ON THE RIEMANN HYPOTHESIS AND HILBERT'S TENTH PROBLEM

ARAN NAYEBI

ABSTRACT. The Riemann hypothesis is one of the most famous unresolved problems in modern mathematics. The discussion here will present an overview of the methods that prove the Riemann hypothesis is a Π_1^0 sentence.

CONTENTS

1. INTRODUCTION

The Riemann zeta function is the function of the complex variable s defined in the half-plane $\Re(s) > 1$ by the sum of the infinite series

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

By analytic continuation, we can define the zeta function on the entire complex plane $\mathbb{C}$ except at $s = 1$ where $\zeta(s)$ has its unique pole. In his seminal 1859 memoir entitled "On the number of primes less than a given magnitude", Riemann [29] derives an analytic formula for the distribution of prime numbers expressed in terms of the zeros of $\zeta(s)$. The function $\zeta(s)$ has as *trivial zeros* the negative even integers -2, -4, . . . and as *nontrivial zeros* the complex numbers $\frac{1}{2} + i\beta$, where β is a zero of the even entire function $\xi(t)$ of the complex variable t defined (by Riemann) as

$$\xi(t) := \frac{1}{2}s(s-1)\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s),$$

where $s = \frac{1}{2} + it$ and, as usual, $\Gamma(s)$ is the gamma function. The zeros of $\xi(t)$ have imaginary part between $-i/2$ and $i/2$. The Riemann hypothesis is the statement that all zeros of $\xi(t)$ are real, or equivalently,

Riemann hypothesis. *The nontrivial zeros of $\zeta(s)$ have real part of $\frac{1}{2}$.*

From a first glance, it may seem that the Riemann hypothesis is only an interesting property of $\zeta(s)$, and one may be led to think that even Riemann himself took that view, for he wrote "Without doubt it would be desirable to have a rigorous proof of this proposition; however I have left this research aside for the time being after some quick unsuccessful attempts, because it appears to be unnecessary for the immediate goal of my study" [7, pp. 3-4]. However, one should not conclude that the Riemann hypothesis was of only minor interest to him, since from his memoir it is quite likely that he was aware of the importance of his hypothesis
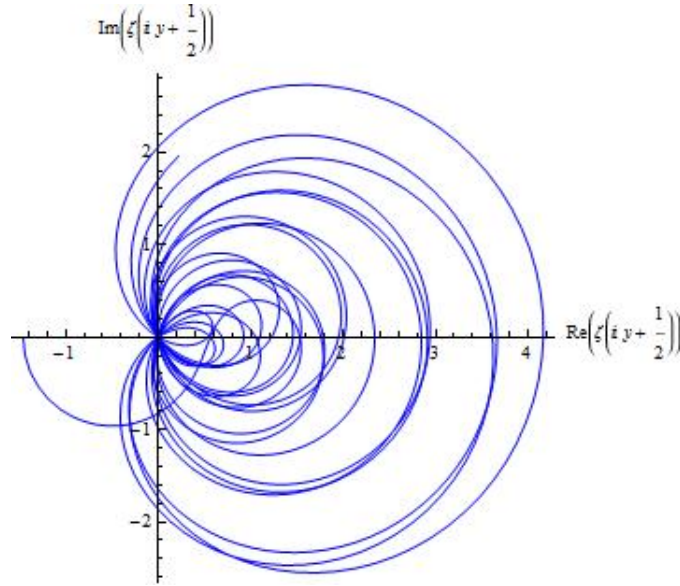
FIGURE 1. Plot of the real and imaginary parts of $\zeta(s)$ along the critical line $\Re(s) = \frac{1}{2}$ as y is varied varied from 0 to 80.

in approximating the distribution of prime numbers, as we will explain below.

The Riemann hypothesis has many startling consequences for analytic number theory. If we let $\pi(x)$ denote the number of primes $\leq x$ which is well approximated by

$$\text{Li}(x) = \int_2^x \frac{dt}{\log t},$$

then the Riemann hypothesis is equivalent to saying that

$$\pi(x) = \text{Li}(x) + O(x^{1/2} \log x).$$

The error term is the best possible in this case since it is known to oscillate in both directions to an order of at least $\text{Li}\left(x^{1/2}\right) \log^{(3)} x$, where $\log^{(3)} x$ is the three-fold iterated logarithm.[1] A more precise result due to Schoenfeld [30] is that the Riemann hypothesis is equivalent to

$$|\pi(x) - \text{Li}(x)| < \frac{1}{8\pi} x^{1/2} \log x,$$

for all $x \geq 2657$. The Riemann hypothesis is one of the main open questions in prime number theory due to the fact that its failure would wreak havoc in the distribution of prime numbers [7]. Moreover, it has become a central problem of pure mathematics as well, for instance due to its consequences for global L-functions. A discussion of these functions is beyond the scope of this article; however, the reader is referred to §2 of Bombieri's [7] for an informal yet informative treatment of the topic.

Our interest in the Riemann hypothesis stems from the consequences of the negative solution to Hilbert's tenth problem by Davis, Putnam, and Robinson [10], and subsequently by Matiyasevich [23]. In 1900, listed as problem 10 of his famous 23 problems[2], the eminent mathematician Hilbert asked,

"Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: *To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers*" [20, pg. 458].

---

[1]Von Koch [35] in fact proved that the Riemann hypothesis is the best possible bound for the error of the prime number theorem (which states that $\pi(x) \sim \frac{x}{\log x}$).

