A Theorem on Prime Numbers with Applications in Proving Irreducibility

Author: Isobel Davies
Supervisor: Dr Brian Winn
Module Code: 19MAD300
May 2020
Loughborough University

Abstract

This thesis explores Schur's work from 1929, in which he proves a theorem on prime numbers and two other theorems on irreducibility. In particular, it follows from Schur's work that Hermite polynomials are irreducible. This thesis focuses on the algebraic and arithmetical tools Schur used, introducing algebraic number theory and the distribution of prime numbers. Some results on intervals containing primes are also given.

Acknowledgements

I would like to thank my supervisor Dr Brian Winn for introducing me to Schur's work and for his enthusiasm and helpful discussion. I would also like to thank Szymon Łopaciuk and Manuel Wehrsig for their support both personally and academically.

Contents

0 Notation

$\mathbb{N} = \{1, 2, 3, 4 \ldots\}$ = the set of natural numbers.
$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ = the set of integers.
$\mathbb{P} = \{2, 3, 5, 7, 11 \ldots\}$ = the set of prime numbers.
$\mathbb{Q}$ = the set of rational numbers.
$\mathbb{R}$ = the set of real numbers.

$u_{2n} = (2n-1)!! = 1 \cdot 3 \cdot 5 \cdot 7 \cdots (2n-1)$.
More information on this can be found in Section 6.2.

1 Introduction

1.1 Some Background

In 1929, Issai Schur wrote two papers, both of the name *Einige Sätze über Primzahlen mit Anwendugen auf Irreduzibilitätsfragen* which roughly translates to *Some theorems on prime numbers with applications in proving irreducibility.*
An important consequence of this work is that Hermite polynomials are irreducible. This thesis transports the reader back to 1929 for an in depth look at the content of these papers as well as an introduction to the theory upon which Schur's proofs depend.

1.2 Outline

In the first paper, Schur proves some results on the distribution of prime numbers, in particular, Schur gives and proves an approximation for the prime counting function. The prime counting function is defined in Section 2.1 and Schur's approximation is given in Section 2.2. Schur also proves that the interval $x < p \leq \frac{5}{4}x$ will always contain a prime number p for $x \geq 29$, the proof of which is given in Section 2.3. Inspired by Schur's work, the final section of this thesis investigates the distribution of prime numbers from a modern point of view.
In the second paper, Schur proves the following theorem on sequences of consecutive odd numbers and the prime factors of their terms.

Theorem 1.
For $k \in \mathbb{N}$ $(k > 2)$ such that $p = 2k + 1 \in \mathbb{P}$ $(p > 5)$, it is true that any sequence of k consecutive odd numbers, for which all terms are greater than $2k + 1$, will contain at least one term with a prime factor greater than $2k + 1$. For $p = 3$, the only counterexamples are powers of $3^\alpha > 3$ and for $p = 5$, the only counterexample is 25, 27.

In Section 7, the proof of this theorem is given which not only uses the theory of the distribution of prime numbers, developed in Section 2 but also an understanding of how to solve the Pell equation $x^2 - Dy^2 = 4$ and Størmer's theorem, on P-smooth numbers. These are the subjects of Sections 3 and 4, respectively.
Schur suggests that if the above theorem is true for $2k+1 \in \mathbb{P}$, then it is also true for all $2k+1 \in \mathbb{N}$. This is presented as a corollary in Section 7.2.

Corollary 1 (Corollary of Theorem 1)**.**
For $k \in \mathbb{N}$ $(k > 2)$, it is true that any sequence of k consecutive odd numbers, for which all terms are greater than $2k+1$, will contain at least one term with a prime factor greater than $2k+1$. For $k = 1$, the only counterexamples are powers of $3^\alpha > 3$ and for $k = 2$, the only counterexample is 25, 27.

Schur also proves the following two theorems on irreducibility, which follow from the above corollary.

Theorem 2.
For $n > 1$, every polynomial of the form

$$f(x) = 1 + g_1\frac{x^2}{u_2} + g_2\frac{x^4}{u_4} + \cdots + g_{n-1}\frac{x^{2n-2}}{u_{2n-2}} \pm \frac{x^{2n}}{u_{2n}}$$

with $g_\nu \in \mathbb{Z}$, is irreducible over $\mathbb{Q}$.

Theorem 3.
Every polynomial of the form

$$g(x) = 1 + g_1\frac{x^2}{u_4} + g_2\frac{x^4}{u_6} + \cdots + g_{n-1}\frac{x^{2n-2}}{u_{2n}} \pm \frac{x^{2n}}{u_{2n+2}}$$

with $g_\nu \in \mathbb{Z}$, is irreducible over $\mathbb{Q}$, except for the case that $2n = 3^r - 1$ for some $r \geq 2$. In this case, $g(x)$ has just one factor $x^2 \pm 3$ and division by this factor results in an irreducible polynomial over $\mathbb{Q}$.

The proofs of these theorems are presented in Section 8. It is necessary to understand some algebraic number theory before understanding these proofs, this is therefore the subject of Section 5. Schur uses these two theorems to show that Hermite polynomials are irreducible. This is presented as a corollary in Section 8.3.

Corollary 2 (Corollary of Theorems 2 and 3)**.**
The m^{th} Hermite polynomial

$$H_m(x) = (-1)^m e^{\frac{x^2}{2}} \cdot \frac{d^m e^{-\frac{x^2}{2}}}{dx^m}$$

is irreducible over $\mathbb{Q}$ for even $m > 2$ and irreducible after division by x for odd m.

Hermite polynomials are a classical sequence of orthogonal polynomials. More information on Hermite polynomials and orthogonal polynomials in general can be found in [15].

1.3 How to Read This Thesis

If you are interested in understanding the proofs of the above theorems, you could start with Sections 7 and 8, referring back to the introductory sections where necessary. The proof has not only been translated into english but also treated in much more detail, in order to make Schur's work more accesible. Schur's original proofs can be found in [13]. For an introduction to the Pell equation and algebraic number theory, you could start with Sections 3 and 5. More information on the history of the Pell equation and its connection to algebraic number theory can be found in [4]. Finally, if you are interested in the distribution of prime numbers, you may like to read Sections 2 and 9 for a comparison of results from 1929 and modern results.

2 The Distribution of Prime Numbers

Schur makes use of several functions related to the distribution of prime numbers in his work. In this section, these functions are introduced as well as the approximations that Schur uses in his work. At the end of this section, the proof of the first Lemma needed in order to prove Theorem 1 is also presented.

2.1 Prime Number Functions

Definition 1. *The prime counting function $\pi(x)$ is defined to be the number of prime numbers p in the interval $2 \leq p \leq x$. e.g. $\pi(10) = 4$.*
Note that $\pi(x) = \sum_{\substack{p \in \mathbb{P} \\ 2 \leq p \leq x}} 1$.

Definition 2. *The prime gaps function Δp gives the gap between consecutive prime numbers p and p' (with $p' > p$)*

$$\Delta p = p' - p.$$
$$e.g.\ \ \Delta 13 = 17 - 13 = 4.$$

Definition 3. *The function $L(x)$ gives the length of the longest sequence of consecutive composite numbers up to and including x. e.g. $L(10) = 3$.*

Remark 1. *If $M(x) = \max\{\Delta p : 2 \leq p \leq x\}$, then*

$$L(p^*) = M(p^*) - 1.$$

for any $p^* \in \mathbb{P}$.

Definition 4. *The first Chebyshev function $\vartheta(x)$ is defined to be* $\vartheta(x) = \sum_{2 \leq p \leq x} \log p$.
e.g. $\vartheta(6) = \log 2 + \log 3 + \log 5 = \log 30$.

Definition 5. *The second Chebyshev function $\psi(x)$ is defined to be* $\psi(x) = \sum_{2 \leq p^k \leq x} \log p$.
e.g. $\psi(6) = \log 2 + \log 3 + \log 2 + \log 5 = 2\log 2 + \log 3 + \log 5 = \log 60$.

Remark 2. *Sometimes it is useful to define $\psi(x)$ in one of the following alternative (but equivalent) ways:*

$$\psi(x) = \sum_{2 \leq p \leq x} [\log_p x] \log p,$$
$$\psi(x) = \sum_{n=1}^{\infty} \vartheta(x^{\frac{1}{n}}).$$
$$\begin{aligned} e.g.\ \ \psi(6) &= \vartheta(6) + \vartheta(\sqrt{6}) + \cdots \\ &= (\log 2 + \log 3 + \log 5) + (\log 2) + 0 + 0 + \cdots \\ &= 2\log 2 + \log 3 + \log 5. \end{aligned}$$

2.2 Approximations

Schur proves and uses the following approximation in his work.

Approximation 1 (Schur [12])**.**

$$\pi(x) < \frac{3}{2}\frac{x}{\log x},$$

for $x \geq 2$.

Schur also uses approximations for the Chebyshev functions, given by Landau.

Approximation 2 (Landau [5])**.**

$$\vartheta(x) < \frac{6}{5}ax + 3\log^2 x + 8\log x + 5,$$
$$\vartheta(x) \geq ax - \frac{12}{5}a\sqrt{x} - \frac{3}{2}\log^2 x - 13\log x - 15$$

for $x \geq 1$, *where* $a = \log\left(\frac{2^{\frac{1}{2}}\cdot 3^{\frac{1}{3}}\cdot 5^{\frac{1}{5}}}{30^{\frac{1}{30}}}\right) = 0.92129\ldots$

Approximation 3 (Landau [5])**.**

$$\psi(x) < \frac{6}{5}ax + 3\log^2 x + 8\log x + 5,$$
$$\psi(x) \geq ax - 5\log x - 5$$

for $x \geq 1$ *where* a *is defined as in Approximation 2.*

Schur used a table of prime numbers up to 300000, in order to give the following approximations of Δp for certain ranges of p

Approximation 4.

$$\Delta p < 1000 \text{ for } p < 162754,$$
$$\Delta p < 100 \text{ for } p < 4000,$$
$$\Delta p \leq 14 \text{ for } p < 400$$

and the following approximations of $L(x)$ for certain values of x.

Approximation 5.

$$L(300000) < 2000,$$
$$L(100000) < 1000,$$
$$L(50000) < 100,$$
$$L(5000) < 47.$$

2.3 Intervals Containing Primes

Bertrand's Postulate.
For $x > 1$ there exists at least one prime number p in the interval

$$x < p \leq 2x.$$

Since Bertrand's Postulate was proven, other intervals have been found for which there must exist a prime number. Schur proves the following Lemma, which he then uses for the proof of Theorem 1.

Lemma 1 (Schur [12])**.**
For $x \geq 29$ there exists at least one prime number p such that

$$x < p \leq \frac{5}{4}x.$$

Proof of Lemma 1.
Since $y^2 - 8y - 5$ is positive for $y > 10$, it follows that

$$3y^2 + 8y + 5 < 4y^2$$

holds for $y > 10$.
Similarly,

$$\frac{3}{2}y^2 + 13y + 15 < 3y^2$$

holds for $y > 10$.
Letting $y = \log x$ implies that

$$3\log^2 x + 8\log x + 5 < 4\log^2 x,$$
$$\frac{3}{2}\log^2 x + 13\log x + 15 < 3\log^2 x$$

hold for $x > e^{10}$ and therefore from Approximation 2, it follows that

$$\vartheta(x) < \frac{6}{5}ax + 4\log^2 x,$$
$$\vartheta(x) > ax - \frac{12}{5}a\sqrt{x} - 3\log^2 x$$

for $x > e^{10}$.
Using this approximation, we find that

$$\vartheta\left(\frac{5x}{4}\right) - \vartheta(x) > \frac{1}{20}ax - \frac{12}{5}a\sqrt{\frac{5x}{4}} - 3\log^2\frac{5x}{4} - 4\log^2 x,$$

for $x > e^{10}$.
Using the fact that

$$\log\left(1+\frac{1}{4}\right) < \frac{1}{4},$$
$$\frac{12}{5}\sqrt{\frac{5}{4}} < \frac{14}{5}$$

it follows that

$$\vartheta\left(\frac{5x}{4}\right) - \vartheta(x) > \frac{1}{20}g(x)$$

for $x > e^{10}$, where

$$g(x) = ax - 56a\sqrt{x} - 140\log^2 x - 30\log x - 4.$$

Note that $\dfrac{g(x)}{x}$ is monotonically increasing for $x > e^2$, then it follows that for $x > e^{12}$

$$\begin{aligned}\vartheta\left(\frac{5x}{4}\right) - \vartheta(x) &> \frac{1}{20}g(x)\\ &> \frac{1}{x}g(x)\\ &> 0\end{aligned}$$

since $g(e^{12}) > 0$.
The fact that $\vartheta\left(\frac{5x}{4}\right) - \vartheta(x) > 0$ for $x > e^{12}$ means that there must exist a prime number in the interval $x < p \leq \frac{5}{4}x$ and we have therefore proven the Lemma for $x > e^{12}$=162754.79....

