The Diophantine Equation $\left(1+1^2\right)\left(1+2^2\right)\ldots\left(1+n^2\right)=b^2$

Thang Pang Ern

February 2023

1 Abstract

In Number Theory, a Diophantine Equation is an equation, typically a polynomial equation in two or more unknowns with integer coefficients, such that the only solutions of interest are the integer ones. This paper discusses the integer solutions to the Diophantine Equation

$$\prod_{k=1}^{n}(k^2+1)=b^2, \tag{1}$$

and we state some extensions of the problem. The reader should be familiar with the following terminologies and theorems, though these are not exhaustive: modulus and arguments of complex numbers (although it would not be the bulk of the proof as it plays a minor role in the motivation as to why the original Number Theory problem was posed), integral test for convergence, floor and ceiling functions (including some inequalities involving them), the Legendre Symbol, the Law of Quadratic Reciprocity, in particular primes p of the form $4k+1$, Fermat's Sum of Two Squares Theorem, elementary Ring Theory, Lifting the Exponent Lemma, the Prime Number Theorem, Bertrand's Postulate, the von Mangoldt Function $\Lambda(n)$, the First and Second Chebyshev Functions denoted by $\vartheta(n)$ and $\psi(n)$ respectively and some important bounds involving the prime-counting function $\pi(n)$.

2 Introduction

I thought of this question on Complex Numbers towards the end of my Junior College days in September 2021. It was *disguised* as a Number Theory problem and it states that

$$\prod_{k=1}^{n}(k+i) \tag{2}$$

is purely imaginary if and only if $n=3$.

2.1 Motivation

I believed that this was true but was not sure how to prove it rigorously back then. My friend verified it for up to 9-digit numbers using a code but did not manage to find any contradiction. What motivated me to consider the product of complex numbers in (2) is due to the Three Square Geometry Problem (Figure 1) which I came across when I was in Secondary School. The problem was discussed on YouTube by a channel called Numberphile.

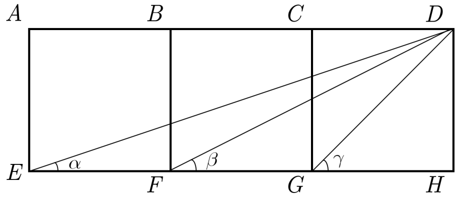

Figure 1: The Three Square Geometry Problem

The illustration on Figure 1 shows the essence of the problem. Arrange three identical squares $ABFE$, $BCGF$ and $CDHG$ in the following manner. From vertex D, construct a line segment from it to the bottom-left vertex of each square — the vertices are namely E, F and G. Let $\angle DEF=\alpha$, $\angle DFG=\beta$ and $\angle DGH=\gamma$. It can be proven, using elementary geometry, though using some sort of an ingenious solution, that $\alpha+\beta+\gamma=\pi/2$. Well, it is clear that $\gamma=\pi/4$ since $\triangle\ DGH$ is isosceles, so this identity is *reduced* to $\alpha+\beta=\pi/4$.

In contrast, using complex numbers makes the problem far simpler. In particular, using arguments, it is easy to show that

$$\arg\left((1+i)(2+i)(3+i)\right)=\arg(1+i)+\arg(2+i)+\arg(3+i)=\frac{\pi}{2}. \tag{3}$$

Thereafter, I thought of generalising this problem to n squares. Initially, I had the perception that the angle would converge but to my surprise, it diverges by the integral test. This is due to

$$\lim_{n\to\infty}\sum_{k=1}^{n}\arctan\left(\frac{1}{k}\right)\ [1] \tag{4}$$

being a divergent series.

Proof. We first state the integral test for convergence.

Theorem 2.1. *For a continuous, positive and decreasing function $f(x)$ on the interval $[1, \infty)$ and that $f(k) = a_k$, if*

$$\int_1^\infty f(x)\ dx \textit{ is divergent, then so is } \sum_{k=1}^\infty a_k.$$

The arctangent function is continuous, and in particular, for $x \geq 1$, $f(x) = \arctan(1/x)$ is positive. Now, we prove that f is decreasing, so

$$f'(x) = \left[\frac{1}{1 + (1/x)^2}\right]\left(-\frac{1}{x^2}\right) = -\frac{1}{x^2(1 + 1/x^2)} = -\frac{1}{x^2 + 1}. \tag{5}$$

Hence, $f'(x) < 0$ for all $x \geq 1$. We evaluate the improper integral, so using the method of by parts,

$$\begin{aligned}\int_1^\infty \arctan\left(\frac{1}{x}\right)\ dx &= [x \cdot \operatorname{arccot} x]_0^\infty - \int_0^\infty \frac{-x}{x^2+1}\ dx &(6)\\ &= [x \cdot \operatorname{arccot} x]_0^\infty + \left[\frac{1}{2}\log\left(x^2+1\right)\right]_0^\infty &(7)\\ &= \lim_{n\to\infty}\ (n \cdot \operatorname{arccot} n) + \frac{1}{2}\lim_{n\to\infty}\log\left(x^2+1\right) \to \infty &(8)\end{aligned}$$

which asserts that the sum diverges. □

Some of my friends tried to use a recurrence relation involving the addition formula of inverse tangent, that is

$$\arctan u + \arctan v = \arctan\left(\frac{u+v}{1-uv}\right) \tag{9}$$

but their attempts were futile as there were no *nice* properties of the above formula.

3 The Problem

This question actually belongs to the realm of Number Theory. Note that for $1 \leq k \leq n$, the modulus of the complex number $k+i$ is $\sqrt{k^2+1}$, and every complex number $z \in \mathbb{C}$ can be expressed as $z = a + bi$, where $a, b \in \mathbb{R}$. If

$$\prod_{k=1}^{n} (k+i) \tag{10}$$

is purely imaginary, then $z = bi$ (i.e. $a = 0$), and so $|z| = b$. Consider the product

$$\prod_{k=1}^{n} \sqrt{k^2+1} \tag{11}$$

which is the product of the moduli of the complex numbers $k+i$ for all $1 \leq k \leq n$. Hence, the problem translates to the following, which is of course, related to Number Theory.