[2]It is of relevance to point out that the Riemann hypothesis is part of Hilbert's eighth problem.

The term 'rational integers' here simply refers to the integers, and the words 'process' and 'finite number of operations' refers to the modern notion of an algorithm.[3] In clearer terms, Hilbert was essentially asking for a general algorithm to decide whether a given diophantine equation with integer coefficients has a solution in integers. The negative solution to this problem is commonly referred to as the DPRM theorem[4], and formally states that

Theorem 1 (DPRM theorem). *Every recursively enumerable set is diophantine.*[5]

Since there exist recursively enumerable sets which are not computable, then it is an immediate consequence that Hilbert's tenth problem is unsolvable over $\mathbb{Z}$. Therefore, a Turing machine cannot decide whether a given diophantine equation has solutions or not over $\mathbb{Z}$.[6]

Ultimately, the DPRM theorem bridges computability theory and number theory (this relationship, for instance, is made incredibly explicit by the nondeterministic diophantine machine (NDDM) of Adleman and Manders [1]), and since recursively enumerable sets are diophantine, it is well-known many open problems in number theory can be expressed as the assertion that a particular diophantine equation has no solution in nonnegative integers. The Riemann hypothesis is one of these problems, and there have been several reductions of the Riemann hypothesis to a system of diophantine equations (and therefore to a single polynomial that is unsolvable in nonnegative integers if the Riemann hypothesis is true, and solvable if otherwise). The first formulation [11] is based on a decidability condition that considers the behavior of a Cauchy integral on a path around the zeros of the Riemann zeta function and involves the computable function $\delta(x)$ defined for positive integers as such

$$\delta(x) := \prod_{n < x} \prod_{j \leq n} \eta(j),$$

where $\eta(j) = 1$ unless j is a prime power, and $\eta(p^k) = p$. The second, much simpler formulation [25] utilizes the relation

$$\mathrm{explog}(a, b) \Leftrightarrow \exists x \left\{ x > b + 1 \ \& \ \left(1 + \frac{1}{x}\right)^{xb} \leq a + 1 < 4 \left(1 + \frac{1}{x}\right)^{xb} \right\}.$$

Essentially, it is possible to write a computer program to search for a counterexample to the Riemann hypothesis, and this program will halt with a counterexample if and only if a certain diophantine equation has a solution.[7]

This article will proceed as follows. In §2 we will discuss in detail both approaches to the reduction of the Riemann hypothesis to a system of diophantine equations. And in §3 we will discuss two significant open problems in number theory that have not yet been proven to be Π_1^0 propositions.

---

[3]The formalization of the concept of the algorithm began with the 1931 incompleteness theorems of Gödel [15] regarding the unsolvability of the *Entscheidungsproblem* ('decision problem'). Subsequent formalizations were centered upon defining 'effective calculability', which included the recursive functions of Herbrand [19] and Gödel [16], Church's λ-calculus [8], Post's 'Formulation 1' [28], and Turing's a-machines [33].

[4]This result is either referred to as the MRDP (Matiyasevich-Robinson-Davis-Putnam) theorem or the DPRM (Davis-Putnam-Robinson-Matiyasevich) theorem (Matiyasevich favors the latter and Davis the former [22]). To preserve the historical integrity of the order of succession of results that led to the negative solution to Hilbert's tenth problem, we will use the latter naming convention in this article.

[5]Equivalently, by the DPRM theorem, it follows that every Π_1^0 proposition is equivalent to the unsolvability of a particular diophantine equation.

[6]The analog of Hilbert's tenth problem over $\mathbb{Q}$ has still not been proven, although Poonen [27] poses a conjecture, that if true, would imply the unsolvability of Hilbert's tenth problem over $\mathbb{Q}$. Furthermore, the unsolvability of Hilbert's tenth problem has been proven by several authors for many rings. A recent paper by Mazur and Rubin [26] shows that conditional on the 2-primary part of the Shafarevich-Tate conjecture, Hilbert's tenth problem is unsolvable over the ring of integers of *every* number field. Shlapentokh [31] provides an excellent survey of the developments arising from the attempts to solve the analog of Hilbert's tenth problem for the field of rational numbers and the rings of integers of number fields.

[7]Of course, the diophantine representations of these famous problems are not currently considered a *viable* approach towards a proof.

2. Proof that the Riemann hypothesis is a Π_1^0 proposition

The key step in proving that the Riemann hypothesis is a Π_1^0 proposition is to prove a decidable property (this is a nontrivial task) which can then be written in terms of system of diophantine equations, from which all that remains is to combine these equations into a single equation (which is easily done either by the simple sum of squares method or, to minimize the number of variables, by the more specialized Matiyasevich-Robinson relation-combining theorem [24]). The reason why the decidable property is essential is that if we have an algorithm that tells us in a finite number of steps whether an arbitrary natural number has a particular property P, then we can reduce the assertion that every natural number has the property P to the unsolvability of a particular diophantine equation which we can explicitly write down. Hence, when discussing the two approaches to proving that the Riemann hypothesis is Π_1^0, we will focus on the derivation of the decidable property, rather than the explicit system of equations that is produced. And in the case of the Riemann hypothesis, it is not immediately evident that it can be formulated in the desired form $\forall n$ $P(n)$.