It is left to prove the Lemma for values of x in the interval $29 \leq x \leq 162754$. For this section, we make use of the function Δp as defined in Definition 2. If we are able to prove that

$$\Delta p < \frac{p}{4} \tag{1}$$

for prime numbers in the interval $29 \leq p < 162754$, then the Lemma is proven. We know from Approximation 4 that for $p < 162754$, $\Delta p < 1000$ so if (1) were not true for some p, then

$$1000 > \Delta p \geq \frac{p}{4}$$

and $p < 4000$ must be true. It follows that (1) is true for $4000 < p < 162754$ and it is left to investigate $29 \leq p < 4000$.
We also know from Approximation 4 that for $p < 4000$, $\Delta p < 100$ so we know that (1) holds for $400 < p < 4000$ and it is left to investigate $29 \leq p < 400$.
Finally, from Approximation 4, we know that for $p < 400$, $\Delta p \leq 14$ so we know that (1) holds for $56 < p < 400$ and it is left to investigate $29 \leq p < 56$.
There are only seven prime numbers in this interval, so it is easy to verify that (1) holds for each of them. □

3 The Pell Equation $x^2 - Dy^2 = 4$

In order to understand Schur's proof of Lemma 2, it is necessary to be able to solve the Pell Equation $x^2 - Dy^2 = 4$. This section focuses on this Pell Equation, in particular, the properties of its solutions and how these can be used to generate all solutions.

We are looking for integer solutions to the Pell Equation $x^2 - Dy^2 = 4$, where D is a non-square positive integer. We represent solutions in two different ways: either (x, y) or

$$\frac{x + y\sqrt{D}}{2}.$$

The trivial solution is $(x_0, y_0) = (2, 0)$. A solution for which x and y are both positive is called a positive solution.

Pell Property 1.
Let (x_1, y_1) and (x_2, y_2) be two positive solutions of $x^2 - Dy^2 = 4$. Then,

$$x_1 > x_2 \iff y_1 > y_2.$$

Proof of Pell Property 1.
In order for (x, y) to be a positive solution, $x > 2$, $y > 0$. The statement therefore follows from the fact that

$$y = \sqrt{\frac{x^2 - 4}{D}}$$

is strictly increasing for $x > 2$, $y > 0$. □

It follows that finding the smallest positive solution is equivalent to minimising x *or* minimising y.

Definition 6 (Fundamental Solution)**.**
If (x_1, y_1) is the smallest positive solution of $x^2 - Dy^2 = 4$, then (x_1, y_1) is called the fundamental solution of $x^2 - Dy^2 = 4$.

In order to find the fundamental solution, one could look for solutions for $y = 1, 2, 3, \ldots$. The first solution one finds would be the fundamental solution. This method by "brute force" suffices for understanding the proof of Lemma 2, since every Pell equation used, has a small fundamental solution ($1 \leq y \leq 4$). However, in general this method is poor and I encourage the reader to explore alternative methods. For example, Lagrange developed a method for finding the fundamental solution of $x^2 - Dy^2 = z$ for some integer z (also known as the generalised Pell equation), a description of this method can be found in [8].

Pell Property 2.
The following expression

$$\frac{x_* + y_*\sqrt{D}}{2}$$

is a solution of $x^2 + Dy^2 = 4$ *if and only if*

$$\frac{x_* - y_*\sqrt{D}}{2}, \quad \frac{-x_* + y_*\sqrt{D}}{2}, \quad \frac{-x_* - y_*\sqrt{D}}{2}.$$

are also solutions of $x^2 + Dy^2 = 4$.

Proof of Pell Property 2.
Follows trivially from the fact that $(x_*)^2 = (-x_*)^2$ and $(y_*)^2 = (-y_*)^2$. □

It follows from Pell Property 2 that if we find all positive solutions, then we are able to find all solutions.

Pell Property 3.
The product of any two solutions of $x^2 - Dy^2 = 4$ *is also a solution of* $x^2 - Dy^2 = 4$.

Proof of Pell Property 3.
Suppose (x_1, y_1) and (x_2, y_2) are arbitrary solutions of $x^2 - Dy^2 = 4$, then

$$\left(\frac{x_1 + y_1\sqrt{D}}{2}\right) \cdot \left(\frac{x_2 + y_2\sqrt{D}}{2}\right) = \frac{x_1x_2 + x_1y_2\sqrt{D} + x_2y_1\sqrt{D} + y_1y_2D}{4}.$$

Therefore, it is left to show that

$$(x_3, y_3) = \left(\frac{x_1x_2 + y_1y_2D}{2}, \frac{x_1y_2 + x_2y_1}{2}\right)$$

is a solution of $x^2 - Dy^2 = 4$, which can be easily verified:

$$\begin{aligned} x_3^2 - Dy_3^2 &= \frac{x_1^2x_2^2 + 2x_1x_2y_1y_2D + y_1^2y_2^2D^2}{4} - D\frac{x_1^2y_2^2 + 2x_1x_2y_1y_2 + x_2^2y_1^2}{4} \\ &= \frac{x_1^2x_2^2 + y_1^2y_2^2D^2 - Dx_1^2y_2^2 - Dx_2^2y_1^2}{4} \\ &= \frac{(x_1^2 - Dy_1^2)(x_2^2 - Dy_2^2)}{4} \\ &= 4. \end{aligned}$$

□

It follows from this that if (x_*, y_*) is a solution of $x^2 - Dy^2 = 4$, then we are able to generate infinitely many solutions.

Pell Property 4.
For any solution (x_*, y_*) of $x^2 - Dy^2 = 4$, it follows that

$$\left(\frac{x_* + y_*\sqrt{D}}{2}\right)^{-n} = \left(\frac{x_* - y_*\sqrt{D}}{2}\right)^{n}.$$

Proof of Pell Property 4.
If $x_*^2 - Dy_*^2 = 4$, then

$$\begin{aligned}\left(\frac{x_* + y_*\sqrt{D}}{2}\right)^{-n} &= \left(\frac{2}{x_* + y_*\sqrt{D}}\right)^{n} \\ &= \left(\frac{2(x_* - y_*\sqrt{D})}{x_*^2 - y_*^2 D}\right)^{n} \\ &= \left(\frac{x_* - y_*\sqrt{D}}{2}\right)^{n}.\end{aligned}$$

□

Pell Property 5.
If (x_1, y_1) is the fundamental solution of $x^2 - Dy^2 = 4$, then all positive solutions are given by

$$\frac{x_n + y_n\sqrt{D}}{2} = \left(\frac{x_1 + y_1\sqrt{D}}{2}\right)^{n} \quad n \in \mathbb{N} \tag{2}$$

Proof of Pell Property 5.
If (x_1, y_1) is the fundamental solution, then x_n and y_n are clearly positive and it follows from Pell Property 3 that (x_n, y_n) is a positive solution of $x^2 - Dy^2$. It is left to show that (2) gives *all* positive solutions.
Suppose $x_* + y_*\sqrt{D}$ is a positive solution of $x^2 - Dy^2 = 4$, that is not equal to some power of the fundamental solution, then

$$\left(\frac{x_1 + y_1\sqrt{D}}{2}\right)^{n} < \left(\frac{x_* + y_*\sqrt{D}}{2}\right) < \left(\frac{x_1 + y_1\sqrt{D}}{2}\right)^{n+1}$$

for some $n \in \mathbb{N}$.
If follows that,

$$1 < \left(\frac{x_* + y_*\sqrt{D}}{2}\right) \cdot \left(\frac{x_1 + y_1\sqrt{D}}{2}\right)^{-n} < \left(\frac{x_1 + y_1\sqrt{D}}{2}\right).$$

It follows then, from Pell Property 4 that,

$$1 < \left(\frac{x_* + y_*\sqrt{D}}{2}\right) \cdot \left(\frac{x_1 - y_1\sqrt{D}}{2}\right)^{n} < \left(\frac{x_1 + y_1\sqrt{D}}{2}\right).$$

Since $(x_1, -y_1)$ is a solution, by Pell Property 2, it follows from Pell Property 3 that there exists a positive solution of $x^2 - Dy^2 = 4$ which is less than the fundamental solution. This cannot be true and therefore there cannot be a positive solution which is not equal to some power of the fundamental solution. □

At this point, one may falsely conjecture that all generalised Pell equations can be solved in this manner. Whilst this may not be true, there are several methods that will solve any generalised Pell equation, see [1] for an example of such a method.

Pell Property 6.
If (x_n, y_n) is the smallest positive solution of $x^2 - Dy^2 = 4$ such that y_n is divisible by some given m, then for all solutions (x_{qn}, y_{qn}), $q \in \mathbb{N}$, y_{qn} will be divisible by y_n and therefore m. Furthermore, for all solutions $(x, y) \neq (x_{qn}, y_{qn})$, y is not divisible by m.

Proof of Pell Property 6.
Using Pell Property 5 it is clear that y_{qn} is divisible by y_n $\forall q \in \mathbb{N}$ as,

$$\begin{aligned}\frac{x_{qn} + y_{qn}\sqrt{D}}{2} &= \left(\frac{x_1 + y_1\sqrt{D}}{2}\right)^{nq} \\ &= \left(\frac{x_n + y_n\sqrt{D}}{2}\right)^{q},\end{aligned}$$

and therefore if y_n is divisible by m then y_{qn} will be divisible by m $\forall q \in \mathbb{N}$.
Suppose there exists a positive solution (x_r, y_r) of $x^2 - Dy^2 = 4$ where y_r is also divisible by m but r is not a multiple of n. Then, there must exist $q_* \in \mathbb{N}$ such that $n \leq q_* n < r < (q_* + 1)n$. However, this means that,

$$\left(\frac{x_1 + y_1\sqrt{D}}{2}\right)^{r - q_* n} < \left(\frac{x_1 + y_1\sqrt{D}}{2}\right)^{n}.$$

Let $s = r - q_* n$. Since $1 \leq s < n$ and $s \in \mathbb{N}$, it follows from Pell Property 5 that (x_s, y_s) will be a positive solution of $x^2 - Dy^2 = 4$ smaller than (x_n, y_n).
From Pell Property 4 we know that

$$\left(\frac{x_1 + y_1\sqrt{D}}{2}\right)^{s} = \left(\frac{x_r + y_r\sqrt{D}}{2}\right)\left(\frac{x_{q_* n} - y_{q_* n}\sqrt{D}}{2}\right).$$

Since y_r and $y_{q_* n}$ are divisible by m, y_s is clearly also divisible by m which contradicts the fact that $(x, y) = (x_n, y_n)$ is the smallest positive solution such that y divides m. As a result, no such y_r can exist, i.e. only y_{qn} will be divisible by m. □

4 Størmer's Method

Definition 7. *We define P to be a set of prime numbers*

$$P = \{p_1, p_2, \ldots\} \subset \mathbb{P}.$$

Then, a positive integer is called P-smooth if and only if all of its prime factors are contained in P.

Example 1. A $\{3\}$-smooth number is any number of the form 3^α, for example 27 is a 3-smooth number.

Example 2. A $\{2, 3, 5\}$-smooth number is any number of the form $2^\alpha 3^\beta 5^\gamma$, for example, $6, 15, 16$ and 72 are all $\{2, 3, 5\}$-smooth numbers.

Note that P-smooth numbers don't need to be divisible by *every* element of P.

Størmer's Theorem (Størmer [14])**.** *For any set $P \subset \mathbb{P}$ there are only finitely many consecutive P-smooth pairs.*

Example 3. The only consecutive pairs of $\{2, 3\}$-smooth numbers are

$$1, 2 \quad 2, 3 \quad 3, 4 \quad 8, 9$$

The proof of Størmer's Theorem is often referred to as Størmer's Method as it not only proves the statement but also gives the P-smooth consecutive pairs for some P. Schur proved the following Lemma in order to prove Theorem 1 but accredits his method of proof to Størmer. As we will see, Størmer's method is to solve a number of Pell equations in order to find pairs of P-smooth numbers, Størmer's original work can be found in [14].

Lemma 2. [Schur, [13]] *For all numbers of the form $3^\alpha 5^\beta$ there only exist the following pairs $a < b$ with the difference $b - a \leq 20$;*

1, 3	1, 5	3, 5	5, 9	25, 27	1, 9	1, 15	3, 9
3, 15	5, 15	5, 25	9, 15	9, 25	9, 27	15, 25	15, 27
25, 45	27, 45	75, 81	125, 135	225, 243			

Proof of Lemma 2.
Suppose $b - a = 2$ or 4 and let D' be the largest non-square divisor of ab such that

$$ab = D'y^2$$

for some $y \in \mathbb{N}$.

For $b - a = 2$,

$$\begin{aligned} D'y^2 &= ab \\ &= a\,(a+2) \\ &= a^2 + 2a \end{aligned}$$

and since

$$(2a+2)^2 - 4\left(a^2 + 2a\right) = 4a^2 + 8a + 4 - 4a^2 - 8a = 4.$$

it is true that,

$$x^2 - 4D'y^2 = 4 \;\text{ where }\; x = 2a + 2.$$

Similarly, it can shown that for $b - a = 4$

$$x^2 - D'y^2 = 4 \;\text{ where }\; x = a + 2$$

Recall that a and b are of the form $3^\alpha 5^\beta$ so since $ab = D'y^2$, D' and y must also be of this form. In particular, as D' must be non-square, the only possible values of D' are 1, 3, 5 and 15.