Problem 3.1. *Find all pairs (b, n) of natural numbers such that*

$$\prod_{k=1}^{n} (k^2+1) = b^2. \tag{12}$$

Problem 3.1 is what we wish to solve in this paper, and we assert that $(b, n) = (10, 3)$ is the only solution to this Diophantine Equation. This would conclude that the product in (2) is purely imaginary if and only if $n = 3$.

Sometime in early 2022, I found a link on StackExchange regarding the proof to the question. It directed me to a page by Prof. Javier Cilleruelo [4], a former Mathematics Lecturer at the Autonomous University of Madrid in Spain. Fortunately, the proof was only four pages long. I started analysing the proof in early July. This paper aims to make Cilleruelo's proof more accessible by explaining the parts that were deemed trivial.

4 Proof

We first explore the following problem taken from the 17th China Western Mathematical Invitational Competition in 2017. It is from Problem 1 of Day 1 of the competition [8]. This would help us find a bound for p in terms of n.

Theorem 4.1. *Let p be a prime and n be a positive integer such that p^2 divides*

$$\prod_{k=1}^{n}(k^2+1). \tag{13}$$

Then, $p < 2n$.

Proof. Define P_n to be the above product. Since $p^2 \mid P_n$, then $p \mid P_n$. One case to consider is $p^2 \mid (k^2+1)$ for some $1 \leq k \leq n$. Then, $p^2 < n^2+1$ and hence, $p < \sqrt{n^2+1} < 2n$. Suppose otherwise, then there exists $1 \leq a < b \leq n$ such that $p \mid (a^2+1)$ and $p \mid (b^2+1)$, and so, taking the difference, $p \mid (b+a)(b-a)$. As $a+b < 2n$ and $b-a > 0$, $b^2-a^2 < 2n$. Thus, p is a divisor of some number less than $2n$ and the result follows. □

Theorem 4.2. *For $n > 3$,*

$$P_n = \prod_{k=1}^{n}(k^2+1) \tag{14}$$

is non-square.

Suppose on the contrary that for $n > 3$, P_n is square. Then, we can write it as a product of some primes p, where $p < 2n$, in the following form:

$$P_n = \prod_{p<2n} p^{\alpha_p}, \text{ where } \alpha_p \in \mathbb{N}. \tag{15}$$

Note that

$$P_n = \prod_{k=1}^{n}(k^2+1) > \prod_{k=1}^{n} k^2 = (n!)^2. \tag{16}$$

Consider writing $n!$ as

$$n! = \prod_{p \leq n} p^{\beta_p} \tag{17}$$

since $n!$ is a product of all the natural numbers from 1 to itself inclusive, and there are some numbers which are composite and hence, can be written as the product of primes. This expression is apt when we compare it with the expression for P_n in relation to α_p we claimed at the start.

We have the following as we make use of the property that the logarithm of a product is the sum of that logarithm:

$$\left(\prod_{p\le n} p^{\beta_p}\right)^2 < \prod_{p<2n} p^{\alpha_p} \tag{18}$$

$$2\log\left(\prod_{p\le n} p^{\beta_p}\right) < \log\left(\prod_{p<2n} p^{\alpha_p}\right) \tag{19}$$

$$\sum_{p\le n} \beta_p \log p < \frac{1}{2}\sum_{p<2n} \alpha_p \log p \tag{20}$$

Corollary 4.1. *For $n \ge 1$, $\alpha_2 = \lceil n/2 \rceil$.*

Proof. Since $k^2 \equiv 0$ or $1 \pmod 4$, then $k^2+1 \equiv 1$ or $2 \pmod 4$. The initial result can be easily derived by considering the cases where k is odd or even. Note that α_2 denotes the number of times P_n can be divided by 2. We try for $1 \le n \le 7$ to see the pattern.

$$P_1 = 2 \implies \alpha_2 = 1 = \lceil 1/2 \rceil \tag{21}$$

$$P_2 = 2\cdot 5 \implies \alpha_2 = 1 = \lceil 2/2 \rceil \tag{22}$$

$$P_3 = 2^2\cdot 5^2 \implies \alpha_2 = 2 = \lceil 3/2 \rceil \tag{23}$$

$$P_4 = 2^2\cdot 5^2\cdot 17 \implies \alpha_2 = 2 = \lceil 4/2 \rceil \tag{24}$$

$$P_5 = 2^3\cdot 5^2\cdot 13\cdot 17 \implies \alpha_2 = 3 = \lceil 5/2 \rceil \tag{25}$$

$$P_6 = 2^3\cdot 5^2\cdot 13\cdot 17\cdot 37 \implies \alpha_2 = 3 = \lceil 6/2 \rceil \tag{26}$$

$$P_7 = 2^4\cdot 5^4\cdot 13\cdot 17\cdot 37 \implies \alpha_2 = 4 = \lceil 7/2 \rceil \tag{27}$$

If k is odd, then k^2+1 is even, which is why for all odd k, P_k contributes an additional multiplicity of 2 (other than odd multiples) as compared to P_{k-1}. Hence, for odd k, consider the pair (P_k, P_{k+1}), where both their values of α_2 are the same. As there are $n/2$ such pairs, then $\alpha_2 = \lceil n/2 \rceil$. □

Before we state and prove an important lemma, we define the Legendre Symbol and state the major theorem known as the Law of Quadratic Reciprocity.