2.1. **Davis, Matiyasevich, and Robinson (1976).** As mentioned before, Davis, Matiyasevich, and Robinson's [11] approach to establishing a decidable property involves the computable function $\delta(x)$ defined for positive integers as such

$$\delta(x) := \prod_{n<x} \prod_{j\leq n} \eta(j),$$

where $\eta(j) = 1$ unless j is a prime power, and $\eta(p^k) = p$. From which they proved the following decidable property

Theorem 2 (Davis, Matiyasevich, and Robinson)**.** *The Riemann hypothesis is equivalent to the assertion (for $n = 1, 2, 3, \ldots$) that*

$$(2.1) \qquad \left(\sum_{k\leq\delta(n)} \frac{1}{k} - \frac{n^2}{2} \right)^2 < 36n^3.$$

It is rather simple, using the methods of Matiyasevich [23], to obtain an explicit diophantine equation which has no solution in case the decidable property above holds. Furthermore, the authors remark that the constant 36 can be readily improved. Indeed, after we present the proof of Theorem 2, it will be a trivial observation to the reader that one can obtain the slightly improved bound

$$(2.2) \qquad \left(\sum_{k\leq\delta(n)} \frac{1}{k} - \frac{n^2}{2} \right)^2 < (\gamma^2 + 8\gamma + 16)n^3 + (2\gamma + 8)n^{3/2} + 1,$$

where $\gamma = 0.577\ldots$ is the Euler-Mascheroni constant. Note that the system of diophantine equations cannot contain γ because it cannot be written explicitly. A bound to Theorem 2 which does not involve γ but obviously weaker than the one presented in (2.2) is

$$(2.3) \qquad \left(\sum_{k\leq\delta(n)} \frac{1}{k} - \frac{n^2}{2} \right)^2 < 25n^3 + 10n^{3/2} + 1.$$

Of course, neither (2.2) or (2.3) are intended to be *practical* replacements to the bound given in Theorem 2; we simply presented them to affirm that it is an easy task, as Davis, Matiyasevich, and Robinson pointed out, to improve the bound in (2.1).

We now proceed to present the proof of Theorem 2. First, the following basic facts (from number theory) must be stated, which will be used in the proof, and therefore we will present these as lemmas without proof (the references that contain their proofs can be found on page 335 of [11] in the same order as they are listed here).

Lemma 1. *It is well-known that*

$$\frac{\Gamma^{'}(3/2)}{\Gamma(3/2)} = 2 - \gamma - \log 4.$$

Lemma 2. *If we let R to denote the set of nontrivial zeros of $\zeta(s)$,*

$$\frac{\zeta^{'}(s)}{\zeta(s)} = \log 2\pi - 1 - \frac{\gamma}{2} - \frac{1}{s-1} - \frac{1}{2}\frac{\Gamma^{'}\left(\frac{s}{2}+1\right)}{\Gamma\left(\frac{s}{2}+1\right)} + \sum_{\rho \in R}\left(\frac{1}{s-\rho} + \frac{1}{\rho}\right).$$

Moreover,

$$\lim_{s \to 1}\left(\frac{\zeta^{'}(s)}{\zeta(s)} + \frac{1}{s-1}\right) = \gamma.$$

Lemma 3. *For $x \in \mathbb{R}$, where $x > 0$,*

$$\psi(x) = \sum_{p^k \leq x}\log p = \sum_{j \leq x}\log \eta(j),$$

and

$$\psi_1(x) = \int_1^x \psi(u)du.$$

Thus, for integral x, $\psi(x) \leq \sum_{j \leq x}\log x = x\log x \leq x^{3/2}$ and $\psi_1(x) = \log \delta(x)$. This gives us the following expression for $\psi_1(x)$ for $x \geq 1$,

$$\psi_1(x) = \frac{x^2}{2} - \sum_{\rho \in R}\frac{x^{\rho+1}}{\rho(\rho+1)} - x\frac{\zeta^{'}(0)}{\zeta(0)} + \frac{\zeta^{'}(-1)}{\zeta(-1)} - \sum_{r=1}^{\infty}\frac{x^{1-2r}}{2r(r-1)}.$$

Lemma 4. *We also have that*

$$\frac{\zeta^{'}(0)}{\zeta(0)} = \log 2\pi,$$

and

$$\frac{\zeta^{'}(1)}{\zeta(1)} = 12\log A - 1 = 1.985\ldots,$$

where A is the Glaisher-Kinlekin constant defined exactly as such

$$A = \lim_{n \to \infty}\frac{H(n)}{n^{n^2/2+n/2+1/12}e^{-n^2/4}},$$

where $H(n)$ is the hyperfactorial function.

Lemma 5.

$$\left(\sum_{k \leq n}\frac{1}{k}\right) - 1 < \log n < \sum_{k \leq n}\frac{1}{k},$$

for n a positive integer.

We need one additional lemma, whose proof will be shown, as it is derived from the above lemmas.