Suppose $D' = 1$, then in the case $b - a = 4$ we will have $x^2 - y^2 = 4$, this implies $x + y = 4$ and $x - y = 1$ as this is the only product of unequal integers which gives 4. However, this would imply that $1 + 2y = 4$ which is clearly false. A similar argument can be used to show that D' cannot be 1 in the case $b - a = 2$. It follows that the only possible values of D' are 3, 5 and 15.

Letting $D = 4D'$ where $b - a = 2$ and $D = D'$ where $b - a = 4$ reduces the problem to finding solutions for the following Pell equations

$$x^2 - Dy^2 = 4 \;\text{ for }\; D = 3,\, 5,\, 15,\, 12,\, 20,\, 60. \tag{3}$$

For $D = 3$, the fundamental solution is $(4, 2)$ and therefore by Pell Property 5, all positive solutions of $x^2 - 3y^2 = 4$ are given by

$$x_n + y_n\sqrt{3} = 2(2 + \sqrt{3})^n$$

for some $n \in \mathbb{N}$. Note that this means that for all solutions of $x^2 - 3y^2 = 4$, y will be an even number and therefore not of the form $3^\alpha 5^\beta$ we are looking for. It is also true for $D = 15$, 20 that for all solutions of $x^2 - Dy^2 = 4$, y must be even and therefore not of the form we are looking for. So we must only consider the cases $D = 5$, 12, 60.

In the cases $b - a = 2$ or 4, one number must be of the form 3^α and the other of the form 5^β since otherwise $\gcd(a, b) > 1$ and $b - a$ must be divisible by at least 3 or 5.

For $D = 5$, the fundamental solution is $(3, 1)$ and therefore by Pell Property 5, all positive solutions of $x^2 - 5y^2 = 4$ are given by

$$\frac{x_n + y_n\sqrt{5}}{2} = \left(\frac{3 + \sqrt{5}}{2}\right)^n$$

and therefore,

$$y_1 = 1,\ y_2 = 3,\ y_3 = 8,\ y_4 = 21,\ y_5 = 55, \ldots$$

Since y_5 is the smallest y that is divisible by 5 we know by Pell Property 6 that only y_{5q} are divisible by 5 but these are also divisible by 11 and therefore not of the form $3^\alpha 5^\beta$, so it is not possible to find a solution (x, y) such that y is divisible by 5, therefore

$$y = 3^\alpha.$$

It follows that

$$ab = D'y^2 = 3^{2\alpha}5$$

and a, b must be of one of the following forms

$$a = 3^{2\alpha},\ b = 5 \text{ or } a = 5,\ b = 3^{2\alpha}.$$

The only a, b pairs where $b - a = 4$ are therefore 1, 5 and 5, 9.

For $D = 12$ ($D' = 3$), the fundamental solution is $(4, 1)$ and therefore by Pell Property 5, all positive solutions of $x^2 - 12y^2 = 4$ are given by

$$\frac{x_n + y_n\sqrt{12}}{2} = \left(\frac{4 + \sqrt{12}}{2}\right)^n$$

and therefore

$$y_1 = 1,\ y_2 = 4,\ y_3 = 15,\ y_4 = 56,\ y_5 = 209,$$
$$y_6 = 780,\ y_7 = 2911,\ y_8 = 10864,\ y_9 = 40545 \ldots$$

Since y_9 is the smallest y that is divisible by 9 we know by Pell Property 6 that only y_{9q} are divisible by 9 but these are also divisible by 17 and therefore not of the form $3^\alpha 5^\beta$, so it is not possible to find a solution (x, y) such that y is divisible by 9, therefore

$$y = 3 \cdot 5^\beta \text{ or } y = 5^\beta.$$

It follows that

$$ab = D'y^2 = 3^3 \cdot 5^{2\beta} \text{ or } 3 \cdot 5^{2\beta}$$

and a, b must be of one of the following forms

$$a = 3,\ b = 5^{2\beta} \text{ or } a = 27,\ b = 5^{2\beta}$$
$$\text{or } a = 5^{2\beta},\ b = 3 \text{ or } a = 5^{2\beta},\ b = 27.$$

The only pairs where $b - a = 2$ are therefore 1, 3 and 25, 27.

Finally, for $D = 60$ ($D' = 15$), the fundamental solution is $(8, 1)$ and therefore by Pell Property 5, all positive solutions of $x^2 - 60y^2 = 4$ are given by

$$\frac{x_n + y_n\sqrt{60}}{2} = \left(\frac{8 + \sqrt{60}}{2}\right)^n \tag{4}$$

and therefore

$$y_1 = 1,\ y_2 = 8,\ y_3 = 63\ldots$$

Since y_3 is the smallest y that is divisible by 3 we know by Pell Property 6 that only y_{3q} are divisible by 3 but these are also divisible by 7 and therefore not of the form $3^\alpha 5^\beta$, so it is not possible to find a solution (x, y) such that y is divisible by 3, therefore

$$y = 5^\beta.$$

It follows that

$$ab = D'y^2 = 3 \cdot 5^{2\beta+1}$$

and a, b must be of one of the following forms

$$a = 3,\ b = 5^{2\beta+1} \text{ or } a = 5^{2\beta+1},\ b = 3.$$

The only pair where $b - a = 2$ is therefore 3, 5.

Since $b - a$ must be even, we have now shown that for $b - a \leq 4$ there are only 5 possible pairs:

$$1,\ 3 \quad 1,\ 5 \quad 3,\ 5 \quad 5,\ 9 \quad 25,\ 27 \tag{5}$$

It is left to find the pairs for which $4 < b - a \leq 20$. We first consider only a, b such that $\gcd(a, b) = 1$. i.e. $a = 3^\alpha$, $b = 5^\beta$ or $a = 5^\beta$, $b = 3^\alpha$ or $a = 1$, $b = 3^\alpha 5^\beta$. So $b - a$ cannot be a multiple of 3 or 5. i.e. $b - a = 8,\ 14,\ 16$.

Suppose that $a = 1$, $b = 3^\alpha 5^\beta$, then clearly 1, 9 and 1, 15 are the only pairs such that $4 < b - a \leq 20$.

Let's investigate the case that $a = 3^\alpha$, $b = 5^\beta$ or $a = 5^\beta$, $b = 3^\alpha$.

First note that

$$\begin{aligned} 3^\alpha &\equiv \pm 1 \mod 5 && \text{if } \alpha \text{ is even} \\ 3^\alpha &\equiv +1 \mod 4 && \text{if } \alpha \text{ is even} \\ 5^\beta &\equiv +1 \mod 4 && \text{for all } \beta. \end{aligned}$$

If $b - a = 14$ then

$$\begin{aligned} 3^\alpha - 5^\beta &= \pm(b-a) \\ &= \pm 14 \\ &\equiv \mp 1 \mod 5 \end{aligned}$$

i.e. $3^\alpha \equiv \pm 1 \mod 5$, so α must be even.
But if α is even then,

$$\begin{aligned} 14 &= \pm(b-a) \\ &= 3^\alpha - 5^\beta \\ &\equiv 0 \mod 4. \end{aligned}$$

i.e. $14 \equiv 0 \mod 4$, which is clearly not true, so $b - a \neq 14$. This means $b - a = 8$ or 16. In both these cases it must be true that $3^\alpha \equiv 5^\beta \mod 8$.
Note that

$$\begin{aligned} 3^\alpha &\equiv 1 \mod 8 && \text{if } \alpha \text{ is even} \\ 3^\alpha &\equiv 3 \mod 8 && \text{if } \alpha \text{ is odd} \\ 5^\beta &\equiv 1 \mod 8 && \text{if } \beta \text{ is even} \\ 5^\beta &\equiv 5 \mod 8 && \text{if } \beta \text{ is odd} \end{aligned}$$

So α and β must both be even. i.e. a and b are square numbers.
Note that for $n \in \mathbb{N}$

$$\begin{aligned} (n+1)^2 - n^2 &= 2n + 1 \geq 3 \\ (n+2)^2 - n^2 &= 4n + 4 \geq 8 \\ (n+3)^2 - n^2 &= 6n + 9 \geq 15 \\ (n+4)^2 - n^2 &= 8n + 16 \geq 24. \end{aligned}$$

Since $b - a = 8$ or 16 can only be true when $a = n^2$ and $b = (n+1)^2$, $(n+2)^2$ or $(n+3)^2$, we look for values of n that satisfy

$$2n + 1 = 8 \text{ or } 16 \tag{6}$$
$$4n + 4 = 8 \text{ or } 16 \tag{7}$$
$$6n + 9 = 16. \tag{8}$$

Clearly, no values of n satisfy (6) or (8), but from (7) we find two possibilities ($n = 1$ or 3).

The only pairs of the form $3^\alpha 5^\beta$ such that $\gcd(a, b) = 1$ and $4 < b - a \leq 20$ are 1, 9, 1, 15 and 9, 25. Adding these pairs to our list in (5) gives us all pairs of the form $3^\alpha 5^\beta$ such that $\gcd(a, b) = 1$ and $b - a \leq 20$.

$$1, 3 \quad 1, 5 \quad 1, 9 \quad 1, 15 \quad 3, 5 \quad 5, 9 \quad 9, 25 \quad 25, 27 \tag{9}$$

Clearly, it is always possible to write $b-a = (\gcd(a, b))\cdot(b^*-a^*)$ where $\gcd(a^*, b^*) = 1$, so multiplication of the pairs we have found so far by powers of 3 and 5 such that $b - a \leq 20$ still holds will give all possible pairs. □

5 Introduction to Algebraic Number Theory

5.1 Algebraic Number Fields and Rings of Integers

Definition 8 (Algebraic Number)**.** *An algebraic number α is any number (real or complex) that is a root of some monic rational polynomial that is irreducible over $\mathbb{Q}$. We call this polynomial the minimal polynomial of α.*

Definition 9 (Algebraic Integer)**.** *An algebraic integer is any number (real or complex) that is a root of some monic integer polynomial that is irreducible over $\mathbb{Q}$. We call this polynomial the minimal polynomial of α.*

Example 4. Every integer a is an algebraic integer with minimal polynomial $x - a$.

Example 5. We have already seen algebraic integers in Section 3. In the proof of Lemma 2, we found that the fundamental solution of $x^2 - 5y^2 = 4$ is $3 + \sqrt{5}$. This is an algebraic integer with minimal polynomial $x^2 - 6x + 4$.

Remark 3. *Clearly, the set of algebraic integers is a subset of the set of algebraic numbers.*

Definition 10 (Algebraic Number Field)**.** *Any field $\mathbb{K}$ formed by adjoining algebraic numbers to $\mathbb{Q}$ is an algebraic number field. The degree of this field extension is finite.*

Definition 11 (Simple Algebraic Number Field)**.** *Any field $\mathbb{K}$ formed by adjoining a single algebraic number α to $\mathbb{Q}$ is a simple algebraic number field. The degree of this field extension is the degree of the minimal polynomial of α.*

Definition 12 (Ring of Integers)**.** *The set of algebraic integers in a given algebraic number field $\mathbb{K}$ form a commutative ring with a multiplicative identity, which we call the ring of integers and denote $\mathcal{O}_{\mathbb{K}}$.*

Example 6. *The ring of integers $\mathcal{O}_{\mathbb{Q}}$ in the algebraic number field $\mathbb{Q}$ is $\mathbb{Z}$.*

Example 7. *The ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ in the algebraic number field $\mathbb{Q}(\sqrt{5})$ is $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, in particular, all solutions of the Pell Equation $x^2 - 5y^2 = 4$ are contained in the ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$.*

Definition 13 (Units)**.** *An element u of a ring of integers $\mathcal{O}_{\mathbb{K}}$ is called a unit if there exists a multiplicative inverse u^{-1} of u in $\mathcal{O}_{\mathbb{K}}$. In particular, the units of a particular ring of integers $\mathcal{O}_{\mathbb{K}}$ form an abelian group under multiplication.*

Example 8. *The elements of the unit group of $\mathbb{Z}$ are $\{1, -1\}$.*

Example 9. *The elements of the unit group of $\mathcal{O}_{\mathbb{Q}(\sqrt{3})} = \mathbb{Z}\left[\sqrt{3}\right]$ are the solutions $\frac{x+\sqrt{3}y}{2}$ of the Pell equation $x^2 - 3y^2 = 4$.*

Definition 14 (Irreducible Elements)**.** *An element p of a ring of integers $\mathcal{O}_{\mathbb{K}}$ is called an irreducible element if its only factorisation in $\mathcal{O}_{\mathbb{K}}$ is the trivial factorisation $p = u \cdot u^{-1} \cdot p$, where u is some unit in $\mathcal{O}_{\mathbb{K}}$.*

Example 10. *The irreducible elements of $\mathbb{Z}$ are the prime numbers $\mathbb{P}$.*

The Fundamental Theorem of Arithmetic states that every positive integer has a unique prime factorisation. It follows therefore, that every element of $\mathbb{Z}$ can be expressed as a unique product of prime numbers multiplied by 1 or -1. However, it does not follow for all rings of integers, that every element can be expressed as a unique product of irreducible elements multiplied by some unit. In order to define some unique prime factorisation in rings of integers, we need to introduce the concept of an ideal.