Definition 4.1. *Let p be an odd prime. An integer a is a quadratic residue modulo p if it is congruent to a perfect square modulo p and is a quadratic non-residue modulo p otherwise. The Legendre Symbol is a function of a and p defined as*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \textit{if } a \textit{ is a quadratic residue modulo } p \textit{ and } a \not\equiv 0 \pmod{p}, \\ -1 & \textit{if } a \textit{ is a non-quadratic residue modulo } p, \\ 0 & \textit{if } a \equiv 0 \pmod{p}. \end{cases}$$

Theorem 4.3. *The Law of Quadratic Reciprocity states that for distinct odd primes p and q,*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}. \tag{28}$$

Lemma 4.1. *Let p be an odd prime. If $p \mid (k^2+1)$ for $1 \leq k \leq n$, then $p \equiv 1 \pmod 4$.*

Proof. As $k^2 \equiv -1 \pmod p$, -1 is a quadratic residue modulo p. Here, we set $a = -1$ and so

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

By the Law of Quadratic Reciprocity, $p \equiv 1 \pmod 4$. □

Lemma 4.1 is closely related to a theorem by Fermat (Theorem 4.4), which is known as the Sum of Two Squares Theorem. Consequently, such p can be represented as the sum of two squares.

Theorem 4.4. *An odd prime p can be written as x^2+y^2, where $x, y \in \mathbb{Z}$ if and only if $p \equiv 1 \pmod 4$.*

Lemma 4.2. *For any prime p, $x^2 \equiv 0 \pmod p$ has the unique solution $x \equiv 0 \pmod p$.*

Proof. The only zero divisor in the ring $\mathbb{Z}/p\mathbb{Z}$ is 0. As such, if a product is 0, one of the factors must be 0 as well, and the result follows. □

Theorem 4.5. *For any prime p, each interval of length p^j contains two solutions to the congruence $x^2 \equiv 1 \pmod{p^j}$ [10].*

Let us investigate this property. For example, consider an interval of length 3^2 which contains any set of 9 consecutive numbers, say $\{5, 6, \ldots, 13\}$. Then, observe that the solutions to $x^2 \equiv 1 \pmod 9$ are $x = 8$ and $x = 10$. We try another example. Consider an interval of length 7^2 which contains any set of 49 consecutive numbers, say $\{100, 101, \ldots, 148\}$. Then, the solutions to $x^2 \equiv 1 \pmod{49}$ are 146 and 148. Sounds too good to be true, but why?

We use Lemma 4.2 to prove Theorem 4.5.

Proof. We proceed by induction. First, we solve the base case $x^2 \equiv 1 \pmod p$. Then, our induction hypothesis would be for $j > 1$, given a solution to $x^2 \equiv 1 \pmod{p^j}$, we find a solution to $x^2 \equiv 1 \pmod{p^{j+1}}$. The existence of the two and only two solutions, say x_1 and $-x_1$, is a consequence of the Law of Quadratic Reciprocity. For this to occur, we must have

$$\left(\frac{1}{p}\right) = 1. \tag{29}$$

The base case is an immediate consequence of the Law of Quadratic Reciprocity too.

Assume that there exists a solution x_0 such that $x_0^2 \equiv 1 \pmod{p^j}$. We wish to find a lift of $x_0 \pmod{p^j}$ to $x_1 \pmod{p^{j+1}}$ that satisfies $x_1^2 \equiv 1 \pmod{p^{j+1}}$. To ensure that $x_1 \pmod{p^{j+1}}$ is indeed a lift of $x_0 \pmod{p^j}$, consider

$$x_1 = x_0 + p^j y_0. \tag{30}$$

Squaring both sides,

$$\begin{aligned} x_1^2 &= x_0^2 + 2p^j x_0 y_0 + p^{j+1} y_0 && (31)\\ &\equiv x_0^2 + 2p^j x_0 y_0 \pmod{p^{j+1}} && (32)\\ x_0^2 + 2p^j x_0 y_0 &\equiv 1 \pmod{p^{j+1}} && (33) \end{aligned}$$

Since $x_0^2 - 1$ is a multiple of p^j, setting $x_0^2 - 1 = \lambda p^j$, (33) implies $\lambda p^j + 2p^j x_0 y_0$ is a multiple of p^{j+1}. Since $\gcd(2x_0, p) = 1$, then $\gcd(2p^j x_0, p^{j+1}) = p^j$ and hence, $\lambda + 2x_0 y_0$ is a multiple of p. As such, there exists a unique solution to

$$2x_0 y_0 \equiv \frac{1 - x_0^2}{p^j} \pmod{p} \tag{34}$$

and so

$$y_0 \equiv \frac{1 - x_0^2}{2p^j x_0} \pmod{p}. \tag{35}$$

The existence of the two solutions follows by the Law of Quadratic Reciprocity. □

Lemma 4.3. *If* $p \equiv 1 \pmod 4$*, then*

$$\frac{1}{2}\alpha_p - \beta_p \leq \sum_{j \leq \log n/\log p} \left(\left\lceil \frac{n}{p^j} \right\rceil - \left\lfloor \frac{n}{p^j} \right\rfloor \right) + \sum_{\log n/\log p < j \leq \log(n^2+1)/p} \left\lceil \frac{n}{p^j} \right\rceil. \tag{36}$$

Proof. Let S_1 and S_2 denote the following sets:

$$S_1 = \left\{ 1 \leq k \leq n,\ p \text{ prime} : p^j | (k^2+1) \right\} \text{ and } S_2 = \left\{ 1 \leq k \leq n,\ p \text{ prime} : p^j | k \right\} \tag{37}$$