Lemma 6.

$$\sum_{\rho \in R}\frac{1}{\rho(1-\rho)} = \gamma + 2 - \log 4\pi.$$

Proof. We have that

$$\sum_{\rho \in R}\frac{1}{\rho(1-\rho)} = \sum_{\rho \in R}\left(\frac{1}{1-\rho} + \frac{1}{\rho}\right).$$

From Lemma 2 it follows that

$$\sum_{\rho \in R} \left(\frac{1}{1-\rho} + \frac{1}{\rho} \right) = \lim_{s \to 1} \left(\frac{\zeta'(s)}{\zeta(s)} + \frac{1}{s-1} \right) - \log 2\pi + 1 + \frac{\gamma}{2} + \frac{1}{2} \frac{\Gamma'(3/2)}{\Gamma(3/2)}.$$

Lastly, from Lemmas 1 and 2, we have then that

$$\lim_{s \to 1} \left(\frac{\zeta'(s)}{\zeta(s)} + \frac{1}{s-1} \right) - \log 2\pi + 1 + \frac{\gamma}{2} + \frac{1}{2} \frac{\Gamma'(3/2)}{\Gamma(3/2)} = \gamma + 2 - \log 4\pi.$$

∎

Now, assume the Riemann hypothesis, namely that $\rho \in R$ implies $\Re(\rho) = \frac{1}{2}$. Moreover, for $\rho \in R$, the complex conjugate $\bar{\rho} = 1 - \rho$. Thus,

$$\sum_{\rho \in R} \frac{1}{|\rho| \cdot |\rho+1|} \leq \sum_{\rho \in R} \frac{1}{|\rho|^2} = \sum_{\rho \in R} \frac{1}{\rho \bar{\rho}} = \sum_{\rho \in R} \frac{1}{\rho(1-\rho)}.$$

Hence, from Lemma 6,

(2.4)
$$\sum_{\rho \in R} \frac{1}{|\rho| \cdot |\rho+1|} \leq \gamma + 2 - \log 4\pi.$$

Using (2.4) and Lemma 3, and noting that the Riemann hypothesis implies that for $\rho \in R$, $x \geq 1$, we have that $|x^{\rho+1}| = x^{3/2}$, then

$$|\psi_1(x) - \frac{x^2}{2}| \leq x^{3/2} \left(\sum_{\rho \in R} \frac{1}{|\rho| \cdot |\rho+1|} + |\frac{\zeta'(0)}{\zeta(0)}| + |\frac{\zeta'(-1)}{\zeta(-1)}| + \sum_{r=1}^{\infty} \frac{1}{2r(2r-1)} \right).$$

A subsequent simplification of the infinite sum gives us,

$$\sum_{r=1}^{\infty} \frac{1}{2r(2r-1)} = \sum_{r=1}^{\infty} \left(\frac{1}{2r-1} - \frac{1}{2r} \right) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} = \log 2.$$

And with the additional use of Lemma 4,

$$|\psi_1(x) - \frac{x^2}{2}| \leq x^{3/2} \left(\gamma + 2 - \log 4\pi + \log 2\pi + 2 + \log 2 \right) = (4+\gamma)x^{3/2} < 5x^{3/2}.$$

But by Lemma 5,

$$| \sum_{k \leq \delta(x)} \frac{1}{k} - \psi_1(x) | < 1.$$

As a result, we have

$$| \sum_{k \leq \delta(x)} \frac{1}{k} - \frac{x^2}{2} | < 1 + 5x^{3/2} \leq 6x^{3/2}.$$

Thus,

$$\left(\sum_{k \leq \delta(x)} \frac{1}{k} - \frac{x^2}{2} \right)^2 < 36x^3,$$

which gives us (2.1).

To prove the implication in the other direction, suppose that (2.1) holds for all positive integers. Then by Lemma 5, for $x = 1, 2, 3, \ldots$,

$$|\psi_1(x) - \frac{x^2}{2}| < 1 + 6x^{3/2}.$$

Hence, for any real $x \geq 1$, by Lemma 3,

$$|\psi_1(x) - \frac{x^2}{2}| \leq \int_{[x]}^{x} \psi(u)du + |\psi_1([x]) - \frac{[x]^2}{2}| + |\frac{[x]^2 - x^2}{2}| < \psi([x]) + 1 + 6x^{3/2} + x \leq 9x^{3/2}.$$

We now employ arguments that are modeled after those used by Ingham [21]. For $s > 1$, it is a well-known fact

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}},$$

where p runs through all primes. Therefore,

$$\log \zeta(s) = -\sum_p \log(1 - p^{-s}) = \sum_{p,m} \frac{1}{mp^{ms}},$$

where m runs through all positive integers. By differentiation,

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_p \frac{p^{-s} \log p}{1 - p^{-s}} = \sum_{p,m} \frac{\log p}{p^{ms}}.$$

In terms of the von Mangoldt function, $\Lambda(n)$, we can rewrite this as,

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s},$$

where $\Lambda(n)$ is $\log p$ if n is a positive power of a prime p, and is 0 otherwise. Moreover, note that $\psi(x) = \sum_{n \leq x} \Lambda(n)$. Therefore, we have that

$$-\frac{\zeta'(s)}{\zeta(s)} = s \int_1^{\infty} \frac{\psi(x)}{x^{s+1}} dx.$$

Or, in terms of $\psi_1(x)$,

$$-\frac{\zeta'(s)}{\zeta(s)} = s(s+1) \int_1^{\infty} \frac{\psi_1(x)}{x^{s+2}} dx.$$

Hence,

(2.5)
$$-\frac{\zeta'(s)}{\zeta(s)} - \frac{s(s+1)}{2(s-1)} = s(s+1) \int_1^{\infty} \frac{\psi_1(x) - \frac{x^2}{2}}{x^{s+2}} dx.$$

So, assuming our inequality,

$$\left| \frac{\psi_1(x) - \frac{x^2}{2}}{x^{s+2}} \right| \leq \frac{9}{|x^{s+1/2}|},$$

the integral in (2.5) uniformly converges on the region $\Re(s) > \sigma_0$, for any $\sigma_0 > 1/2$. (2.5) must be valid for $\Re(s) > 1/2$, and the function on the left is analytic in this domain. But clearly, this implies that $\zeta(s)$ does not vanish for $1/2 < \Re(s) < 1$, which means that the Riemann hypothesis holds.