5.2 Introduction to Ideal Theory

Definition 15 (Ideal)**.** *Let R be a commutative ring with a multiplicative identity and suppose I is a subring (not necessarily containing the multiplicative identity) of R. Then I is an ideal if and only if*

$$\begin{aligned} x + y \in I \ \ \forall x, y \in I \\ rx \in I \ \ \forall x \in I, r \in R. \end{aligned}$$

Definition 16 (Principal Ideal)**.** *A principal ideal is an ideal that is generated by just one element of R. We denote the principal ideal generated by α as $\langle \alpha \rangle$.*

$$\langle \alpha \rangle = \{ r\alpha : r \in R \}$$

Example 11. *A principal ideal in $\mathbb{Z}$ is the set of all multiples of a particular integer. For example, $\langle 5 \rangle$ is the set of all multiples of 5. It is easy to verify that $\langle 5 \rangle$ is an ideal by observing that the sum of two multiples of 5 is also a multiple of 5 and the product of a multiple of 5 with any other integer is still a multiple of 5.*

Definition 17 (Prime Ideal)**.** *A prime ideal P is an ideal such that for all x, $y \in R$,*

$$x \cdot y \in P \implies x \in P \text{ or } y \in P.$$

Example 12. *The prime ideals of $\mathbb{Z}$ are exactly the principal ideals generated by prime numbers. For example, if we factorise an element of $\langle 3 \rangle$, then at least one of its factors must be a multiple of 3.*

Definition 18 (Product of Ideals)**.** *If I and J are two ideals of R, then $I \cdot J$ is the ideal generated by all $i \cdot j$, where $i \in I$ and $j \in J$.*

Example 13. *Clearly, $\langle 5 \rangle \cdot \langle 3 \rangle = \langle 15 \rangle$ because every $i \in \langle 3 \rangle$ is of the form $i = 3m$ and every $j \in \langle 5 \rangle$ is of the form $j = 5n$, so every linear combination of $i \cdot j = 3m \cdot 5n$ will be of the form $15l$ and therefore exactly the ideal generated by 15.*

Definition 19 (Ideal Division)**.** *Let I and J be two ideals of R. We say that J divides I if and only if there exists an ideal K of R such that $I = J \cdot K$.*

Remark 4. *We say "I divides α" when "I divides $\langle\alpha\rangle$" is to be understood.*

5.3 Properties of Ideals

Ideal Property 1.
For any two ideals I and J of a commutative ring R,

$$J \text{ divides } I \iff J \text{ contains } I \quad (I \subset J)$$

As a result, the words "divides" and "contains" are used interchangeably.

Ideal Property 2.
For any two principal ideals $\langle\alpha\rangle$ and $\langle\beta\rangle$ of a commutative ring R,

$$\alpha \text{ divides } \beta \iff \langle\alpha\rangle \text{ divides } \langle\beta\rangle$$

Ideal Property 3 (Fundamental Theorem of Ideal Theory in Number Fields)**.**
For every non-zero proper ideal I of some ring of integers $\mathcal{O}_{\mathbb{K}}$, there exists a unique factorisation of I into prime ideals P_i of $\mathcal{O}_{\mathbb{K}}$. (I is non-zero iff $I \neq \langle 0\rangle$ and proper iff $I \neq \mathcal{O}_{\mathbb{K}}$.)

Schur not only makes use of the above properties of ideals, but also the following Lemma.

Lemma 3 (Perron, [10])**.** *A prime number in an algebraic number field of degree n, can have at most n factors.*

6 Some Basic Results

We are almost ready to start understanding Schur's proofs of Theorems 1,2 and 3. Schur makes regular use of various properties related to the Gauss bracket and double factorials throughout his work. I have provided a more detailed explanation of these statements in this section.

6.1 The Gauss Bracket

The Gauss bracket $[\cdot] : \mathbb{R} \to \mathbb{Z}$ is a function mapping real numbers x to the greatest integer $z \leq x$. In Schur's proof of Theorem 1, he makes use of the following properties of the Gauss Bracket:

Gauss Bracket Property 1.
$[x] + \left[x + \frac{1}{2}\right] = [2x] \qquad \forall x \in \mathbb{R},$

Gauss Bracket Property 2.
$\left[x + y + \frac{1}{2}\right] - \left[x + \frac{1}{2}\right] - \left[y + \frac{1}{2}\right] = -1, 0 \;\; or \;\; 1 \;\; \forall x, y \in \mathbb{R}.$

Gauss Bracket Property 3.
In the sequence of x consecutive odd numbers $1, 3, 5, \ldots, 2x-1$, there are exactly

$$\left[\frac{2x}{y}\right] - \left[\frac{x}{y}\right].$$

multiples of an odd number y.

Gauss Bracket Property 4.
In any sequence of x consecutive odd numbers, there are at most

$$\left[\frac{x+y-1}{y}\right].$$

multiples of an odd number y.

Proof of Gauss Bracket Property 1.
Let $x = a + b$ where

$$a = \max\{z \in \mathbb{Z} : z \leq x\}, \quad b \in \mathbb{R}.$$

Then clearly, $[x] = a$ and $0 \leq b < 1$ so that,

$$\left[x + \tfrac{1}{2}\right] = \begin{cases} a & 0 \leq b < \frac{1}{2} \\ a+1 & \frac{1}{2} \leq b < 1. \end{cases}$$

Similarly,

$$2x = 2a + 2b \text{ and } 0 \leq b < 1,$$

so that,

$$[2x] = \begin{cases} 2a & 0 \le b < \frac{1}{2} \\ 2a+1 & \frac{1}{2} \le b < 1. \end{cases}$$

From this, Gauss Bracket Property 1 follows easily. □

Proof of Gauss Bracket Property 2. Let $x = a + b$ and $y = c + d$ where

$$\begin{aligned} a &= \max\{z \in \mathbb{Z} : z \le x\}, \quad b \in \mathbb{R}, \\ c &= \max\{z \in \mathbb{Z} : z \le y\}, \quad d \in \mathbb{R}. \end{aligned}$$

Then,

$$\left[x + \tfrac{1}{2}\right] = \begin{cases} a & 0 \le b < \frac{1}{2} \\ a+1 & \frac{1}{2} \le b < 1, \end{cases}$$

$$\left[y + \tfrac{1}{2}\right] = \begin{cases} c & 0 \le d < \frac{1}{2} \\ c+1 & \frac{1}{2} \le d < 1, \end{cases}$$

$$\left[x + y + \tfrac{1}{2}\right] = \begin{cases} a+c & 0 \le b+d < \frac{1}{2} \\ a+c+1 & \frac{1}{2} \le b+d < 1 \\ a+c+1 & 1 \le b+d < \frac{3}{2} \\ a+c+2 & \frac{3}{2} \le b+d < 2. \end{cases} \tag{10}$$

If we look at each of the cases in (10) then we see that

$$0 \le b+d < \tfrac{1}{2} \implies 0 \le b, d < \tfrac{1}{2},$$

$$\begin{aligned} \tfrac{1}{2} \le b+d < 1 \implies & 0 \le b, d < \tfrac{1}{2} \\ & \text{or } \ 0 \le b < \tfrac{1}{2} \ \text{ and } \ \tfrac{1}{2} \le d < 1 \\ & \text{or } \ 0 \le d < \tfrac{1}{2} \ \text{ and } \ \tfrac{1}{2} \le b < 1, \end{aligned}$$

$$\begin{aligned} 1 \le b+d < \tfrac{3}{2} \implies & 0 \le b < \tfrac{1}{2} \ \text{ and } \ \tfrac{1}{2} \le d < 1 \\ & \text{or } \ 0 \le d < \tfrac{1}{2} \ \text{ and } \ \tfrac{1}{2} \le b < 1 \\ & \text{or } \ \tfrac{1}{2} \le b, d < 1, \end{aligned}$$

$$\tfrac{3}{2} \le b+d < 2 \implies \tfrac{1}{2} \le b, d < 1.$$

This gives,

$$\left[x + \tfrac{1}{2}\right] + \left[y + \tfrac{1}{2}\right] = \begin{cases} a+c & 0 \le b+d < \frac{1}{2} \\ a+c \ \text{ or } \ a+c+1 & \frac{1}{2} \le b+d < 1 \\ a+c+1 \ \text{ or } \ a+c+2 & 1 \le b+d < \frac{3}{2} \\ a+c+2 & \frac{3}{2} \le b+d < 2. \end{cases} \tag{11}$$

Subtracting (11) from (10) in each case, we get

$$\left[x+y+\tfrac{1}{2}\right]-\left[x+\tfrac{1}{2}\right]-\left[y+\tfrac{1}{2}\right]=\begin{cases}0 & 0\le b+d<\frac{1}{2}\\ 1 \text{ or } 0 & \frac{1}{2}\le b+d<1\\ 0 \text{ or } -1 & 1\le b+d<\frac{3}{2}\\ 0 & \frac{3}{2}\le b+d<2\end{cases}$$

and Gauss Bracket Property 2 follows. □

The following trivial statements will be made use of in order to prove Gauss Bracket Properties 3 and 4:

Statement 1.
Given a sequence of x terms

$$a_1, a_2, \ldots a_x,$$

and dividing the sequence into disjoint subsequences of y terms as follows

$$a_1, \ldots, a_y, \quad a_{y+1}, \ldots, a_{2y}, \quad \ldots \tag{12}$$

will result in

$$\left[\frac{x}{y}\right] \text{ disjoint subsequences of } y \text{ terms}$$
$$\text{and } 1 \text{ remaining subsequence of } r \text{ terms,}$$

where $0 \le r < y$.

Statement 2. *Every sequence of y consecutive numbers contains exactly one multiple of y.*

Statement 3. *Every sequence of y consecutive odd numbers contains exactly one multiple of y, where y is odd.*

The Gauss Bracket Properties below follow from the above trivial statements:

Gauss Bracket Property 3a.
The number of multiples of y in the sequence $1, 2, 3, \ldots, x$ is $\left[\frac{x}{y}\right]$ $\forall x, y \in \mathbb{N}$.

Proof of Gauss Bracket Property 3a.
Dividing the sequence as in (12) gives disjoint subsequences of y numbers, ending in a multiple of y. It follows from Statement 2 that the remaining sequence cannot contain a multiple of y. The number of multiples of y in the whole sequence coincides with the number of disjoint subsequences of y which can be found using Statement 1. □

Gauss Bracket Property 4a.
Given a sequence of x consecutive odd integers and an odd y, exactly

$$\left[\frac{x}{y}\right] \text{ multiples of } y$$

will appear in the sequence if and only if, after dividing the sequence into disjoint subsequences of y consecutive odd integers as in (12), the remaining sequence does not contain a multiple of y.

Proof of Gauss Bracket Property 4a.
If the remaining sequence does not contain a multiple of y, then it follows from Statement 3 that the number of multiples of y coincides with the number of disjoint subsequences of y, which can be found using Statement 1. □

Gauss Bracket Property 4b.
Given a sequence of x consecutive odd integers and an odd y, exactly

$$\left[\frac{x+y-r}{y}\right] \text{ multiples of } y$$

will appear in the sequence if and only if, after dividing the sequence into disjoint subsequences of y consecutive odd integers as in (12), the remaining sequence of r consecutive odd numbers contains a multiple of y.

Proof of Gauss Bracket Property 4b.
If the remaining sequence of r numbers contains a multiple of y, then the sequence (starting with the same number) of $x+y-r$ consecutive odd numbers has a remaining sequence of 0 numbers and therefore a remaining sequence which does not contain a multiple of y. Clearly, the number of multiples of y in our original sequence coincides with the number of multiples of y in our new sequence of $x+y-r$ consecutive odd numbers, which can be found using Gauss Bracket Property 4a. □

We are now ready to prove Gauss Bracket Properties 3 and 4.

Proof of Gauss Bracket Property 3.
In order to find the number of multiples of an odd number y in the sequence

$$1, 3, 5, \ldots, 2x-1$$

we can find the number of multiples of y in the sequence

$$1, 2, 3, \ldots, 2x \tag{13}$$

and then subtract the number of multiples of $2y$ in (13). We know from Gauss Bracket Property 3a that,

$$\left[\frac{2x}{y}\right] = \text{ number of multiples of } y \text{ that appear in (13)},$$

$$\left[\frac{2x}{2y}\right] = \text{ number of multiples of } 2y \text{ that appear in (13)}.$$

From this, Gauss Bracket Property 3 follows easily. □

Proof of Gauss Bracket Property 4.
Follows easily from Gauss Bracket Properties 4a and 4b. □

6.2 Double Factorials

While a factorial is a product of consecutive integers, a double factorial is a product of consecutive even or odd integers. Schur uses double factorials in his work, denoting the product of odd integers up to $2n$ as u_{2n}. In this section, we will explore u_{2n}. Firstly, we will express u_{2n} in terms of factorials and use Stirlings's formula to find an expression for $\log u_{2n}$. Then, we will use Gauss Bracket Properties 1 and 3 in order to find powers of prime factors of u_{2n} and in turn an expression for the prime factorisation of u_{2n}.