Then, using Theorem 4.5, we can find an upper bound for α_p and an equation for β_p. That is,

$$\alpha_p = \sum_{j \leq \log(n^2+1)/\log p} |S_1| \leq \sum_{j \leq \log(n^2+1)/\log p} 2\lceil n/p^j \rceil \tag{38}$$

and

$$\beta_p = \sum_{j \leq \log n/\log p} |S_2| = \sum_{j \leq \log n/\log p} \left\lfloor \frac{n}{p^j} \right\rfloor. \tag{39}$$

Hence,

$$\begin{aligned} \frac{1}{2}\alpha_p - \beta_p &\leq \sum_{j \leq \log(n^2+1)/\log p} \left\lceil \frac{n}{p^j} \right\rceil - \sum_{j \leq \log n/\log p} \left\lfloor \frac{n}{p^j} \right\rfloor && (40)\\ &= \sum_{j \leq \log n/\log p} \left\lceil \frac{n}{p^j} \right\rceil + \sum_{\log n/\log p \leq j \leq \log(n^2+1)/\log p} \left\lceil \frac{n}{p^j} \right\rceil - \sum_{j \leq \log n/\log p} \left\lfloor \frac{n}{p^j} \right\rfloor && (41)\\ &= \sum_{j \leq \log n/\log p} \left(\left\lceil \frac{n}{p^j} \right\rceil - \left\lfloor \frac{n}{p^j} \right\rfloor \right) + \sum_{\log n/\log p \leq j \leq \log(n^2+1)/\log p} \left\lceil \frac{n}{p^j} \right\rceil && (42) \end{aligned}$$

and we have established Lemma 4.3. □

We observe a nice property related to the floor and ceiling function before stating an important theorem.

Lemma 4.4. *Let* $C = \lceil x \rceil - \lfloor x \rfloor$*. If* $x \in \mathbb{Z}$*,* $C = 0$*, otherwise,* $C = 1$*.*

Proof. If $x \in \mathbb{Z}$, $\lceil x \rceil = \lfloor x \rfloor = x$, and so $C = 0$. Suppose $x \in \mathbb{Z} \backslash \mathbb{R}$. By definition, $m < \lceil x \rceil \leq m + 1$ and $m \leq \lfloor x \rceil < m + 1$, where $m \in \mathbb{Z}$. Hence, $-m - 1 < -\lceil x \rceil \leq -m$, and so $-1 < C \leq 1$. Since C is an integer, $0 \leq C \leq 1$. However, $\lfloor x \rfloor \neq \lceil x \rceil$, which asserts that $C = 1$. □

Theorem 4.6. *If* $p \equiv 1 \pmod 4$*, then*

$$\frac{1}{2}\alpha_p - \beta_p \leq \frac{\log\left(n^2+1\right)}{\log p}. \tag{43}$$

Proof. The proof hinges on Lemma 4.3 and Lemma 4.4. Note that $\lceil n/p^j \rceil - \lfloor n/p^j \rfloor \leq 1$ for all $j \leq \log n / \log p$. Hence,

$$\sum_{j \leq \log n / \log p} \left(\left\lceil \frac{n}{p^j} \right\rceil - \left\lfloor \frac{n}{p^j} \right\rfloor \right) \leq \sum_{j \leq \log n / \log p} . \tag{44}$$

It is also clear that for all $\log n / \log p \leq j \leq \log(n^2+1)/\log p$, $\lceil n/p^j \rceil \leq 1$. As such,

$$\sum_{\log n / \log p \leq j \leq \log(n^2+1)/\log p} \left\lceil \frac{n}{p^j} \right\rceil \leq \sum_{\log n / \log p \leq j \leq \log(n^2+1)/\log p} . \tag{45}$$

Combining both inequalities, we have

$$\begin{aligned} \frac{1}{2}\alpha_p - \beta_p &\leq \sum_{j \leq \log n / \log p} + \sum_{\log n / \log p \leq j \leq \log(n^2+1)/\log p} &(46)\\ &= \sum_{1 \leq j \leq \log(n^2+1)/\log p} &(47)\\ &\leq \frac{\log\left(n^2+1\right)}{\log p} &(48) \end{aligned}$$

and we are done. □

Returning to the inequality established in (20), which is

$$\sum_{p \leq n} \beta_p \log p < \frac{1}{2} \sum_{p < 2n} \alpha_p \log p, \tag{49}$$

if we can establish that P_n is never a perfect square for n greater than or equal to some number, say λ, then we are done. Consequently, we just need to verify the initial claim for $1 \leq n \leq \lambda - 1$. We shall make use of two well-known ideas, which are namely the prime-counting function (related to the much celebrated Prime Number Theorem) and Bertrand's Postulate.

Definition 4.2. *The prime-counting function, $\pi(x)$, denotes the number of primes p less than or equal to x.*

Theorem 4.7. *The Prime Number Theorem provides an asymptotic relation for $\pi(n)$. That is, for large n,*

$$\pi(n) \sim \frac{n}{\log n}. \tag{50}$$

Theorem 4.8. *Bertrand's Postulate states that for every $n > 1$, there exists at least one prime p such that $n < p < 2n$.*

Chebyshev, Ramanujan and Erdős proved Bertrand's Postulate independently. We will discuss the proof by Erdős [5], but we need some lemmas before we can delve into the main result.