Theorem 2 is now proved.

2.2. **Matiyasevich (1993).** Of course, Theorem 2 is not the only method of proving that the Riemann hypothesis is a Π_1^0 statement. Another, albeit lesser known, formulation is due to Matiyasevich [25] and involves the usage of less variables in its diophantine representation than the Davis, Matiyasevich, and Robinson [11] result. Matiyasevich essentially takes advantage of the fact that the Riemann hypothesis implies that for

(2.6)
$$n \geq 600,$$

(2.7)
$$|\psi(n) - n| < n^{1/2} \log^2 n.$$

Since

$$\psi(n) = \log(\mathrm{lcm}(1, 2, \ldots, n)),$$

we can reduce (2.7) to a system of diophantine equations because the function lcm (least common multiple) is diophantine. However, this is only immediately obvious when lcm is considered as a function of two

arguments, not with indefinite numbers of arguments. Namely, the diophantine representation of lcm for positive integers b and c is

$$a = \mathrm{lcm}(b, c) \Leftrightarrow bc = a \gcd(b, c),$$

where the generalized diophantine representation for gcd is

$$a = \gcd(b, c) \Leftrightarrow bc > 0 \ \& \ a \mid b \ \& \ a \mid c \ \& \ \exists xy\{a = bx - cy\},$$

and as usual $\mid$ denotes the relation of divisibility which is diophantine since

$$a \mid b \Leftrightarrow \exists x\{ax = b\}.$$

Matiyasevich [25] avoids this problem by way of a bounded universal quantifier, namely, the number m is a common multiple of $1, 2, \ldots, n$ if and only if

(2.8) $$\forall y < n\{(y + 1) \mid m\}$$

and is the least common multiple if, in addition,

(2.9) $$m > 0 \ \& \ \forall y < m\{y = 0 \vee \exists x < n\{(x + 1) \nmid y\}\}.$$

Now, the next problem we face is whether or not $\log n$ is diophantine. Since its values are not generally integers, one method would be to show that $\lfloor \log n \rfloor$ is diophantine, but this is a nontrivial task. Instead, Matiyasevich [25] introduces the relation mentioned before, namely,

(2.10) $$\mathrm{explog}(a, b) \Leftrightarrow \exists x \left\{ x > b + 1 \ \& \ \left(1 + \frac{1}{x}\right)^{xb} \leq a + 1 < 4\left(1 + \frac{1}{x}\right)^{xb} \right\}.$$

We will first prove that for all a and b,

(2.11) $$\mathrm{explog}(a, b) \Rightarrow |b - \log(a + 1)| < 2,$$

and second, that

(2.12) $$\forall a \exists b \{\mathrm{explog}(a, b)\}.$$

We proceed as follows. It is a well-known fact from calculus that for $x > 0$,

$$\left(1 + \frac{1}{x}\right)^{x} < e < \left(1 + \frac{1}{x}\right)^{x+1}.$$

Raising this inequality to the power b, we have

$$\left(1 + \frac{1}{x}\right)^{xb} < e^b < \left(1 + \frac{1}{x}\right)^{(x+1)b}.$$

Dividing by e, we have,

$$\frac{e^b}{e} \leq \frac{(1 + \frac{1}{x})^{(x+1)b}}{(1 + \frac{1}{x})^{x}} < \left(1 + \frac{1}{x}\right)^{xb} \leq a + 1 < 4\left(1 + \frac{1}{x}\right)^{xb} \leq 4e^b,$$

which implies (2.11).

Now, for any a one can find b such that

$$b \leq \log(a + 1) < b + \log 3.$$

Choosing a very large x, we can make both $\left(1 + \frac{1}{x}\right)^{x}$ and $\left(1 + \frac{1}{x}\right)^{x+1}$ arbitrarily close to e since

$$e = \lim_{x \to \infty} \left(1 + \frac{1}{x}\right)^{x} = \lim_{x \to \infty} \left(1 + \frac{1}{x}\right)^{x+1},$$

thereby validating the inequalities in (2.10).

Theorem 3 (Matiyasevich)**.** *The negation of the Riemann hypothesis is equivalent to the existence of numbers k, l, m, and n satisfying conditions* (2.6)*,* (2.7)*,* (2.8)*, and*

$$(2.13) \qquad\qquad \mathrm{explog}(m-1, l),$$

$$(2.14) \qquad\qquad \mathrm{explog}(n-1, k),$$

$$(2.15) \qquad\qquad (l-n)^2 > 4n^2 k^4.$$

Proof. First, let us assume that such k, l, m, and n exist. Then by (2.7) and (2.8),

$$(2.16) \qquad\qquad m = e^{\psi(n)}.$$

Moreover, by (2.11), it follows from (2.14) that

$$(2.17) \qquad\qquad |l - \psi(n)| < 2.$$

And from (2.15) that

$$(2.18) \qquad\qquad |k - \psi(n)| < 2.$$

As a result, we obtain

$$|\psi(n) - n| \geq |l - n| - |l - \psi(n)| > 2n^{1/2}k^2 - 2 > n^{1/2}\log^2 n,$$

which with (2.7), gives us the desired contradiction.