6.2.1 Stirling's Formula

Stirling's formula is an approximation for the logarithm of a factorial given by

$$\log n! = (n + \tfrac{1}{2}) \log n - n + \log \sqrt{2\pi} + R_n \ \ (0 < R_n < \tfrac{1}{12})$$

For more information on Stirling's formula, I refer the reader to [2].

Let

$$u_{2n} = \frac{(2n)!}{2^n n!}. \tag{14}$$

Note that this is equivalent to our original definition

$$u_{2n} = (2n-1)!!$$

as

$$\begin{aligned}\frac{(2n)!}{2^n n!} &= \frac{1\cdot 2\cdot 3\cdots(2n-1)\cdot 2n}{2^n\cdot 1\cdot 2\cdot 3\cdots(n-1)\cdot n}\\ &= \frac{1\cdot 2\cdot 3\cdots(2n-1)\cdot 2n}{(2\cdot 1)\cdot(2\cdot 2)\cdot(2\cdot 3)\cdots(2\cdot(n-1))\cdot(2\cdot n)}\\ &= \frac{1\cdot 2\cdot 3\cdots(2n-1)\cdot 2n}{2\cdot 4\cdot 6\cdots(2n-2)\cdot 2n}\\ &= 1\cdot 3\cdot 5\cdots(2n-1)\\ &= (2n-1)!!\end{aligned}$$

Using Stirling's formula and (14), we are able to find an expression for $\log u_{2n}$

$$\begin{aligned}\log u_{2n} &= \log\left(\frac{(2n)!}{2^n n!}\right)\\ &= \log(2n)! - \log 2^n - \log n!\\ &= \left(2n+\tfrac{1}{2}\right)\log 2n - 2n + \log\sqrt{2\pi} + R_{2n}\\ &\qquad - n\log 2 - \left(n+\tfrac{1}{2}\right)\log n + n - \log\sqrt{2\pi} - R_n\\ &= n\log n + n\log 2 + \tfrac{1}{2}\log 2 - n + S_n,\end{aligned}$$

where $S_n = R_{2n} - R_n$ and therefore $-\frac{1}{12} < S_n < \frac{1}{12}$.

6.2.2 Finding Powers of Prime Factors of u_{2n}

We can find the highest power $\lambda_n(p)$ of $p \in \mathbb{P}$ such that $p^{\lambda_n(q)}$ divides u_{2n} by counting how many multiples of p appear in the sequence $1, 3, \ldots, 2n-1$. We then count multiples of powers of p since these will account for division by p several times. A multiple of p^n is also a multiple of p^{n-1} so if we count multiples of p, p^2,...,p^n we will indeed count multiples of p^n n times.
Using Gauss Bracket Property 3, we can represent $\lambda_n(p)$ as

$$\lambda_n(p) = \sum_{\mu=1}^{m}\left\{\left[\frac{2n}{p^\mu}\right] - \left[\frac{n}{p^\mu}\right]\right\}, \tag{15}$$

where m is the highest power of p, for which $p^m < 2n$.
Using Gauss Bracket Property 1 we can rewrite (15) as

$$\lambda_n(p) = \sum_{\mu=1}^{m}\left[\frac{2n+p^\mu}{2p^\mu}\right]. \tag{16}$$

6.2.3 The Prime Factorisation of u_{2n}

It follows from the previous section that we are able to write the prime factorisation of u_{2n} as

$$u_{2n} = \prod_{\substack{p\in\mathbb{P}\\ 3\leq p\leq 2n}} p^{\lambda_n(p)}. \tag{17}$$

Note that we don't consider $p = 2$ as u_{2n} is always odd.
Let us now look at an example:

Example 14. Let $n = 8$. Then

$$u_{16} = \prod_{\substack{p\in\mathbb{P}\\ 3\leq p\leq 16}} p^{\lambda_8(p)}. \tag{18}$$

First note, that we must only consider $p = 3$, 5, 7, 11, 13 as these are the only prime numbers in the interval $3 \leq p \leq 16$. Using (16) we are able to find $\lambda_8(p)$ for each p. Starting with $p = 3$ we find

$$\lambda_8(3) = \sum_{\mu=1}^{m} \left[\frac{16 + 3^\mu}{2 \cdot 3^\mu}\right].$$

Since,

$$3^2 < 16 < 3^3,$$

it follows that $m = 2$ and therefore,

$$\lambda_8(3) = \left[\frac{19}{6}\right] + \left[\frac{25}{18}\right] = 4.$$

Similarly,

$$\begin{aligned}\lambda_8(5) &= 2\\ \lambda_8(7) &= 1\\ \lambda_8(11) &= 1\\ \lambda_8(13) &= 1.\end{aligned}$$

Using our values of $\lambda_8(p)$ and our expression for the prime factorisation of u_{16} given in (18), we have

$$u_{16} = 3^4 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13.$$

In Schur's work, he proves the following Lemma and uses it in the proof of Theorem 3.

Lemma 4 (Schur, [13])**.**
If $p^{\lambda_n(p)}$ is the highest power of an odd prime p which divides u_{2n}, then for $n \geq 1$

$$\lambda_n(p) < \frac{2n}{p}$$

Proof of Lemma 4.
If $p > 2n$, then p clearly does not divide u_{2n} and $\lambda_n(p) = 0$.
If $p < 2n$, then we can use (16).

Let m be the highest power of p such that $p^m < 2n$.

If $m = 1$, then because $p < 2n$ (and therefore $\frac{1}{2} < \frac{n}{p}$), it follows from (16) that

$$\begin{aligned}\lambda_n(p) &= \left[\frac{2n+p}{2p}\right] \\ &\leq \frac{2n+p}{2p} \\ &= \frac{n}{p} + \frac{1}{2} \\ &< \frac{2n}{p},\end{aligned}$$

If $m = 2$, then since $p \geq 3$, it follows from (16) that

$$\begin{aligned}\lambda_n(p) &\leq \frac{2n+p}{2p} + \frac{2n+p^2}{2p^2} \\ &= \frac{n}{p} + \frac{n}{p^2} + 1 \\ &\leq \frac{n}{p} + \frac{n}{3p} + 1.\end{aligned}$$

Since $p^2 < 2n$, it follows that

$$\begin{aligned}\frac{2n}{p} - \frac{n}{p} - \frac{n}{3p} - 1 &= \frac{2n}{3p} - 1 \\ &\geq \frac{2n}{p^2} - 1 \\ &> 0.\end{aligned}$$

Therefore,

$$\lambda_n(p) \leq \frac{n}{p} + \frac{n}{3p} + 1 < \frac{2n}{p}.$$

If $m \geq 3$. Then, from (16),

$$\begin{aligned}\lambda_n(p) &\leq \frac{m}{2} + \frac{n}{p} + \frac{n}{p^2} + \cdots + \frac{n}{p^m} \\ &< \frac{m}{2} + \frac{n}{p} + \frac{n}{p}\left(\frac{1}{3} + \frac{1}{3^2} + \cdots\right) \\ &< \frac{m}{2} + \frac{n}{p} + \frac{n}{2p}.\end{aligned}$$

From this, we know that $\lambda_n(p) < \frac{2n}{p}$ if $mp < n$. We know that $2n > p^m$, so it is left to show that $p^m > 2mp$ or equivalently $p^{m-1} > 2m$ for $m \geq 3$. From,

$$\begin{aligned}p^{m-1} &\geq 3^{m-1} \\ &= (1+2)^{m-1} \\ &= \sum_{k=0}^{m-1} \binom{m-1}{k} 1^{m-1-k} \cdot 2^k \\ &> \sum_{k=0}^{2} \binom{m-1}{k} 1^{m-1-k} \cdot 2^k \\ &= \binom{m-1}{0} 1^{m-1} \cdot 2^0 + \binom{m-1}{1} 1^{m-2} \cdot 2^1 + \binom{m-1}{2} 1^{m-3} \cdot 2^2 \\ &\geq 1 + 2(m-1) + 4\binom{m-1}{2} \\ &> 2m,\end{aligned}$$

we see that this inequality holds for $m \geq 3$ and therefore, $\lambda_n < \frac{2n}{p}$ is true for $m \geq 3$. This was the final case, so we have now proven the Lemma. □

7 A Theorem on Prime Numbers

7.1 Proof of Theorem 1

Theorem 1. *For $k \in \mathbb{N}$ $(k > 2)$ such that $p = 2k + 1 \in \mathbb{P}$ $(p > 5)$, it is true that any sequence of k consecutive odd numbers, for which all terms are greater than $2k + 1$, will contain at least one term with a prime factor greater than $2k + 1$.*

$$2h + 1, \quad 2h + 3, \quad \ldots, \quad 2h + 2k - 1 \quad (h > k)$$

For $p = 3$, the only counterexamples are powers of $3^\alpha > 3$ and for $p = 5$, the only counterexample is 25, 27.

Let us consider the case $k = 5$.
According to the theorem, every sequence

$$2h + 1, \quad 2h + 3, \quad 2h + 5, \quad 2h + 7, \quad 2h + 9 \quad (h > 5)$$

of 5 consecutive odd numbers, for which all terms are greater than 11, will contain at least one term with a prime factor greater than 11. Let us take, for example, the sequence

$$21, 23, 25, 27, 29 \quad (h = 10)$$

In this sequence, we have two prime numbers (23 and 29), so their prime factors are indeed greater than 11. Note that it is not necessary for any of the terms to be prime, we are only interested in the prime factors of the terms. Another sequence for $k = 5$ would be

$$115, 117, 119, 121, 123 \quad (h = 57)$$

None of these terms are prime numbers but all of them except 121 are divisible by some prime number greater than 11.

According to the theorem, which sequences don't necessarily have this property?

1. If $p \leq 5$ $(k \leq 2)$.
   For $p = 5$ $(k = 2)$, there exists a counterexample: 25, 27 so it is not possible to delete this condition.

2. If any of the terms are less than or equal to $p = 2k + 1$. i.e. $h < k$.
   For $p = 7$ $(k = 3)$, there would exist a counterexample: 5, 7, 9 so it is not possible to delete this condition.

3. If $2k + 1$ is not prime. The theorem actually holds for all $2k + 1 \in \mathbb{N}$, this is a nice Corollary of Theorem 1 which we will prove later.

Proof of Theorem 1.
Suppose there exists a counterexample $\mathfrak{C}_{h,p}$.
i.e. Suppose there exists a sequence of k consecutive odd numbers

$$2h+1, \quad 2h+3, \quad \ldots, \quad 2h+2k-1 \quad (h>k) \tag{19}$$

such that all terms have prime factors less than or equal to $p = 2k+1 \in \mathbb{P}$.

Then, for any counterexample $\mathfrak{C}_{h,p}$, let

$$C = \frac{(2h+1)\cdot(2h+3)\cdot\cdots\cdot(2h+2k-1)}{1\cdot 3\cdot 5\cdot\cdots\cdot(2k-1)} \tag{20}$$

$$= \frac{u_{2k+2h}}{u_{2k}\cdot u_{2h}}. \tag{21}$$

Part 1
We will now use the theory developed in Section 6.2 to tell us more about C in the case that $\mathfrak{C}_{h,p}$ is a counterexample.

It follows from Section 6.2.3, that

$$u_{2h+2k} = \prod_{\substack{q\in\mathbb{P}\\ 3\le q\le 2h+2k}} q^{\lambda_{h+k}(q)} \tag{22}$$

$$u_{2h} = \prod_{\substack{q\in\mathbb{P}\\ 3\le q\le 2h}} q^{\lambda_{h}(q)} \tag{23}$$

$$u_{2k} = \prod_{\substack{q\in\mathbb{P}\\ 3\le q\le 2k}} q^{\lambda_{k}(q)} \tag{24}$$

Let us consider

$$\frac{u_{2k+2h}}{u_{2h}} = (2h+1)\cdot(2h+3)\cdot\ldots\cdot(2h+2k-1)\,.$$

Since

$$2h+1, \quad 2h+3, \quad \ldots, \quad 2h+2k-1 \quad (h>k)$$

is a counterexample, the prime factorisation of each of these numbers cannot contain prime divisors greater than $p = 2k+1$, so we need only consider $3 \le q \le p$.
So, for any counterexample $\mathfrak{C}_{h,p}$, it is true that

$$C = \prod_{\substack{q\in\mathbb{P}\\ 3\le q\le p}} q^{v_q} \tag{25}$$

where $v_q = \lambda_{h+k}(q) - \lambda_h(q) - \lambda_k(q)$, which we know from Section 6.2.2 to be,

$$v_q = \sum_{\mu=1}^{m} \left\{ \left[\frac{2h + 2k + q^\mu}{2q^\mu} \right] - \left[\frac{2k + q^\mu}{2q^\mu} \right] - \left[\frac{2h + q^\mu}{2q^\mu} \right] \right\} \tag{26}$$

and m is the highest power of q such that $q^m < 2h + 2k$. Note that we have not assumed that v_q is positive and so (25) does not represent a prime factorisation of C and C is not necessarily a natural number.

Part 2

We now use C to find an inequality that must be satisfied if there exists a counterexample $\mathfrak{C}_{h,p}$.