Lemma 4.5. *Define $r(p)$ such that it satisfies*

$$p^{r(p)} \leq 2n < p^{r(p)+1}. \tag{51}$$

Then,

$$\binom{2n}{n} \mid \sum_{p \leq 2n} p^{r(p)}. \tag{52}$$

Proof. Note that the number of integers less than n and divisible by m is $\lfloor n/m \rfloor$. Hence, the number of integers from 1 to n inclusive which are exactly a multiple of p^j is

$$\left\lfloor \frac{n}{p^j} \right\rfloor - \left\lfloor \frac{n}{p^{j-1}} \right\rfloor. \tag{53}$$

It is then clear that the exponent of p in $n!$ is

$$\sum_{j=1}^{k-1} j \left(\left\lfloor \frac{n}{p^j} \right\rfloor - \left\lfloor \frac{n}{p^{j+1}} \right\rfloor \right) + \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{j=1}^{k} \left\lfloor \frac{n}{p^j} \right\rfloor, \tag{54}$$

where k is such that it satisfies $p^k \leq n < p^{k+1}$. Hence, the exponent of p in $\binom{2n}{n}$ is

$$\sum_{j=1}^{r(p)} \left\{ \left\lfloor \frac{2n}{p^j} \right\rfloor - 2 \left\lfloor \frac{n}{p^j} \right\rfloor \right\} \leq \sum_{j=1}^{r(p)} \tag{55}$$

$$= r\left(p\right) \tag{56}$$

and the result follows. □

Lemma 4.6. *If $p > 2$ and $2n/3 < p \leq n$, then*

$$p \textit{ does not divide } \binom{2n}{n}. \tag{57}$$

Proof. The proof is quite obvious because if p satisfies the inequality $2n/3 < p \leq n$, then p occurs only once in the prime factorisation of $n!$. Suppose on the contrary otherwise and say that p occurs twice in that prime factorisation. Then, $2p \leq n$, so

$$p \leq \frac{n}{2} < \frac{2n}{3} < p, \tag{58}$$

which is a contradiction. Hence, p occurs twice in the prime factorisation of $(2n)!$ as $2n < 3p$. The result follows. □

Lemma 4.7. *For all $n \geq 2$,*

$$\prod_{p \leq n} p < 4^n. \tag{59}$$

Proof. We use strong induction. Let $P(n)$ denote the proposition (59). We omit the proofs for the base cases $P(2)$ and $P(3)$ as they are trivial.

For the induction hypothesis, assume that the proposition holds true for $P(2), P(3), \ldots, P(2m-1)$. A subtle yet key observation is that $m+1 < 2m-1$. As we assumed $P(2m-1)$ to be true, we shall prove that $P(2m)$ and $P(2m+1)$ are true.

For the former, note that for $m > 1$,

$$\begin{aligned} \prod_{p \leq 2m} p &= \prod_{p \leq 2m-1} p && (60) \\ &\leq 4^{2m-1} && (61) \\ &< 4^{2m} && (62) \end{aligned}$$

so $P(2m)$ is true.

For the latter, each prime in the interval $[m+2, 2m+1]$ is a factor of $\binom{2m+1}{m}$ as

$$\begin{aligned} \binom{2m+1}{m} &= \frac{(2m+1)!}{m!(m+1)!} && (63) \\ &= \frac{(2m+1)(2m)\ldots(m+2)}{m!} && (64) \end{aligned}$$

The primes in the interval $[m+2, 2m+1]$ do not appear in the denominator of (63), or rather (64). Also, aforementioned, $P(m+1)$ is assumed to be true, so

$$\begin{aligned} \prod_{p \leq 2m+1} p &= \prod_{m+2 \leq p \leq 2m+1} p \cdot \prod_{p \leq m+1} p && (65) \\ &\leq \binom{2m+1}{m} 4^{m+1} && (66) \end{aligned}$$

However, in the binomial expansion of $(1+1)^{2m+1}$, it is easy to see that

$$2^{2m+1} \geq 2\binom{2m+1}{m}. \tag{67}$$

As such,

$$\binom{2m+1}{m} < 4^m \tag{68}$$

and the result follows by the fact that

$$\prod_{p \leq 2m+1} p \leq 4^{2m+1}. \tag{69}$$

Hence, the lemma is proven by strong induction. □

We make use of the prime-counting function and Theorem 4.6 to find an upper bound for the sum of $\beta_p \log p$ in terms of $\alpha_p \log p$, where the sum is taken over appropriate values of p. We will state this in a while.

Definition 4.3. *Let $\pi(n,a,b)$ denote the number of primes less than or equal to n which satisfies $n \equiv a \pmod{b}$.*

Theorem 4.9.

$$\sum_{\substack{p \leq n \\ p \not\equiv 1 \pmod{4}}} \beta_p \log p \leq \frac{1}{2}\left\lceil \frac{n}{2} \right\rceil \log 2 + \log(n^2+1)\pi(n,1,4) + \frac{1}{2}\sum_{n<p<2n} \alpha_p \log p \tag{70}$$

We will not prove Theorem 4.9 in detail. The definition of $\pi(n,a,b)$ is crucial here since if $p \equiv 1 \pmod{4}$, then

$$\log p \sum_{\substack{p \leq n \\ p \equiv 1 \pmod{4}}} \left(\frac{1}{2}\alpha_p - \beta_p\right) \leq \log\left(n^2+1\right)\pi(n,1,4). \tag{71}$$

Also, note that $\lfloor n/2 \rfloor \log 2/2$ is just $\alpha_2 \log 2/2$, and the open interval $(n,2n)$ can be expressed as $(1,2n)\backslash(1,n]$.