On the other hand, assume that the Riemann hypothesis is not true. Since the Riemann hypothesis is equivalent to the statement

$$\psi(n) = n + O(n^{1/2}\log^2 n),$$

then there is a number n satisfying (2.6) such that

$$|\psi(n) - n| > 10n^{1/2}\log^2 n.$$

Choosing m according to (2.16), conditions (2.8) and (2.13) will be satisfied. Then by (2.12), we can find numbers k and l satisfying (2.13) and (2.14). By (2.11), the inequalities (2.17) and (2.18) will be satisfied, which in turn imply that

$$|l - n| \geq |\psi(n) - n| - |l - \psi(n)| > 10n^{1/2}\log^2 n - 2 > 2n^{1/2}(\log n + 2)^2 > 2n^{1/2}k^2,$$

thereby satisfying the inequality (2.15). ∎

Since all of the conditions given in Theorem 3 are diophantine, then we can construct a diophantine equation whose unsolvability is equivalent to the Riemann hypothesis.

3. Open problems that have not yet been shown to be Π_1^0 sentences

Now, the natural question is whether or not every problem can be reduced to a question concerning the solvability of diophantine equations. Davis, Matiyasevich, and Robinson [11] are keen to observe that not all open problems in number theory have been proven to be Π_1^0 sentences. The example they present is the twin prime conjecture, namely, the statement

$$\forall n\{\exists p\{p > n \ \& \ p \text{ prime} \ \& \ p + 2 \text{ prime}\}\}.$$

As Matiyasevich [25] mentions, since we can eliminate only bounded universal quantifiers, we have no obvious way to restate the twin prime conjecture as the problem of the solvability or unsolvability of a particular diophantine equation. However, as Davis, Matiyasevich, and Robinson [11] suggest, if we strengthen the conjecture to the statement,

$$\forall n\{\exists p\{n + 4 < p < 2^{n+4} \ \& \ p \text{ prime} \ \& \ p + 2 \text{ prime}\}\},$$

then this strong twin prime conjecture can be transformed into the unsolvability of a particular diophantine equation. Note that like the twin prime conjecture, the strong twin prime conjecture is also widely believed to be true.

We will add to this list another number-theoretic problem that has not been shown to be a Π_1^0 proposition.

This is the Elliott-Halberstam conjecture, which is related to the Riemann hypothesis in that, if true, it results in deeper estimates for the distribution of primes in arithmetic progressions than the generalized Riemann hypothesis (which is a generalization of the Riemann hypothesis to a statement regarding the distribution of the zeros of global L-functions) does. We shall now quantify what we mean by 'deeper'. Given an arithmetic progression $a \pmod q$, we let $\pi(x; q, a)$ denote the number of primes $\leq x$ lying in the progression with $\gcd(a, q) = 1$.

$$\pi(x; q, a) = \frac{1}{\phi(q)} \mathrm{Li}(x) + E(x; q, a),$$

where $\phi(q)$ is Euler's totient function and $E(x; q, a)$ is the error term. For every $A > 0$ there is a constant $\theta(q, A)$ that may depend on q for which

$$|E(x; q, a)| \leq \theta(q, A) \frac{x}{(\log x)^A}.$$

This result is rather weak; however, under the assumption of the generalized Riemann hypothesis, we derive the much stronger bound

(3.1) $$|E(x; q, a)| \leq \theta x^{1/2} \log x,$$

for a positive constant θ *independent* of q if $q \leq x$.

In 1965, Vinogradov [34] and Bombieri [4] independently improved Barban's results [3] regarding Linnik's large sieve, and proved the following

Theorem 4 (Bombieri-Vinogradov theorem). *For any positive constant A there exists a positive constant $B = B(A)$ such that $Q = x^{1/2}(\log x)^{-B}$, with*

(3.2) $$\sum_{q \leq Q} E^*(x; q) \ll \frac{x}{(\log x)^A},$$

where for a modulus q, the functions $E(x; q)$ and $E^*(x; q)$ are defined as

$$E(x; q) = \max_{\gcd(a,q)=1} |E(x; q, a)|$$

$$E^*(x; q) = \max_{y \leq x} E(y, q).$$

B can be computed explicitly, a possible value of B is $3A + 23$ [4]; $B = 24A + 46$ is also permissible [32]. From the Bombieri-Vinogradov theorem, we have on average over $q \leq Q$,

(3.3) $$E(x; q) \leq \theta x^{1/2} (\log x)^{B-A}.$$

The bound given in (3.3) can sometimes be used as a substitute for the bound (3.1) that assumes the generalized Riemann hypothesis. Thus, for many situations that involve sufficiently many Dirichlet L-functions, and therefore require the use of the generalized Riemann hypothesis, the Bombieri-Vinogradov theorem can be employed instead.