Let us now investigate C, by first determining possible values of v_q. From Gauss Bracket Property 2, it follows that every term of v_q in (26) is equal to -1, 0 or 1 so,

$$v_q \leq m < \frac{\log(2h + 2k)}{\log q}. \tag{27}$$

We know from (25) that

$$\begin{aligned} \log C &= \sum_{\substack{q \in \mathbb{P} \\ 3 \leq q \leq p}} \log(q^{v_q}) \\ &= \sum_{\substack{q \in \mathbb{P} \\ 3 \leq q \leq p}} v_q \log q. \end{aligned} \tag{28}$$

From (27), we therefore know that

$$\begin{aligned} \log C &< \sum_{\substack{q \in \mathbb{P} \\ 3 \leq q \leq p}} \frac{\log(2h + 2k)}{\log q} \log q \\ &= \sum_{\substack{q \in \mathbb{P} \\ 3 \leq q \leq p}} \log(2h + 2k) \\ &= (\pi(p) - 1) \log(2h + 2k). \end{aligned} \tag{29}$$

where $\pi(p)$ is defined, as in Section 2 to be the amount of prime numbers in the interval $2 \leq q \leq p$.

In Section 6.2.1, we used Stirling's formula to find the following expression for $\log u_{2n}$

$$\log u_{2n} = n \log n + n \log 2 + \tfrac{1}{2} \log 2 - n + S_n \quad (-\tfrac{1}{12} < S_n < \tfrac{1}{12})$$

We can now use this to find an expression for $\log C$.

$$\begin{aligned}
\log C &= \log\left(\frac{u_{2h+2k}}{u_{2h}u_{2k}}\right) \\
&= \log u_{2h+2k} - \log u_{2h} - \log u_{2k} \\
&= (h+k)\log(h+k) + (h+k)\log 2 + \tfrac{1}{2}\log 2 - (h+k) + S_{h+k} \\
&\quad - h\log h - h\log 2 - \tfrac{1}{2}\log 2 + h - S_h \\
&\quad - k\log k - k\log 2 - \tfrac{1}{2}\log 2 + k - S_k \\
&= (h+k)\log(h+k) - h\log h - k\log k - \tfrac{1}{2}\log 2 + S, \qquad (30)
\end{aligned}$$

where $S = S_{h+k} - S_h - S_k$ and therefore $-\frac{1}{4} < S < \frac{1}{4}$.
Letting

$$h = Qk \qquad (31)$$

and expressing (30) in terms of Q gives

$$\log C = (Qk+k)\log(Qk+k) - Qk\log Qk - k\log k - \tfrac{1}{2}\log 2 + S.$$

Since $Q+1 = Q\left(1+\frac{1}{Q}\right)$ and therefore $\log(Q+1) = \log Q + \log\left(1+\frac{1}{Q}\right)$ it follows that

$$\begin{aligned}
\log C &= (Qk+k)\log Qk + (Qk+k)\log\left(1+\tfrac{1}{Q}\right) \\
&\quad - Qk\log Qk - k\log k - \tfrac{1}{2}\log 2 + S \\
&= k\log Qk + Qk\log\left(1+\tfrac{1}{Q}\right) + k\log\left(1+\tfrac{1}{Q}\right) - k\log k - \tfrac{1}{2}\log 2 + S \\
&= k\log Q + Qk\log\left(1+\tfrac{1}{Q}\right) + k\log\left(1+\tfrac{1}{Q}\right) - \tfrac{1}{2}\log 2 + S \\
&= k\log(Q+1) + Qk\log\left(1+\tfrac{1}{Q}\right) - \tfrac{1}{2}\log 2 + S \qquad (32)
\end{aligned}$$

Using the Maclaurin expansion of $\log(1+x)$, we find that $\log\left(1+\frac{1}{Q}\right)$ can be represented as

$$\begin{aligned}
\log\left(1+\frac{1}{Q}\right) &= \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n}\left(\frac{1}{Q}\right)^n \\
&= \sum_{n=1}^{\infty}\left\{\frac{1}{(2n-1)\,Q^{2n-1}} - \frac{1}{(2n)\,Q^{2n}}\right\}. \qquad (33)
\end{aligned}$$

Since $Q = \dfrac{h}{k}$ and $h > k$, it follows that $Q > 1$ and

$$\frac{1}{(2n-1)\,Q^{2n-1}} - \frac{1}{(2n)\,Q^{2n}} = \frac{1}{Q^{2n}}\left(\frac{2n\,(Q-1)+1}{2n\,(2n-1)}\right) > 0 \quad \forall n \in \mathbb{N}.$$

i.e every term in (33) is positive.
It follows that if we take only finitely many terms of (33), the result will be smaller than $\log\left(1+\frac{1}{Q}\right)$.
Therefore,

$$\log\left(1+\frac{1}{Q}\right) > \frac{1}{Q} - \frac{1}{2Q^2}.$$

Substituting this inequality into (32) and using the fact that $-\frac{1}{4} < S < \frac{1}{4}$ gives

$$\log C > k\log(Q+1) + k - \frac{k}{2Q} - \frac{1}{2}\log 2 - \frac{1}{4}. \tag{34}$$

Furthermore,

$$\begin{aligned}(\pi(p)-1)\log(2h+2k) &= (\pi(p)-1)\log(2kQ+2k)\\ &= (\pi(p)-1)\left(\log 2k + \log(Q+1)\right)\\ &= (\pi(p)-1)\log(Q+1) + \pi(p)\log 2k - \log 2k\\ &< (\pi(p)-1)\log(Q+1) + \pi(p)\log p - \log\frac{p-1}{2}. \end{aligned}\tag{35}$$

From (34), (29) and (35) we have

$$\begin{aligned}k\log(Q+1) + k - \frac{k}{2Q} - \frac{1}{2}\log 2 - \frac{1}{4} &< \log C\\ &< (\pi(p)-1)\log(2h+2k)\\ &< (\pi(p)-1)\log(Q+1) + \pi(p)\log p - \log\frac{p-1}{2}\end{aligned}$$

Which rearranges to give

$$(k-\pi(p)+1)\log(Q+1) < -k + \frac{k}{2Q} + \frac{1}{2}\log 2 + \frac{1}{4} + \pi(p)\log p - \log\frac{p-1}{2}$$

Remembering $p = 2k+1$ and expressing everything in terms of p gives

$$\begin{aligned}\left(\frac{p+1}{2} - \pi(p)\right)\log(Q+1) &< -\frac{p-1}{2} + \frac{p-1}{4Q} + \frac{1}{2}\log 2 + \frac{1}{4} + \pi(p)\log p - \log\frac{p-1}{2}\\ &= -\frac{p}{2} + \frac{1}{2} + \frac{p}{4Q} - \frac{1}{4Q} + \pi(p)\log p + \frac{1}{2}\log 2 + \frac{1}{4} - \log\frac{p-1}{2}\\ &< -\frac{p}{2} + \frac{p}{4Q} + \pi(p)\log p + \frac{1}{2}\log 2 + \frac{1}{2} + \frac{1}{4} - \log\frac{p-1}{2},\end{aligned}\tag{36}$$

since $-\dfrac{1}{4Q} < 0 \ \ \forall Q > 1$.

For $p > 7$ it is true that

$$\frac{p-1}{2} \geq 5 > e^{\frac{1}{2}\log 2 + \frac{1}{4} + \frac{1}{2}} \tag{37}$$

It follows from (36) that if there exists a counterexample for some $p \geq 11$ then the following inequality must hold

$$\left(\frac{p+1}{2} - \pi(p)\right)\log(Q+1) < -\frac{p}{2} + \frac{p}{4Q} + \pi(p)\log p \tag{38}$$

Part 3

Using this inequality, we will show that if we introduce a lower bound R on $Q+1$, then the values of p for which there can exist a counterexample are bounded from above.

For $Q \leq 4$

$$\frac{2h+2k}{2h} = \frac{Q+1}{Q} \leq \frac{5}{4}$$

The odd numbers contained in the interval

$$2h < x \leq \frac{5}{4} \cdot 2h \tag{39}$$

will be the elements of our sequence (19) of consecutive odd numbers between $2h$ and $2h+2k$.
Note that,

$$2h \geq 2k+2 > 2k+1 = p.$$

It follows that for $p \geq 29$, $2h \geq 29$ and therefore, by Lemma 1, the interval (39) must contain at least one prime number $P > 2h > p$. Therefore, for $p \geq 29$, a counterexample can only exist for $Q > 4$.

Let us now introduce an upper bound R on $Q+1$.

If there is a counterexample for which

$$Q+1 \geq R > 5 \tag{40}$$

Then, using Approximation 1,

$$\pi(p) < \frac{3}{2}\frac{p}{\log p}$$

and the inequality (38), it follows that

$$\left(\frac{p}{2} - \frac{3}{2}\frac{p}{\log p}\right)\log R < -\frac{p}{2} + \frac{p}{4\left(\log R - 1\right)} + \frac{3}{2}p.$$

So,

$$\left(\log R - 2 - \frac{1}{2R-2}\right)\log p < 3\log R.$$

In particular, if $\log R > 3$ then the coefficient of $\log p$ will be positive and the inequality will still hold after division by the coefficient of $\log p$ on both sides. Therefore, we suppose

$$\log(Q+1) \geq \log R > 3 \tag{41}$$

In this case, we get $p < e^b$ where

$$b = \frac{3\log R}{\log R - 2 - \frac{1}{2R-2}}.$$

If we choose $R = 21$ then $\log R > 3$ as required, so it must follow that $p < e^b$, where

$$b = \frac{3\log 21}{\log 21 - 2 - \frac{1}{40}} < 9 + \frac{1}{4}$$

It follows that for $Q + 1 \geq 21$,

$$p < e^{9+\frac{1}{4}} = 10404.56...$$

Part 4

By considering large values of p we can find another inequality which must hold if there exists a counterexample for p. We will however show that the inequality does not hold, in turn proving the theorem for large p.

Suppose that, $p \geq 14285$ then it follows from the previous part, that $Q + 1 < 21$. For a prime number $q > \sqrt{21p}$ we have

$$\begin{aligned} q^2 &> 21p \\ &> (Q+1)p \\ &> \left(\frac{h}{k} + 1\right)2k \\ &= 2h + 2k. \end{aligned}$$

It follows from (28) that

$$\log C = \sum_{\substack{q\in\mathbb{P}\\ 3\le q\le\sqrt{21p}}} v_q \log q + \sum_{\substack{q\in\mathbb{P}\\ \sqrt{21p}<q\le p}} v_q \log q.$$

For $q > \sqrt{21}$, it follows from (27) that $v_q \le 1$, giving us

$$\begin{aligned}\log C &\le \sum_{\substack{q\in\mathbb{P}\\ 3\le q\le\sqrt{21p}}} v_q \log q + \sum_{\substack{q\in\mathbb{P}\\ \sqrt{21p}<q\le p}} \log q \\ &= \Big(\pi(\sqrt{21p}) - 1\Big)\log(2h+2k) + \vartheta(p) - \vartheta(\sqrt{21p}),\end{aligned}$$

where $\vartheta(p)$, is defined, as in Section 2, to be the sum of the logarithms of primes up to and including p.
Using this inequality, we can use a similar method as in Part 2 to find another inequality (similar to (38)), that must hold if there exists a counterexample for p:

$$\left(\frac{p+1}{2} - \pi(\sqrt{21p})\right)\log(Q+1) < -\frac{p}{2} + \frac{p}{4Q} + \pi(\sqrt{21p})\log p + \vartheta(p) - \vartheta(\sqrt{21p}). \tag{42}$$

Note that,

$$Q > 4, \;\; \log 5 > \frac{8}{5} \;\text{ and }\; \pi(\sqrt{21p}) < \frac{3}{2}\frac{\sqrt{21p}}{\log\big(\sqrt{21p}\big)} < \frac{3\sqrt{21p}}{\log p}. \tag{43}$$

Then it follows from (42) and (43) that

$$\begin{aligned}\frac{4p}{5} + \frac{4}{5} - \frac{24\sqrt{21p}}{5\log p} &= \left(\frac{p}{2} + \frac{1}{2} - \frac{3\sqrt{21p}}{\log p}\right)\cdot\frac{8}{5} \\ &< \left(\frac{p}{2} + \frac{1}{2} - \pi(\sqrt{21p})\right)\cdot\log 5 \\ &< \left(\frac{p+1}{2} - \pi(\sqrt{21p})\right)\cdot\log(Q+1) \\ &< -\frac{p}{2} + \frac{p}{4Q} + \pi(\sqrt{21p})\log p + \vartheta(p) - \vartheta(\sqrt{21}) \\ &< -\frac{p}{2} + \frac{p}{16} + 3\sqrt{21p} + \vartheta(p) - \vartheta(\sqrt{21p}),\end{aligned}$$

which rearranges to give

$$\left(\frac{4}{5} + \frac{1}{2} - \frac{1}{16}\right)p < \frac{24}{5}\frac{\sqrt{21p}}{\log p} + 3\sqrt{21p} + \vartheta(p) - \vartheta(\sqrt{21p}). \tag{44}$$

Let $\psi(x)$ be defined as in Section 2 to be

$$\psi(x) = \sum_{n=1}^{\infty} \vartheta(x^{\frac{1}{n}})$$

and then, since $\psi(x) - \vartheta(x)$ is a non-decreasing function and $p > \sqrt{21p}$

$$\vartheta(p) - \vartheta(\sqrt{21p}) \leq \psi(p) - \psi(\sqrt{21p})$$

Using Approximation 3 we know that,

$$\varphi(p) < \frac{6}{5}ap + 3\log^2 p + 8\log p + 5$$
$$\varphi(\sqrt{21p}) \geq a\sqrt{21p} - 5\log\sqrt{21p} - 5$$

for $a = 0.92129...$

This gives

$$\vartheta(p) - \vartheta(\sqrt{21p}) < 1.106p - 0.92 \cdot \sqrt{21p} + 3\log^2 p + 13\log p + 10$$

Dividing (44) by p therefore gives

$$\frac{4}{5} + \frac{1}{2} - \frac{1}{16} - 1.106 < \frac{24}{5}\frac{\sqrt{21}}{\sqrt{p}\cdot\log p} + \frac{2.08\cdot\sqrt{21}}{\sqrt{p}} + \frac{3\log^2 p + 13\log p + 10}{p}. \quad (45)$$

Since the right hand side is monotonically decreasing for $p > e$, if the inequality does not hold for $p = 14285$, then it will not hold for any $p \geq 14285$.
Using the following inequalities

$$9.5 < \log 14285 < 9.6$$
$$\sqrt{14285} > 119$$
$$\sqrt{21} < 4.6$$

it is easy to verify that the inequality (45) does not hold. Therefore no counterexample can occur for $p \geq 14285$.