Lemma 4.8. *If $p > n$, then $\alpha_p \leq 2$.*

Proof. We established the inequality

$$\alpha_p \leq \sum_{j \leq \log(n^2+1)/\log p} 2\left\lceil \frac{n}{p^j} \right\rceil \tag{72}$$

in (38). If $p > n$, then $n/p < 1$. A key observation is that

$$\log(n^2+1) < 2\log p, \tag{73}$$

which is a consequence of $n^2 + 1 < p^2$ (the inequality sign does not change because the logarithmic function is strictly increasing). The solution to this inequality yields

$$
\begin{aligned}
p^2 - n^2 &> 1 \qquad (74)\\
(p+n)(p-n) &> 1 \qquad (75)
\end{aligned}
$$

and this is justified because $p + n$ is obviously positive, and $p - n$ is also positive (because $p > n$). As such, for $j \leq \log(n^2 + 1)/\log p$, it would imply that $j < 2$, so there is only one value of j to consider in the sum for the case where $p > n$, and that is $j = 1$. We briefly discussed this earlier as $n/p < 1$, implying that $\lceil n/p \rceil \leq 1$. □

Lemma 4.9. *If $p \leq n$, then*

$$\beta_p \geq \frac{n-p}{p-1} - \frac{\log n}{\log p} \geq \frac{n-1}{p-1} - \frac{\log(n^2+1)}{\log p}. \tag{76}$$

Proof. Recall that (39) yields the equality

$$\beta_p = \sum_{j \leq \log n/\log p} \left\lfloor n/p^j \right\rfloor. \tag{77}$$

It is worth noting that

$$\frac{n-p}{p-1} = \frac{n}{p-1} - \frac{p}{p-1}. \tag{78}$$

Hence,

$$
\begin{aligned}
\beta_p &= \sum_{j \leq \log n/\log p} \left\lfloor n/p^j \right\rfloor && (79)\\
&\geq \sum_{j \leq \log n/\log p} \frac{n}{p^j} - \sum_{j \leq \log n/\log p} && (80)\\
&= n \sum_{j \leq \log n/\log p} \frac{1}{p^j} - \frac{\log n}{\log p} && (81)\\
&= n \sum_{j=1}^{\lfloor \log n/\log p \rfloor} p^{-j} - \frac{\log n}{\log p} && (82)\\
&= \frac{n}{p-1}\left(1 - \frac{1}{p^{\lfloor \log n/\log p \rfloor}}\right) - \frac{\log n}{\log p} && (83)\\
&= \frac{n}{p-1} - \frac{n}{p^{\lfloor \log n/\log p \rfloor}(p-1)} - \frac{\log n}{\log p} && (84)
\end{aligned}
$$

What is left to show is

$$\frac{n}{p^{\lfloor \log n/\log p \rfloor}(p-1)} \leq \frac{p}{p-1}. \tag{85}$$

In other words,

$$p^{\lfloor \log n/\log p\rfloor+1} \geq n, \tag{86}$$

which is clear because

$$\left\lfloor \frac{\log n}{\log p} \right\rfloor + 1 \geq \frac{\log n}{\log p} \tag{87}$$

and $p^{\log n/\log p} = n$. With these, the lower bound

$$\beta_p \geq \frac{n-p}{p-1} - \frac{\log n}{\log p} \tag{88}$$

is obtained.

Now, we show that

$$\frac{n-p}{p-1} - \frac{\log n}{\log p} \geq \frac{n-1}{p-1} - \frac{\log(n^2+1)}{\log p}. \tag{89}$$

Working backwards,

$$\frac{\log(n^2+1)}{\log p} \geq 1 + \frac{\log n}{\log p} \tag{90}$$

$$\log(n^2+1) \geq \log pn \tag{91}$$

$$n^2 - pn + 1 \geq 1 \tag{92}$$

$$n\,(n-p) \geq 0 \tag{93}$$

For the quadratic inequality $n(n-p) \geq 0$ in (93), since n is always positive, then $n - p \geq 0$, or equivalently, $n \geq p$, which is the condition stated in the lemma. □

Lemma 4.10.

$$(n-1) \sum_{\substack{p\leq n \\ p\not\equiv 1 \pmod 4}} \frac{\log p}{p-1} < (n+1)\,\frac{\log 2}{4} + \log\left(n^2+1\right)\pi\,(n) + \sum_{n<p<2n} \log p \tag{94}$$

Proof. We apply the estimates in Lemma 4.8 and Lemma 4.9 to Theorem 4.9, so

$$\sum_{\substack{p\leq n \\ p\not\equiv 1 \pmod 4}} \left(\frac{n-1}{p-1} - \frac{\log(n^2+1)}{\log p}\right)\log p < \frac{1}{2}\left\lceil \frac{n}{2} \right\rceil \log 2 + \log(n^2+1)\pi(n,1,4) + \sum_{n<p<2n} \log p. \tag{95}$$

As such, an strict upper bound for

$$(n-1) \sum_{\substack{p\leq n \\ p\not\equiv 1 \pmod 4}} \frac{\log p}{p-1} - \sum_{\substack{p\leq n \\ p\not\equiv 1 \pmod 4}} \log(n^2+1) \tag{96}$$

is

$$\frac{1}{2}\left\lceil\frac{n}{2}\right\rceil \log 2 + \log(n^2+1)\pi(n,1,4) + \sum_{n<p<2n} \log p \tag{97}$$

and (71) evaluates to

$$(n+1)\,\frac{\log 2}{4} + \log(n^2+1)\pi(n) + \sum_{n<p<2n} \log p, \tag{98}$$

yielding the desired result. □

5 Chebyshev's Inequalities

Chebyshev's Functions play a pivotal role in Analytic Number Theory. Here, we will discuss the First and Second Chebyshev Functions, denoted by (n) and $\psi(n)$ respectively.

