sigma+\pi)},$$
$$\delta_\sigma = \alpha_\sigma - \alpha_I + \beta_\sigma P^N,$$

with $\beta_I = 0$ so that $\delta_I = 0$. Since $n(\sigma + \pi) < N$,

$$p_\pi^{n(\sigma+\pi)} || \delta_\sigma + \alpha_I. \tag{3.25}$$

The power of p_I occuring above, namely $n(\sigma)$, is different for each σ, hence the δ_σ are unique. If $\sigma \neq \tau$, we have $n(\sigma + \pi) \neq n(\tau + \pi)$ so (3.25) implies

$$p_\pi^{\min(n(\sigma+\pi),n(\tau+\pi))} || \delta_\sigma - \delta_\tau.$$

Thus $E^*_{\sigma\tau} | \delta_\sigma - \delta_\tau$. Also, (3.20) holds for these δ_σ.

It now remains to choose the numbers β_σ so that our numbers δ_σ satsify (3.19) and (3.21). In order to simply the notation, we now equate $\alpha_\sigma = \alpha_{n(\sigma)}$ and $\beta_\sigma = \beta_{n(\sigma)}$. For instance, since $\beta_I = 0$, we now have $\beta_0 = 0$. We define

$$g_M(\beta_1, \ldots, \beta_{M-1}) = \prod_{0 \leq m < n < M} (\alpha_m - \alpha_n + (\beta_m - \beta_n) P^N),$$

so that

$$g_N(\beta_1, \ldots, \beta_{N-1}) = \prod_{n(\sigma) < n(\tau)} (E^*_{\sigma\tau} F^*_{\sigma\tau}).$$

We also define $f_Q(n)$ to be 0 if, for some $p \nmid Q$, $p^2 | n$. Otherwise, $f_Q(n)$=1. We can satisfy (3.19) and (3.21) by finding $\beta_1, \ldots, \beta_{N-1}$ such that

$$f_P(g_N(\beta_1, \ldots, \beta_{N-1})) = 1. \tag{3.26}$$

We do this by a sieve process and by induction.

We find the β_M by induction on M. For $M = 1$, base case, g_M is constant and equal to the empty product, namely 1, so that $f_P(g_M) = 1$. For the induction step, suppose (3.26) holds for $M - 1$ so that there exist $\beta_1, \ldots, \beta_{M-1}$ so that $f_P(g_M(\beta_1, \ldots, \beta_{M-1})) = 1$. We set

$$h(\beta) = \prod_{0 \le m < M} (\alpha_m - \alpha_M + (\beta_m - \beta)P^N).$$

Let $k = g_M(\beta_1, \ldots, \beta_{M-1})$. To show (3.26) holds for M, we must find β so that $f_P(kh(\beta)) = 1$. (Notice that multiplying k by $h(\beta)$ is precisely akin to adding on the M_{th} term.) First, we find a β^* so that $p \nmid h(\beta^*)$ whenever $p|k$ and $p \nmid P$. Since $p \nmid P$, and since $h(x)$ is of degree M,

$$h(x) \equiv 0 \pmod{p}$$

has at most M solutions $\pmod{p}$. Furthermore, since P is defined as the product of the first N primes, $p|h(x)$, and $p \nmid P \implies p > N \ge M$. So $p \ge M$. Hence, there must exist some x_p for which the congruence fails so that $p \nmid h(x_p)$. By the Chinese Remainder Theorem, we may solve the system of simultaneous congruences

$$\beta^* \equiv x_p \pmod{p}$$

for all $p|k, p \nmid P$. Thus, $p|k, p \nmid P$ implies $p \nmid h(\beta^*)$ as desired. We now define $j(\gamma) = h(\beta^* + k\gamma)$, and we wish to find a γ such that $f_{kP}(j(\gamma)) = 1$.

By definition of f, the following inequality applies:

$$f_Q(n) \ge 1 - \sum_{p^2|n, p \nmid Q} 1.$$

Hence

$$\sum_{0 < \gamma \le G} f_{kP}(j(\gamma)) \ge G - \sum_{p \nmid kP} \#\{\gamma : 0 < \gamma \le G, p^2 | j(\gamma)\}. \tag{3.27}$$