Part 5
Using different bounds on $Q+1$, we will treat different intervals of p, showing in turn that no counterexamples can exist for $p > 100$.

If there exists a counterexample for p, of the form

$$2h+1, \quad 2h+3, \quad \ldots, \quad 2h+2k-1 \quad (h > k)$$

then it must be true that there are no prime numbers between $2h$ and $2h + 2k$. Remembering that $h = Qk$ and supposing that

$$Q + 1 < R, \quad (46)$$
$$Rp \leq n. \quad (47)$$

It follows that

$$\begin{aligned} 2h + 2k &= \left(\frac{h}{k} + 1\right) 2k \\ &< (Q+1)p \\ &\leq n. \end{aligned}$$

Since

$$2h, \;\; 2h+1, \;\; 2h+3, \;\; \ldots, \;\; 2h+2k-1, \;\; 2h+2k$$

are all composite numbers, it must be true that $L(2h+2k) > 2k$ where $L(x)$ is defined, as in Section 2, to be the length of the longest sequence of consecutive composite numbers up to and including x.
It follows then, that

$$Q + 1 < R, \;\; Rp \leq n \implies L(n) \geq p. \tag{48}$$

In Part 3 of this proof we found that if

$$\begin{aligned} Q + 1 &\geq R, \\ \log R > a &\geq 3, \\ b = \frac{3a}{a - 2 - \frac{1}{2R-2}} &< \beta, \\ e^{\beta} &< M, \end{aligned}$$

then $p < M$ must hold. Here is a table of particular values for R, a, β, M

R	a	β	M
21	3	9.25	10405
28	3.3	7.8	2450
40	3.6	6.9	1000
50	3.9	6.2	500
100	4.6	5.35	215
230	5.43	4.76	117
400	5.9	4.6	100

(49)

Suppose there exists a counterexample for some p in the interval $10405 < p < 14285$, then $Q + 1 < 21$ (since otherwise, according to the table, $p < 10405$). From (48) we know that if $Q + 1 < 21$ then $L(n) \geq p$ where $n \geq 21p$. In our case

$$21 \cdot 10405 < 21p < 21 \cdot 14285 < 300000 \tag{50}$$

Since $300000 > 21p$ for all p in our interval, then $L(300000) \geq p$ must be true for all p in our interval. However, from Approximation 5, we know that $L(300000) < 2000$. This would imply $p < 2000$. No such p exist in our interval, so there exists no p in our interval for which a counterexample is possible.

Suppose there exists a counterexample for some p in the interval $2450 < p < 10405$, then $Q + 1 < 28$. Since $300000 > 28p$ for all p in our interval, then from (48) we know that $p \leq L(300000)$. Also, we know from Approximation 5, we know that $L(300000) < 2000$, which implies that $p < 2000$. No such p exist in our interval, so there exists no p in our interval for which a counterexample is possible.

Using Approximation 5 and (48) we are able to show that there exists no counterexample for p in any of the following intervals:

$$\begin{aligned} 1000 < p < 2450, \\ 500 < p < 1000, \\ 215 < p < 500, \\ 117 < p < 215, \\ 100 < p < 117. \end{aligned}$$

There exists no counterexample therefore, for $p > 100$.

Part 6

We will use the inequality from Part 2 and the method used in Part 5 to show that there are no counterexamples for $p \geq 47$.

Suppose there exists a counterexample for some p in the interval $47 \leq p \leq 100$, then if we are able to show that $Q + 1 < 50$, then $5000 > 50p$ would be true for all p in our interval and from Approximation 5 and (48) this would imply $p < 47$ and therefore there exists no counterexample for p in our interval.

Suppose by contradiction that $Q + 1 \geq 50$, then it is true that $\log(Q + 1) > 3.9$. At the end of Part 2, we showed that if there exists a counterexample for $p \geq 11$, then the inequality (38) must hold. If $Q + 1 \geq 50$ and therefore $\log(Q + 1) > 3.9$, then it follows from (38) that

$$3.9 \left(\frac{p+1}{2} - \pi(p) \right) < -\frac{p-1}{2} - \frac{1}{2} + \frac{p}{4 \cdot 49} + m \log p.$$

Since $p \leq 97 < 2 \cdot 49$, it follows that

$$\begin{aligned} 3.9 \left(\frac{p+1}{2} - \pi(p) \right) &< -\frac{p-1}{2} + \pi(p) \log p + \frac{p}{4 \cdot 49} - \frac{1}{2} \\ &< -\frac{p-1}{2} + \pi(p) \log p. \end{aligned}$$

This rearranges to give

$$4.9p + 2.9 < 2\pi(p)(3.9 + \log p).$$

It can be verified that this inequality does not hold for any prime numbers in the interval $47 \leq p \leq 97$, so $Q + 1 < 50$.

We can therefore show, by the same method used in Part 5, that there are no counterexamples for p in our interval.

There exists no counterexample therefore, for $p \geq 47$.

Part 7

We will conclude the proof by showing that the counterexamples listed in the Theorem are the only possible counterexamples. In order to do this, we will make use of Lemma 2.

It is obvious that for $p = 3$ then all powers of 3 greater than 3 are counterexamples. From Lemma 2 it follows that the only counterexample for $p = 5$ is the sequence $25, 27$. It is left to investigate the following prime numbers

$$7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43. \tag{51}$$

In a sequence of k consecutive odd numbers, we know from Gauss Bracket Property 4, that there are at most $\left[\frac{k+q-1}{q}\right]$ multiples of an odd prime number q.
Let

$$x_p = k - \sum_{7 \leq q \leq p} \left[\frac{k+q-1}{q}\right].$$

If there exists a counterexample for p and x_p is positive, then at least x_p numbers in our counterexample sequence, must be of the form $3^\alpha \cdot 5^\beta$. For all p in our remaining list of prime numbers (51), $x_p \geq 2$. Therefore, it must be true that at least 2 numbers of the form $3^\alpha \cdot 5^\beta$ would appear in a counterexample. Any two terms of a sequence (19) cannot differ more than $2k-2$, so in order for a pair of numbers a, b of the form $3^\alpha \cdot 5^\beta$ to both appear in a sequence, $b - a \leq 2k - 2 = p - 3$ must hold.

For $p = 7$, so $k = 3$, in order for there to exist a counterexample, there would need to be a pair of numbers a, b of the form $3^\alpha \cdot 5^\beta$ such that $b - a \leq 4$, both of which are greater than 7. From Lemma 2 we know that the only pair satisfying these conditions is 25, 27. There are only 2 sequences of $k = 3$ consecutive odd numbers containing 25, 27 and they are 23, 25, 27 and 25, 27, 29, neither of which are counterexamples as 23 and 29 are prime numbers. Therefore, there is no counterexample for $p = 7$ and we do not consider the pair 25, 27 for $p > 7$.

For $p = 11$, so $k = 5$, we look for a, b greater than 11 such that $b - a \leq 8$ that we have not yet ruled out. From Lemma 2 we know that the only pair satisfying these conditions is $75, 81$. (We already know from the previous case that no counterexample can contain 25 and 27.) Any sequence of 5 consecutive odd numbers containing both 75 and 81 must also contain 77 and 79. Since 79 is a prime number, no such sequence is a counterexample. Therefore, there is no counterexample for $p = 11$ and we do not consider the pair 75, 81 for $p > 11$.

For $p = 13$, so $k = 6$, we look for a, b greater than 13 such that $b - a \leq 10$. From Lemma 2 we know that the only pairs satisfying these conditions that we have not previously ruled out are 15, 25 and 125, 135. Any sequence of 6 consecutive odd numbers containing 15 and 25 must also contain 17, 19 and 23, all of which are prime, meaning that no such sequence is a counterexample. Similarly, any sequence of 6 consecutive odd numbers containing 125 and 135 must also contain 127 and 131, both of which are prime, meaning that no such sequence is a counterexample. Therefore, there is no counterexample for $p = 13$ and we do not consider the pairs 15, 25 or 125, 135 for $p > 13$.

For $p = 17$, so $k = 8$, we look for a, b greater than 17 such that $b - a \leq 14$. From Lemma 2 we know that no such pair exists that we have not previously ruled out. Therefore, there is no counterexample for $p = 17$.

For $p = 19$, so $k = 9$, we look for a, b greater than 19 such that $b - a \leq 16$. From Lemma 2 we know that no such pair exists that we have not previously ruled out. Therefore, there is no counterexample for $p = 13$.

For $p = 23$, so $k = 11$, we look for a, b greater than 23 such that $b - a \leq 20$. From Lemma 2 we know that the only pairs satisfying these conditions that we have not previously ruled out are 25, 45, 27, 45 and 225, 243. Any sequence of 11 consecutive odd numbers containing 25 and 45 or 27 and 45 must also contain 29, 31, 37, 41 and 43, all of which are prime, meaning that no such sequence is a counterexample. Similarly, any sequence of 11 consecutive odd numbers containing 225 and 243 must also contain 227, 229, 233, 239 and 241, all of which are prime, meaning that no such sequence is a counterexample. Therefore, there is no counterexample for $p = 23$ and we do not consider the pairs 25, 45, 27, 45 or 225, 243 for $p > 23$.

We have shown that there is no counterexample for $7 \leq p \leq 23$. Not only that, but we have also shown that there does not exist a counterexample for $p > 23$ that contains a pair a, b of the form $3^\alpha \cdot 5^\beta$ such that $b - a \leq 20$ as we have ruled them all out. Therefore, any pair a, b of the form $3^\alpha \cdot 5^\beta$ that both appear in a counterexample must have a difference of at least 22. For $29 \leq p \leq 43$, $x_p \geq 3$, so it must be true that there are 3 numbers $a < b < c$ of the form $3^\alpha \cdot 5^\beta$ in any counterexample. We also know that $b - a \geq 22$ and $c - b \geq 22$ so it must be true that $2 \cdot 22 \leq c - a \leq p - 3$ but no value of $p \leq 43$ can satisfy this inequality so there cannot exist a counterexample for $29 \leq p \leq 43$.

Therefore, there is no counterexample for $p \geq 7$ and the only counterexamples for $p = 3$ and $p = 5$ are those stated in the theorem. □

7.2 Proof of Corollary 1

Corollary 1 (Corollary of Theorem 1)**.**
For $k \in \mathbb{N}$ $(k > 2)$, it is true that any sequence of k consecutive odd numbers, for which all terms are greater than $2k + 1$, will contain at least one term with a prime

factor greater than $2k+1$.

$$2h+1, \quad 2h+3, \quad \ldots, \quad 2h+2k-1 \quad (h>k)$$

For $k=1$, the only counterexamples are powers of $3^\alpha > 3$ and for $k=2$, the only counterexample is 25.

Proof of Corollary 1.
For every $k>2$ there exists at least one odd prime number p such that $p \leq 2k+1$. Let us take the largest prime number satisfying this inequality and call it p^*. If $p^* = 2k^* + 1$, then

$$p^* \leq 2k+1 \tag{52}$$
$$k^* \leq k \tag{53}$$

Since $p^* = 2k^* + 1$ is prime, we know from Theorem 1 that in any sequence of k^* consecutive odd numbers greater than p^* there exists at least one term of the sequence divisible by a prime number $q > p^*$.
In other words, any sequence satisfying the following condition must have the following property:

Condition 1.
The sequence must have k^* terms, all of which are greater than p^*.

Property 1.
At least one of the terms is divisible by a prime number greater than p^*.

In order to prove Corollary 1 we need to show that any sequence satisfying the following condition must have the following property:

Condition 2.
The sequence must have k terms, all of which are greater than $2k+1$.

Property 2.
At least one of the terms is divisible by a prime number greater than $2k+1$.