Definition 5.1. *For the von Mangoldt Function $\Lambda(n)$, for every integer $n \geq 1$, define*

$$\Lambda\left(n\right) = \begin{cases} \log p & \textit{if } n = p^m \textit{ for some prime } p \textit{ and some } m \geq 1, \\ 0 & \textit{otherwise.} \end{cases}$$

Definition 5.2. *The First Chebyshev Function, denoted by $\vartheta(n)$, states that for any real number $n \geq 1$,*

$$\vartheta(n) = \sum_{p \leq n} \log p. \tag{99}$$

Definition 5.3. *The Second Chebyshev Function, denoted by $\psi(n)$, states that for any real number $n \geq 1$,*

$$\psi(x) = \sum_{n \leq x} \Lambda(n) = \sum_{p^m \leq x} \log p. \tag{100}$$

Lemma 5.1. *For all $n \geq 1$, $\vartheta(n) \leq \psi(n)$ [2].*

Proof. It is clear by the definitions of $\vartheta(n)$ and $\psi(n)$ that

$$\psi(n) = \vartheta(n) + \vartheta\left(\sqrt{n}\right) + \vartheta\left(\sqrt[3]{n}\right) + \dots. \tag{101}$$

The result follows. □

Corollary 5.1. *If p is prime, then*

$$\vartheta(n) \leq \pi(n) \log n \ [7]. \tag{102}$$

Proof. Using Lemma 4.1, as $\vartheta(n) \leq \psi(n)$, by definition of $\psi(n)$, we have

$$\psi(n) = \sum_{p \leq n} \left\lfloor \frac{\log n}{\log p} \right\rfloor \cdot \log p \tag{103}$$

$$\leq \sum_{p \leq n} \frac{\log n}{\log p} \cdot \log p \tag{104}$$

$$= \sum_{p \leq n} 1 \cdot \log n \tag{105}$$

$$= \pi(n) \log n \tag{106}$$

This shows that the First Chebyshev Function is closely related to the prime-counting function. □

Theorem 5.1. *If p is prime, then*

$$\sum_{n<p<2n} \log p \leq \vartheta(2n-1). \tag{107}$$

Proof. This is quite obvious as the sum of $\log p$ over the interval $n < p < 2n$ is $\vartheta(2n-1) - \vartheta(n)$, and the result follows. □

Theorem 5.2. *For all $\varepsilon > 0$, there exists $M > 0$ such that for all $n > M$,*

$$\pi(n) < (1+\varepsilon)\frac{n}{\log n} \text{ [5]}. \tag{108}$$

Theorem 5.3. *An upper bound for $\log p/(p-1)$ is established, and it is given by the inequality*

$$\sum_{\substack{p \leq n \\ p \not\equiv 1 \pmod 4}} \frac{\log p}{p-1} < 4 + \frac{\log 2}{4} \text{ [4]}. \tag{109}$$

Proof.

$$\sum_{\substack{p \leq n \\ p \not\equiv 1 \pmod 4}} \frac{\log p}{p-1} < \frac{n+1}{n-1} \cdot \frac{\log 2}{4} + \frac{\log\left(n^2+1\right)}{n-1}\pi\left(n\right) + \frac{1}{n-1}\sum_{n<p<2n} \log p \tag{110}$$

$$< \frac{n+1}{n-1} \cdot \frac{\log 2}{4} + (1+\varepsilon) \cdot \frac{n}{n-1} \cdot \frac{\log\left(n^2+1\right)}{\log n} + \frac{1}{n-1}\vartheta(2n-1) \tag{111}$$

$$< \frac{n+1}{n-1} \cdot \frac{\log 2}{4} + (1+\varepsilon) \cdot \frac{n}{n-1} \cdot \frac{\log\left(n^2+1\right)}{\log n} + \frac{1}{n-1}(1+\varepsilon)\frac{2n-1}{\log\left(2n-1\right)} \cdot \log\left(2n-1\right) \tag{112}$$

$$= \frac{n+1}{n-1} \cdot \frac{\log 2}{4} + (1+\varepsilon) \cdot \frac{n}{n-1} \cdot \frac{\log\left(n^2+1\right)}{\log n} + (1+\varepsilon) \cdot \frac{2n-1}{n-1} \tag{113}$$

For large n, (86) evaluates to (L'Hôpital's Rule is useful here)

$$\frac{\log 2}{4} + 4(1+\varepsilon). \tag{114}$$

Taking $\varepsilon > 0$ to be arbitrarily small, we see that (109) follows. □

In Cilleruelo's proof [4], he cited different bounds used by Hardy and Wright in the textbook 'An Introduction to the Theory of Numbers (1980)'. We obtained a better bound as mentioned in (114) in our proof although it does not really affect the computation. At this stage, note that $4 + \log 2/4 \approx 4.1732$. For $n \geq 1831$, we obtain the inequality

$$\sum_{\substack{p \leq n \\ p \not\equiv 1 \pmod 4}} \frac{\log p}{p-1} > 4.1732, \tag{115}$$

so we have verified Theorem 4.2 for $n \geq 1831$.

It is worth appreciating the following fact about the function $\log p/(p-1)$.

Theorem 5.4. *We have*

$$\sum_{p \leq n} \frac{\log p}{p-1} = \log n + \mathcal{O}(1) \text{ [9]}, \tag{116}$$

where $\mathcal{O}$ denotes the Big O Notation.

Theorem 5.4 implies that the execution time of this computation is independent of the size of the input. We provide a proof of this theorem.

Proof.

$$\begin{aligned} \sum_{p \leq n} \frac{\log p}{p-1} - \frac{\log p}{p} &= \sum_{p \leq n} \log p \left(\frac{1}{p\,(p-1)} \right) && (117) \\ &\ll \sum_{p \leq n} \frac{\log n}{n\,(n-1)} && (118) \\ &\ll 1 && (119) \end{aligned}$$

Hence,

$$\sum_{p \leq n} \frac{\log p}{p-1} = \sum_{p \leq n} \frac{\log p}{p} \tag{120}$$

and this is bounded above by $\log n + \mathcal{O}(1)$. □

Corollary 5.2. *The sum*

$$\sum_{p \leq n} \frac{\log p}{p-1} \tag{121}$$

diverges for $p \geq 2$.