Let

$$\ell_m = \alpha_m - \alpha_M + (\beta_m - \beta^*)P^N - kP^N\gamma$$

so that $j(\gamma) = \prod_m \ell_m$. If $p|\ell_m, \ell_n$ with $m < n$, then $p|(\ell_m - \ell_n)$. However,

$$\ell_m - \ell_n = \alpha_m - \alpha_n + (\beta_m - \beta_n)P^N,$$

which is a factor of $g_M(\beta_1, \ldots, \beta M - 1) = k$. Thus, if $p \nmid kP$ and $p^2 | j(\gamma)$, then p^2 must divide one of the factors ℓ_m for some m. Since each ℓ_m is linear in γ, there is precisely one $\gamma \pmod{p^2}$ for which $p^2 | \ell_m$. Thus

$$\#\{\gamma : 0 < \gamma \leq G, p^2 | j(\gamma)\} \leq M(Gp^{-2} + 1).$$

Moreover, since $p^2 | \ell_m$ implies $p \ll G$, we may say that $p \leq (cG)^{1/2}$, where c is independent of G (but may depend on N and $\beta_1, \ldots, \beta_{M-1}$). Hence,

$$\begin{aligned} \sum_{p \nmid kP} \#\{\gamma : 0 < \gamma \leq G, p^2 | j(\gamma)\} &\leq M \sum_{N < p \leq (cG)^{1/2}} (Gp^{-1/2} + 1) \\ &\leq GN \sum_{p > N} p^{-2} + O(G^{1/2}). \end{aligned} \tag{3.28}$$

Thus, (3.27) implies

$$\sum_{0 < \gamma \leq G} f_{kP}(j(\gamma)) \geq G - G\left(N \sum_{p > N} p^{-2} + O(G^{-1/2}) \right)$$

Because

$$1 - N \sum_{p > N} p^{-2} > 0,$$

it follows that the sum on the left-hand side of (3.27) is positive when G is sufficiently large. Therefore, a suitable γ exists, which concludes the inductive proof that $\beta_1, \ldots, \beta_{N-1}$ can be found to satisfy (3.26) for arbitrary N.

This completes the proof of Lemma 3.1.5, which in turn completes the proof of the theorem. Heath-Brown remarks that the last argument requires the fact that $p \nmid P \implies p > N$ both in the construction of β^* and in (3.28). This is precisely where the small primes would otherwise have caused trouble had they not been dealt with as factors of P.

Chapter 4

Solutions to $\omega(z) = \omega(z+1)$

Recall that for a positive integer z, we defined $\omega(z)$ to be the number of prime factors of z. As with the divisor function, we have the following theorem.

Theorem 4.0.1. *There are infinitely many z such that z and $z+1$ have the same number of distinct prime factors.*

The argument used in this proof is similar to that given by D. R. Heath-Brown for $d(z) = d(z+1)$; however, since that argument depends on powers of primes, it fails here. Thus, while in the former proof, arbitrarily large sets were constructed in a systematic way, we will construct a special set, numerically, for the proof of this theorem.

We use the following sieve estimate, which follows immediately from a theorem of Heath-Brown [6].

Theorem 4.0.2. *Let $c_1, \ldots, c_5 \in \mathbb{N}$. Then there are infinitely many natural numbers such that*

$$\sum_{i=1}^{5} 2^{\omega(c_i n+1)} \leq 57.$$

Assume there exist 5 integers $a_1, \ldots, a_5$ such that for $1 \leq i < j \leq 5$, we have $(a_i, a_j) = |a_i - a_j|$, and $\omega(a_i/|a_i - a_j|) = \omega(a_j/|a_i - a_j|)$. Set $A = a_1 \cdots a_5$ and $c_i = a_i A$ for each i. If n is an integer, then for some pair $i \neq j$, we have $\omega(a_i An+1) = \omega(a_j An+1)$, or else the sum on the left side in the theorem is at least 62. Moreover, by our assumptions, $a_j(a_i An+1)/|a_i - a_j|$ and $a_i(a_j An+1)/|a_i - a_j|$

are consecutive integers. It remains to show they have the same number of prime factors. Since $a_i|A$, we have $(a_i, a_jAn+1) = 1$. It follows that

$$\begin{aligned}\omega\left(\frac{a_j(a_iAn+1)}{|a_i-a_j|}\right) &= \omega\left(\frac{a_j}{|a_i-a_j|}\right) + \omega(a_iAn+1) \\ &= \omega\left(\frac{a_i}{|a_i-a_j|}\right) + \omega(a_jAn+1) \\ &= \omega\left(\frac{a_i(a_jAn+1)}{|a_i-a_j|}\right).\end{aligned}$$

For any n from Theorem 4.0.2, we now have one pair of consecutive integers with the same number of distinct prime factors. Each pair can only occur for finitely many n; so, by the Pigeon Hole Principle, there are infinitely many pairs.

Now we find $a_1, \ldots, a_5$ with the desired properties. There are ten equations to be checked, which are not all independent. For example, the author shows that no three integers in the set may be consecutive. To avoid similar difficulties, the numbers may be chosen so that $|a_i - a_j|$ are each divisible by many prime factors. However, these differences should also remain reasonably small, or else the a_i will grow large enough to present significant computational problems in checking each quintuple.