Bombieri, Friedlander, and Iwaniec [5] [6] have managed to extend Theorem 4 beyond the $x^{1/2}$ barrier. Specifically, they proved that Q can be taken more explicitly as

$$Q = x^{1/2} \exp \left\{ \frac{\log x}{(\log^{(2)} x)^B} \right\}.$$

We say that primes have a level of distribution ϑ if (3.2) holds for any $A > 0$ and any $\epsilon > 0$ with

$$Q = x^{\vartheta - \epsilon}.$$

According to the Bombieri-Vinogradov theorem, primes have a level of distribution $1/2$. Elliott and Halberstam [13] extended Theorem 4 to conjecture that the primes have a level of distribution 1, namely,

Conjecture 1 (Elliott-Halberstam conjecture). *For any positive constant A and any $\epsilon > 0$ there exists a positive constant $B = B(A)$ such that $Q = x^{1-\epsilon}$, with*

$$\sum_{q \leq Q} E^*(x; q) \ll \frac{x}{(\log x)^A}.$$

Friedlander, Granville, Hildebrand, and Maier [14] have shown that for Q a bit larger, namely if

$$Q = x \cdot \exp\left\{-\frac{1}{4}(A-1)(\log^{(2)} x)^2(\log^{(3)} x)^{-1}\right\},$$

for $A > 1$, then Conjecture 1 does not hold. In fact, it is widely believed that the Elliott-Halberstam conjecture is valid with Q any fixed power x^μ, where $0 < \mu < 1$ [12].

The Elliott-Halberstam conjecture has many startling consequences. Alford, Granville, and Pomerance [2] proved that assuming the conjecture, then for any constant $a < 1$ there exists $C > 0$ such that there are more than x^a Carmichael numbers up to x, once $x > C$. Another, more recent startling consequence was proven by Goldston, Pintz, and Yıldırım [17] in their work on the twin prime conjecture, who showed that assuming Conjecture 1, for infinitely many n,

(3.4) $$p_{n+1} - p_n \le 16,$$

where p_n denotes the n-th prime.

We note that Conjecture 1 lies deeper than the generalized Riemann hypothesis, and Bombieri [4] remarks that nothing more precise than the Bombieri-Vinogradov theorem of Theorem 4 can be obtained even under the assumption of the generalized Riemann hypothesis. Hence, it is of little surprise that not much progress has been made towards proving the Elliott-Halberstam conjecture.

Moreover, as the reader may recall, we mentioned that determining a decidable property is not immediately evident in the case of the Riemann hypothesis. This is even more true with the Elliott-Halberstam conjecture, and for good reason. The author of this article had the idea to use (3.4) of Goldston, Pintz, and Yıldırım [17] to formulate a decidable property. To explain in more detail, (3.4) can be expressed in terms of the solutions of the Pell equation

(3.5) $$x^2 - (a^2 - 1)y^2 = 1,$$

for $a > 0$. This can be shown to be possible by first letting the solutions of (3.5) in order of the size of y be denoted as

$$x = \chi_a(n), \quad y = \psi_a(n),$$

and by utilizing the result from Theorem 419 of Hardy and Wright [18]

$$\lfloor \theta_1 \cdot 10^{2^n} \rfloor = 10^{2^n} \sum_{k=1}^{n} p_k 10^{-2^k},$$

$$\lfloor \theta_1 \cdot 10^{2^{n-1}} \rfloor = 10^{2^{n-1}} \sum_{k=1}^{n-1} p_k 10^{-2^k},$$

and

$$\lfloor \theta_1 \cdot 10^{2^{n+1}} \rfloor = 10^{2^{n+1}} \sum_{k=1}^{n+1} p_k 10^{-2^k}.$$

Giving us,

(3.6) $$p_n = \lfloor \theta_1 \cdot 10^{2^n} \rfloor - 10^{2^{n-1}} \lfloor \theta_1 \cdot 10^{2^{n-1}} \rfloor,$$

and

(3.7) $$p_{n+1} = \lfloor \theta_1 \cdot 10^{2^{n+1}} \rfloor - 10^{2^n} \lfloor \theta_1 \cdot 10^{2^n} \rfloor.$$

Although (3.6) is not practical for strictly evaluating p_n (since the constant $\theta_1 \approx 0.0203000500000007$ should be evaluated to 2^n decimal places, which can only be done if the values of $p_1, \ldots, p_n$ are known), its form is useful in expressing the n-th prime in terms of $\psi_a(n)$, which Matiyasevich and Robinson [24] prove is diophantine. Unfortunately, apart from the issue of including the real number θ_1 to formulate a decidable property involving (3.4), (3.4) only is *implied by* but is not equivalent to the Elliott-Halberstam conjecture. It turns out, however, that the task of finding a statement equivalent to the Elliott-Halberstam conjecture (let alone proving that this statement can be translated into the solvability or unsolvability of a particular diophantine equation) is incredibly nontrivial. Not to mention given that the translation of an open problem

to a particular diophantine equation does not provide much insight into solving the problem, such efforts into finding a decidable property for the Elliott-Halberstam conjecture can appropriately be viewed as fruitless. However, this certainly does not preclude the possibility that a breakthrough in the study of diophantine equations may provide insight into showing that a class of equations (including perhaps an equation of interest in that class that is equivalent to the truth of an important open problem) is unsolvable. One can only anticipate such a result.