Even though it seems that the growth rate of $\log p/(p-1)$ (here, we did not impose the condition that $p \not\equiv 1 \pmod 4$ unlike Theorem 4.3), it is interesting that this sum over all $p \geq 2$ diverges, which is analogous to the case of the harmonic series. Moreover, if one were to attempt to prove Corollary 5.2 using the integral test, it would be futile. Back to $\log p/(p-1)$, if we take the sum of all such primes p such that they are not congruent to 1 modulo 4, it actually converges but at a very slow rate. Recall that convergence was established in (114).

Definition 5.4. *The harmonic series is defined to be the infinite series*

$$\sum_{n=1}^{\infty} \frac{1}{n} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \dots \tag{122}$$

Theorem 5.5. *The harmonic series is divergent.*

Now, it suffices to prove the remaining theorem.

Theorem 5.6. *P_n is not a perfect square for $4 \leq n \leq 1830$.*

Proof. We use Lemma 3.1. We deal with primes that are congruent to 1 modulo 4. Note that $17 = 4^2 + 1$ and $17 \equiv 1 \pmod 4$. The next time 17 divides $k^2 + 1$ occurs when $k = 17 - 4 = 13$. Thus, P_n is not a perfect square for $4 \leq n \leq 12$. Next, $101 = 10^2+1$ and $101 \equiv 1 \pmod 4$. The next time 101 divides k^2+1 occurs when $k = 101-10 = 91$, so P_n is not a perfect square for $10 \leq n \leq 90$. Next, $1297 = 36^2+1$. The next time 1297 divides k^2+1 occurs when $k = 1297-36 = 1261$. Hence, P_n is not a square for $36 \leq n \leq 1260$.

What is left to show is that P_n is not a perfect square for $1260 \leq n \leq 1830$. This can be easily shown. □

To wrap it up, Theorem 4.2 holds true and the only solution to Problem 3.1 is $(b, n) = (10, 3)$.

6 Extensions

Other similar problems have been discussed on the Internet.

Problem 6.1 was discussed by Russelle Guadalupe [6] from the University of the Philippines-Diliman.

Problem 6.1. *Let l be a positive odd integer. Establish a lower bound N_l depending on l such that for all $n \geq N_l$,*

$$\prod_{k=1}^{N} \left(2k^2 + l\right) \tag{123}$$

is non-square. As an application, determine all values of n such that the product in (123) is square for certain values of l.

Problem 6.2 was discussed by Zhang Wenpeng and Wang Tingting [11] from Northwest University.

Problem 6.2. *A positive integer t is called a powerful number if $t > 1$ and $p^2 \mid t$ for every prime divisor p of t. Define $\Omega_k(n)$ to be*

$$\Omega_k(n) = \prod_{a=1}^{n} \left(a^k + 1\right). \tag{124}$$

If k is an odd prime with $k \geq 5$, then $\Omega_k(n)$ is not a powerful number.

Problem 6.3 was discussed by Chen Yonggao and Gong Mingliang [3] from Nanjing Normal University.

Problem 6.3. *For any odd integer ℓ with at most two distinct prime factors and any positive integer n, the product*

$$\prod_{k=1}^{n} \left(k^\ell + 1\right) \tag{125}$$

is not a powerful number. Also, for any integer $r \geq 1$, there exists a positive integer T_r such that if ℓ is a positive odd integer with at most r distinct prime factors and n is an integer with $n \geq T_r$, then the product in (125) is not a powerful number.

References

[1] T. Amdeberhan, L. A. Medina, and V. H. Moll. "Arithmetical properties of a sequence arising from an arctangent sum". In: *Journal of Number Theory* 128.6 (2008), pp. 1807–1846. DOI: doi:10.1016/j.jnt.2007.05.008.

[2] T. M. Apostol. *Introduction to Analytic Number Theory*. Undergraduate Texts in Mathematics. Springer, 1976, p. 76. ISBN: 9781441928054.

[3] Y. Chen and M. Gong. "On the products $(1^\ell+1)(2^\ell+1)\dots(n^\ell+1)$". In: *Journal of Number Theory* 144 (2014), pp. 176–187. DOI: http://dx.doi.org/10.1016/j.jnt.2012.05.025.

[4] J. Cilleruelo. "Squares in $(1^2+1)\dots(n^2+1)$". In: *Journal of Number Theory* 128.8 (2008), pp. 2488–2491. DOI: doi:10.1016/j.jnt.2007.11.001.

[5] D. Galvin. *Erdős's proof of Bertrand's postulate*. 2015. URL: https://www3.nd.edu/~dgalvin1/pdf/bertrand.pdf.

[6] R. Guadalupe. "Squares of the form $\prod_k^n \left(2k^2+1\right)$ with l odd". In: *arXiv* (2022), pp. 1–2. DOI: arXiv:2201.00501.

[7] Stamatopoulos N. and Zhiang W. *Chebyshev's theorem on the distribution of prime numbers*. 2021. URL: https://metaphor.ethz.ch/x/2021/hs/401-3110-71L/ex/eighth.pdf.

[8] Singapore Mathematical Society. *CWMI 2017*. URL: https://sms.math.nus.edu.sg/Simo/CWMO/CWMO-2017_files/Problems_2017.pdf.

[9] L. Villavicencio. *Sum of primes over* $\log p/(p-1)$. 2017. URL: https://math.stackexchange.com/questions/2315585/sum-over-primes-of-log-p-p-1.

[10] C. Vincent. *Solving* $x^2 \equiv a \pmod{n}$. 2017. URL: https://www.uvm.edu/~cvincen1/files/teaching/spring2017-math255/quadraticequation.pdf.

[11] W. Zhang and T. Wang. "Powerful numbers in $(1^k+1)(2^k+1)\dots(n^k+1)$". In: *Journal of Number Theory* 132.11 (2012), pp. 2630–2635. DOI: http://dx.doi.org/10.1016/j.jnt.2012.05.025.