To this end, after experimentation, the author defines: $b_1 = 8$, $b_2 = 9$, $b_3 = 12$, $b_4 = 34$, $b_5 = 576$, $N = 2^4 \cdot 3^5 \cdot 5^3 \cdot 7^2 \cdot 11^2 \cdot 13 \cdot 47^2 \cdot 71^2 \cdot 271$, $k = 110245379356152833616$ and considers the sequence of quintuples $(l \cdot N + k + b_1, \ldots, l \cdot N + k + b_5)$. Setting $l = 1202$ gives:

$$\begin{aligned}a_1 &= 13598765028117829238962 4, \\ a_2 &= 13598765028117829238962 5, \\ a_3 &= 13598765028117829238962 8, \\ a_4 &= 13598765028117829238965 0, \\ a_5 &= 13598765028117829239019 2,\end{aligned}$$

where the a_i factor as follows:

$$
\begin{aligned}
a_1 &= 2^3 \cdot 13 \cdot 29 \cdot 71^2 \cdot 431 \cdot 733 \cdot 28311976573, \\
a_2 &= 3^5 \cdot 5^3 \cdot 7 \cdot 1481 \cdot 3109 \cdot 80737 \cdot 1720429, \\
a_3 &= 2^2 \cdot 3 \cdot 11 \cdot 31^2 \cdot 47^2 \cdot 53 \cdot 6899 \cdot 1327224593, \\
a_4 &= 2 \cdot 5^2 \cdot 11^2 \cdot 13 \cdot 19 \cdot 271 \cdot 1145107 \cdot 293245787, \\
a_5 &= 2^4 \cdot 3^4 \cdot 7^2 \cdot 47 \cdot 71 \cdot 271 \cdot 2367951977749.
\end{aligned}
$$

The quintuple has the following differences:

$$
\begin{aligned}
a_2 - a_1 &= 1, & a_4 - a_2 &= 25 = 5^2, \\
a_3 - a_1 &= 4 = 2^2, & a_5 - a_2 &= 567 = 3^4 \cdot 7, \\
a_4 - a_1 &= 26 = 2 \cdot 13, & a_4 - a_3 &= 22 = 2 \cdot 11, \\
a_5 - a_1 &= 568 = 2^3 \cdot 71, & a_5 - a_3 &= 564 = 2^2 \cdot 3 \cdot 47, \\
a_3 - a_2 &= 3, & a_5 - a_4 &= 542 = 2 \cdot 271.
\end{aligned}
$$

It is simple to check that the quintuple along with the differences satisfy the required properties, thus proving the main theorem.

It is interesting to note, in particular, that a_1 and a_2 are consecutive integers, each with 7 prime factors. In fact, it is easy to see that these are the consecutive integers generated by the choice of $n = 0$ in the construction of the proof.

Recall, however, that this proof allows for any choice of n. Suppose, for instance, we chose $n = 1$. Then we want to find a_i and a_j so that $\omega(a_i A + 1) = \omega(a_j A + 1)$. Unfortunately, even with *Mathematica* on a fast computer, the size of A makes such comparisons difficult.

Chapter 5

Concluding Remarks

When I began the line of research one year ago that lead to this thesis, all I saw before me was an enjoyable paper on the topic of Ruth-Aaron Pairs of the second type. Once I got past the baseball anecdotes, however, I began to see that the methods being used to attempt and to solve a similar group of problems were, in fact, extraordinarily different.

In Chapter 2, we begin with a fairly direct proof and summary of the simplest set of RAP2s. Then, for the next case, which appears almost identical but for a switch between $(\omega(n), \omega(n+1)) = (2, 1)$ and $(\omega(n), \omega(n+1)) = (1, 2)$, we immediately find ourselves thrown into far more detailed proof filled with exhaustive case work. For all this, we have clear results: The first two cases yield precisely 3 RAP2s: $(5, 6)$, $(24, 25)$, and $(49, 50)$.

The final section for Chapter 2, however, barely resembles the previous two. Yes, the topic is still the classification of the RAP2s, but the methods are entirely different. Whereas the previous two sections are deterministic and rely on more classical methods, the last parametrizes a case within a case and does so through entirely computational means.

We return to the classical in Chapter 3 with Heath-Brown's proof of the existence of infinitely many solutions to the equation $d(z) = d(z+1)$, and especially his Key Lemma wherein the natural numbers are afforded nearly unreasonable symmetry by way of a map to powers of the group $\mathbb{Z}_2$. After a long and winding course, we have a set of parameters to enter into a sieve.

Except we do not really have them. We know the parameters exist, and the Key Lemma tells us we can have as many of them as we need, but they are remarkably difficult to locate. It is only in Chapter 4, in a proof of the infinitude of solutions to $\omega(z) = \omega(z+1)$ that effectively mirrors Chapter 3, that we are able to find a set of parameters and use a sieve directly. Whereas Chapter 3 is long and winding, Chapter 4 is a straight run.