References

1. L. Adleman and K. Manders. "Diophantine complexity". *FOCS* (1976): 81-88.
2. W. R. Alford, A. Granville, and C. Pomerance. "There are infinitely many Carmichael numbers". *Ann. Math.* **140** (1990): 703-722.
3. M. B. Barban. "New applications of the large sieve of Yu. V. Linnik". *Akad. Nauk. UzSSR Trudy. Inst. Mat.* **22** (1961): 1-20.
4. E. Bombieri. "On the large sieve". *Mathematika* **12** (1965): 201-225.
5. E. Bombieri, J. B. Friedlander, and H. Iwaniec. "Primes in arithmetic progressions to large moduli". *Acta Math.* **156** (1986): 203-251.
6. E. Bombieri, J. B. Friedlander, and H. Iwaniec. "Primes in arithmetic progressions to large moduli, II". *Math. Ann.* **277** (3) (1987): 361-393.
7. E. Bombieri. "The Riemann hypothesis - official problem description". Clay Mathematics Institute. `http://www.claymath.org/millennium/Riemann_Hypothesis/riemann.pdf`.
8. A. Church. "An unsolvable problem of elementary number theory". *Amer. J. Math.* **58** (1936): 345-363.
9. M. Davis (editor). *The undecidable; basic papers on undecidable propositions, unsolvable problems and computable functions*. Hewlett, New York: Raven Press, 1965.
10. M. Davis, H. Putnam, and J. Robinson. "The decision problem for exponential diophantine equations". *Ann. Math.* **47** (1961): 425-436.
11. M. Davis, Ju. V. Matijasevič, and J. Robinson. "Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution". Mathematical Developments Arising from Hilbert Problems. F. E. Browder (editor). *Proc. Sympos. Pure Math.* Vol. 28, American Mathematical Society, Providence, Rhode Island, 1976: 323-378.
12. P. D. T. A Elliott. *Duality in analytic number theory*. Cambridge University Press, New York, 1997.
13. P. D. T. A Elliott and H. Halberstam. "A conjecture in prime number theory". *Symp. Math.* **4** (1968-1969): 59-72.
14. J. B. Friedlander, A. Granville, A. Hildebrand, and H. Maier. "Oscillation theorems for primes in arithmetic progressions and for sifting functions". *J. Amer. Math. Soc.* **4** (1991): 25-86.
15. K. Gödel. "Über formal unentscheidbare Sätze der *Principia Mathematica* und verwandter Systeme, I". *Monatsh. Math.* **38** (1931): 173-198. English translation in: K. Gödel. *On formally undecidable propositions of Principia Mathematica and related systems*. Translated by B. Meltzer. New York: Basic Books, 1962.
16. K. Gödel. "On undecidable propositions of formal mathematical propositions". In [9]: 39-74. Originally in the form of notes taken by Kleene and Rosser on lectures given by Gödel at the Institute for Advanced Study during the spring of 1934.
17. D. A. Goldston, J. Pintz, and C. Y. Yıldırım. "Primes in tuples, I". *Ann. Math.* **170** (2009): 819-862.
18. G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. 5th ed., Clarendon Press, Oxford, 1979.
19. J. Herbrand. "Sur la non-contradiction de l'arithmétique". *Journal für die reine und angewandte Mathematik* **166** (1931): 1-8.
20. D. Hilbert. "Mathematical problems". *Bull. Amer. Math. Soc.* **8** (1902): 437-479.
21. A. E. Ingham. *The distribution of prime numbers*. Cambridge: Cambridge University Press, 1932.
22. A. Jackson. "Interview with Martin Davis". *Notices Amer. Math. Soc.* **55** (2008): 560-571.
23. Ju. V. Matijasevič. "Diofantovost' perechislimykh mnozhestv". *Dokl. Akad. Nauk SSSR* **191** (1970): 279-282. English translation in: Ju. V. Matijasevič. "Enumerable sets are diophantine". *Soviet Math. Dokl.* **11** (1970): 354-358.
24. Ju. V. Matijasevič and J. Robinson. "Reduction of an arbitrary diophantine equation to one in 13 unknowns". *Acta Arith.* **27** (1975): 521-553.
25. Yu. V. Matiyasevich. *Hilbert's tenth problem*. Cambridge, Massachussetts: MIT Press, 1993.
26. B. Mazur and K. Rubin. "Ranks of twists of elliptic curves and Hilbert's tenth problem". *Invent. Math.* **181** (2010): 541-575.
27. B. Poonen. "Using elliptic curves of rank one towards the undecidability of Hilbert's tenth problem over rings of algebraic integers". Algorithmic Number Theory (Sydney, 2002), *Lecture Notes in Computer Science* **2369**, Berlin: Springer-Verlag (2002): 33-42.
28. E. Post. "Finite combinatory processes. Formulation I". *J. Symbolic Logic* **1** (1936): 103-105.
29. B. Riemann. "Ueber die Anzahl der Primzahlen unter einer gegebenen Grösee". *Monat. der Königl. Preuss. Akad. der Wissen. zu Berlin aus der Jahre* (1859): 671-680.
30. L. Schoenfeld. "Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II". *Math. Comp.* **30** (1976): 337-360.
31. A. Shlapentokh. "Defining integers". *Bull. Symbolic Logic* **17** (2011): 230-251.
32. K. Soundararajan. "Small gaps between prime numbers: The work of Goldston-Pintz-Yıldırım". *Bull. Amer. Math. Soc.* **44** (2007): 1-18.
33. A. M. Turing. "On computable numbers, with an application to the *Entscheidungsproblem*". *Proc. Lond. Math. Soc.* **42** (1936-1937): 230-265. "On computable numbers, with an application to the *Entscheidungsproblem*. A correction". *Proc. Lond. Math. Soc.* **43** (1938): 544-546.
34. A. I. Vinogradov. "The density hypothesis for Dirichlet L-series". *Izv. Akad. Nauk. SSSR Set. Mat.* **29** (1965): 903-934; "Corrigendum". ibid. **30** (1966): 719-720.
35. H. von Koch. "Sur la distribution des nombres premiers". *Acta Math.* **24** (1901): 159-182.

E-mail address: anayebi@stanford.edu

URL: http://www.stanford.edu/~anayebi