There is more to be done, and some questions remain open. There appear to be infinitely many of both the RAPs and the RAP2s, but these remain conjecture. The question of equality over consecutive integers may be asked of other arithmetic functions: ϕ, σ, Ω, and more. The solutions to one of these might be infinite as in the case of d and ω or conjecture as with S and P. They might be finite. They might be trivial. They warrant further study. For now, I let the matter rest.

Appendix A

A.1 Tables

n	$n+1$	$P(n)$
5	6	5
24	25	5
49	50	7
77	78	18
104	105	15
153	154	20
369	370	44
492	493	46
714	715	29
1682	1683	31
2107	2108	50
2299	2300	30
2600	2601	20
2783	2784	34
5405	5406	75
6556	6557	162
6811	6812	146
8855	8856	46
9800	9801	14
12726	12727	113

Table A.1: Ruth Aaron Pairs of the 2nd Type ($P(n) = P(n+1)$)

z	$z+1$	$d(z)$
2	3	2
14	15	4
21	22	4
26	27	4
33	34	4
34	35	4
38	39	4
44	45	6
57	58	4
75	76	6
85	86	4
86	87	4
93	94	4
94	95	4
98	99	6
104	105	8
116	117	6
118	119	4
122	123	4
133	134	4
135	136	8
141	142	4
142	143	4
145	146	4
147	148	6
158	159	4
171	172	6
177	178	4
189	190	8

Table A.2: Solutions to $d(z) = d(z+1)$

z	$z+1$	$\omega(z)$
1	2	1
2	3	1
3	4	1
4	5	1
7	8	1
8	9	1
14	15	2
16	17	1
20	21	2
21	22	2
31	32	1
33	34	2
34	35	2
35	36	2
38	39	2
39	40	2
44	45	2
45	46	2
50	51	2
51	52	2
54	55	2
55	56	2
56	57	2
57	58	2
62	63	2
68	69	2
74	75	2
75	76	2
76	77	2
85	86	2
86	87	2
87	88	2
91	92	2
92	93	2
93	94	2
94	95	2
95	96	2
98	99	2
99	100	2

Table A.3: Solutions to $\omega(z) = \omega(z+1)$

References

[1] Leonard M. Adleman, Carl Pomerance, and Robert S. Rumely. On distinguishing prime numbers from composite numbers. *Ann. of Math. (2)*, 117(1):173–206, 1983.

[2] P. Erdös and L. Mirsky. The distribution of values of the divisor function $d(n)$. *Proc. London Math. Soc. (3)*, 2:257–271, 1952. 9

[3] Paul ErdHos and Carl Pomerance. On the largest prime factors of n and $n+1$. *Aequationes Math.*, 17(2-3):311–321, 1978. 8

[4] H. Halberstam and H.-E. Richert. *Sieve methods*. Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1974. London Mathematical Society Monographs, No. 4. 9, 26, 32

[5] D. R. Heath-Brown. The divisor function at consecutive integers. *Mathematika*, 31(1):141–149, 1984. 3, 10, 26

[6] D. R. Heath-Brown. Almost-prime k-tuples. *Mathematika*, 44(2):245–266, 1997. 42

[7] Douglas E. Iannucci and Alexia S. Mintos. On consecutive integer pairs with the same sum of distinct prime divisors. *Integers*, 5(1):A12, 9 pp. (electronic), 2005. 13

[8] Trygve Nagell. *Introduction to number theory*. Second edition. Chelsea Publishing Co., New York, 1964. 13

[9] C. Nelson, D. E. Penney, and C. Pomerance. 714 and 715. *J. Recreational Math.*, 7(1):87–89, 1974. 8

[10] C. Pomerance. Ruth-Aaron numbers revisited. In *Paul ErdHos and his mathematics, I (Budapest, 1999)*, volume 11 of *Bolyai Soc. Math. Stud.*, pages 567–579. János Bolyai Math. Soc., Budapest, 2002. 9

[11] Kenneth H. Rosen. *Elementary number theory and its applications*. Addison-Wesley, Reading, MA, fifth edition, 2005. 4

[12] J.-C. Schlage-Puchta. The equation $\omega(n) = \omega(n+1)$. *Mathematika*, 50(1-2):99–101 (2005), 2003. 10

[13] C. Spiro. *Thesis*. Urbana, 1981. 9

[14] R. C. Vaughan. A remark on the divisor function $d(n)$. *Glasgow Math. J.*, 14:54–55, 1973. 9

[15] Sheng Gang Xie. On the k-twin primes problem. *Acta Math. Sinica*, 26(3):378–384, 1983. 27