Note that if we have a sequence that satisfies Condition 2, then (from (52) and (53)) a subsequence will satisfy Condition 1. Therefore, any sequence satisfying Condition 2 has Property 1. Since there are no prime numbers between p^* and $2k+1$ by choice of p^*, Property 1 and Property 2 are equivalent. It follows that every sequence satisfying Condition 2 has Property 2 and we have proven Corollary 1. □

8 Some Theorems on Irreducibility

In this section, the proofs of Theorems 2 and 3 are considered. The first parts of the proofs of these theorems are very similar but the proof of theorem 3 takes a bit longer due to the counterexamples that arise. An important corollary of these two theorems, also proven by Schur in [13] is that Hermite polynomials are irreducible, the proof of this will be presented at the end of this section.

8.1 Proof of Theorem 2

Theorem 2.
For $n > 1$, every polynomial of the form

$$f(x) = 1 + g_1\frac{x^2}{u_2} + g_2\frac{x^4}{u_4} + \cdots + g_{n-1}\frac{x^{2n-2}}{u_{2n-2}} \pm \frac{x^{2n}}{u_{2n}}$$

with $g_\nu \in \mathbb{Z}$, is irreducible over $\mathbb{Q}$.

Proof of Theorem 2.
Let $f(x)$ be a polynomial of the form

$$f(x) = 1 + g_1\frac{x^2}{u_2} + g_2\frac{x^4}{u_4} + \cdots + g_{n-1}\frac{x^{2n-2}}{u_{2n-2}} \pm \frac{x^{2n}}{u_{2n}} \tag{54}$$

with $g_\nu \in \mathbb{Z}$. Then, $F(x) = u_{2n}f(x)$ is a polynomial of the form

$$F(x) = u_{2n} + g_1u_{2n}\frac{x^2}{u_2} + g_2u_{2n}\frac{x^4}{u_4} + \cdots + g_{n-1}u_{2n}\frac{x^{2n-2}}{u_{2n-2}} \pm x^{2n}. \tag{55}$$

It follows, that $F(x)$ is an integer polynomial with leading coefficient ± 1. In order to prove the theorem, it is therefore enough to prove that $F(x)$ is irreducible over $\mathbb{Z}$. For $2n = 2$, $F(x) = 1 \pm x^2$. Since $1 - x^2$ is reducible over $\mathbb{Z}$, $F(x)$ could be reducible for $n = 1$. We therefore wish to prove that $F(x)$ is irreducible for $n > 1$ which would, in turn, prove the theorem.

Part 1

Suppose by contradiction, that $F(x)$ is reducible in $\mathbb{Z}$. Then,

$$F(x) = A(x)B(x), \quad A(x) = x^k + a_1x^{k-1} + \cdots + a_k.$$

where $A(x)$ and $B(x)$ are integer polynomials, $A(x)$ is irreducible and $2n \geq 2k$ i.e. $n \geq k$. It follows that the integer a_k must be a factor of u_{2n} and must therefore be odd.
Let $p \geq 3$ be a prime factor of a_k and let α be a root of $A(x)$. Then,

$$A(\alpha) = \alpha^k + a_1\alpha^{k-1} + \cdots + a_k = 0$$

so that

$$\alpha(\alpha^{k-1} + a_1\alpha^{k-2} + \cdots + a_{k-1}) = -a_k$$

and it follows that α divides a_k in the algebraic number field $\mathbb{Q}(\alpha)$. Note that α is an algebraic integer and $\mathbb{Q}(\alpha)$ is an algebraic field extension of degree k. We can therefore define ideals of the ring of integers $\mathcal{O}_{\mathbb{Q}(\alpha)}$. From Ideal Property 2, it follows from the fact that α divides a_k that $\langle\alpha\rangle$ divides $\langle a_k\rangle$. Similarly, by choice of p, we know that $\langle p\rangle$ divides $\langle a_k\rangle$. Since $\langle\alpha\rangle$ and $\langle p\rangle$ are both divisible by $\langle a_k\rangle$, it follows from Ideal Property 3 that there exists a prime ideal $\mathfrak{p}$ which divides $\langle\alpha\rangle$ and $\langle p\rangle$ at least once. Let the highest power of $\mathfrak{p}$ that divides $\langle\alpha\rangle$ be $\mathfrak{p}^r$ and the highest power of $\mathfrak{p}$ that divides $\langle p\rangle$ be $\mathfrak{p}^s$. Clearly, $r \geq 1$ and $s \geq 1$ by choice of $\mathfrak{p}$, but it also follows from Lemma 3 that $s \leq k$. Since α is a root of $A(x)$ and therefore of $F(x)$, it follows that

$$u_{2n} + g_1 u_{2n}\frac{\alpha^2}{u_2} + g_2 u_{2n}\frac{\alpha^4}{u_4} + \cdots + g_{n-1}u_{2n}\frac{\alpha^{2n-2}}{u_{2n-2}} \pm \alpha^{2n} = 0. \tag{56}$$

Let $g_0 = 1$, $g_n = \pm 1$, then every term has the form $g_\nu u_{2n}\frac{\alpha^{2\nu}}{u_{2\nu}}$. Since u_{2n} is divisible by exactly $p^{\lambda_n(p)}$, it follows from our choice of r and s above that

$$u_{2n} \text{ is divisible by exactly } \mathfrak{p}^{\lambda_n(p)s}, \alpha^{2n} \text{ is divisible by exactly } \mathfrak{p}^{2nr}.$$

Since we don't know the divisors of g_ν, it follows that,

$$g_\nu u_{2n}\frac{\alpha^{2\nu}}{u_{2\nu}} \text{ is divisible by at least } \mathfrak{p}^{\lambda_n(p)s+2\nu r-\lambda_\nu(p)s}.$$

Suppose for all $\nu \geq 1$, $2\nu r > \lambda_\nu(p)s$, then every term except u_{2n} is divisible by a higher power of $\mathfrak{p}$ than u_{2n}, which from (56) cannot be true. It therefore follows that there exists at least one $\nu \geq 1$ such that

$$2\nu r \leq \lambda_\nu(p)s.$$

It follows from the fact that

$$r \geq 1, \quad 1 \leq s \leq k$$

that

$$2\nu \leq \lambda_\nu(p)k$$

for some $\nu \geq 1$. From Lemma 4 we know that

$$\lambda_\nu(p) < \frac{2\nu}{p},$$

therefore

$$p < k. \tag{57}$$

For $k \leq 3$ it follows from our choice of p and from the fact that $p < k$, that a_k has no prime factors and must therefore be equal to ± 1.

Part 2

Let us rewrite $F(x)$ as

$$F(x) = \pm x^{2n} + g_{n-1}(2n-1)x^{2n-2} + g_{n-2}(2n-1)(2n-3)x^{2n-4} + \cdots . \tag{58}$$

Clearly, if q is an (odd) prime number which divides $(2n-1)$, then q will divide every term except the first in (58), if instead q divides $(2n-3)$, then q will divide every term except the first two in (58). We can generalise this property by introducing a parameter l. Then, if q divides $(2n-2l+1)$, then $F(x) \mod q$ will be divisible by $x^{2n-2l+2}$. It follows that if q divides any of the following l numbers

$$2n-2l+1,\ 2n-2l+3, \ldots, 2n-1 \quad (l \geq 1)$$

then $F(x) \mod q$ is divisible by at least $x^{2n-2l+2}$.
Suppose that

$$2n-2l+2 > 2n-k \quad (2l < k+2). \tag{59}$$

Recall that $B(x)$ is an integer polynomial of the form

$$B(x) = \pm x^{2n-k} + b_1 x^{2n-k-1} + \cdots + b_{2n-k},$$

therefore, $B(x) \mod q$ can be at most divisible by x^{2n-k} (in the case $b_1, \ldots b_{2n-k}$ are all divisible by q) so since $2l < k+2$, $A(x) \mod q$ must be divisible by at least x and a_k must be divisible by q and therefore from (57) $q < k$.
In particular, if q is a prime divisor of $2n-1$ (the case $l = 1$) then q must divide a_k. Therefore all prime divisors of $2n-1$ (where $2n-1 \geq 3$ because we are considering $n > 1$) are also prime divisors of a_k so that a_k cannot be equal to ± 1 and therefore $k \leq 3$ cannot be true. We therefore only consider $k > 3$.
Let $k > 3$, then for $c \geq 1$, $k = 2c+2$ if k even or $2c+3$ if k odd, we therefore represent k as

$$k = 2c + 2 + \epsilon \quad \epsilon = 0 \text{ or } 1. \tag{60}$$

From (59), it follows that the largest value of l (for k of the above form) is of the form

$$l = c + 1 + \epsilon. \tag{61}$$

Using the fact that $n \geq k$ and the above forms of k and l, we know that

$$2n-2l+1 \geq 2k-2l+1 = 2c+3 > 2c+1 \tag{62}$$

for all $k > 3$ and $2l < k + 2$. Since $q < k$ is an odd prime and $\epsilon = 0$ if k even and $\epsilon = 1$ if k odd, we know that

$$q \leq k - 1 - \epsilon = 2c + 1. \tag{63}$$

In conclusion, if $F(x)$ is reducible over $\mathbb{Z}$, then we must have a sequence of $l = c+1+\epsilon$ i.e. at least $c + 1$ odd numbers which are all greater than $2c + 1$ (from (62)) and are only divisible by prime numbers $q \leq 2c + 1$ (from (63)). It follows from Corollary 1 that this is impossible for $c > 2$ but this also cannot happen for $c = 1$ or $c = 2$. The case $c = 1$ would be a sequence of 2 consecutive numbers, that are both greater than 3 and are only divisible by prime numbers $q \leq 3$, it is impossible that two powers of 3 are consecutive odd numbers and therefore there exists no such sequence. The case $c = 2$ would be a sequence of 3 consecutive numbers, that are both greater than 5 and of the form $3^\alpha 5^\beta$ which we have also shown in the proof of Theorem 1 to not be possible. Since no such sequence exists, $F(x)$ must be irreducible over $\mathbb{Z}$ and therefore so must $f(x)$ be irreducible over $\mathbb{Q}$ for $n > 1$. □

8.2 Proof of Theorem 3

Theorem 3.
Every polynomial of the form

$$g(x) = 1 + g_1\frac{x^2}{u_4} + g_2\frac{x^4}{u_6} + \cdots + g_{n-1}\frac{x^{2n-2}}{u_{2n}} \pm \frac{x^{2n}}{u_{2n+2}} \tag{64}$$

with $g_\nu \in \mathbb{Z}$, is irreducible over $\mathbb{Q}$, except for the case that $2n = 3^r - 1$ for some $r \geq 2$. In this case, $g(x)$ has just one factor $x^2 \pm 3$ and division by this factor results in an irreducible polynomial over $\mathbb{Q}$.

Proof of Theorem 3.
Let $g(x)$ be a polynomial of the form

$$g(x) = 1 + g_1\frac{x^2}{u_4} + g_2\frac{x^4}{u_6} + \cdots + g_{n-1}\frac{x^{2n-2}}{u_{2n}} \pm \frac{x^{2n}}{u_{2n+2}} \tag{65}$$

with $g_\nu \in \mathbb{Z}$. Then $G(x) = u_{2n+2}g(x)$ is a polynomial of the form

$$G(x) = u_{2n+2} + g_1u_{2n+2}\frac{x^2}{u_4} + g_2u_{2n+2}\frac{x^4}{u_6} + \cdots + g_{n-1}u_{2n+2}\frac{x^{2n-2}}{u_{2n}} \pm x^{2n}. \tag{66}$$

In order to prove that $g(x)$ is irreducible over $\mathbb{Q}$, it is enough to prove that $G(x)$ is irreducible over $\mathbb{Z}$.

Part 1

Suppose by contradiction, that $G(x)$ is reducible in $\mathbb{Z}$. Then,

$$G(x) = A(x)B(x), \quad A(x) = x^k + a_1x^{k-1} + \cdots + a_k.$$

where $A(x)$ and $B(x)$ are integer polynomials, $A(x)$ is irreducible and $2n \geq 2k$ i.e. $n \geq k$. It follows that the integer a_k must be a factor of u_{2n+2} and must therefore be odd.
Let $p \geq 3$ be a prime divisor of a_k and let α be a root of $A(x)$. Then,

$$A(\alpha) = \alpha^k + a_1\alpha^{k-1} + \cdots + a_k = 0$$

so that

$$\alpha(\alpha^{k-1} + a_1\alpha^{k-2} + \cdots + a_{k-1}) = -a_k$$

and it follows that α divides a_k in the algebraic number field $\mathbb{Q}(\alpha)$. Just as in the proof of Theorem 2, it follows that there exists a prime ideal $\mathfrak{p}$ which divides $\langle\alpha\rangle$ and $\langle p\rangle$ and the highest powers of $\mathfrak{p}$ which divide $\langle\alpha\rangle$ and $\langle p\rangle$ are $\mathfrak{p}^r$ and $\mathfrak{p}^s$, where

$$r \geq 1, \quad 1 \leq s \leq k \tag{67}$$

Since α is a root of $A(x)$ and therefore of $G(x)$, it follows that

$$u_{2n+2} + g_1u_{2n+2}\frac{\alpha^2}{u_4} + g_2u_{2n+2}\frac{\alpha^4}{u_6} + \cdots + g_{n-1}u_{2n+2}\frac{\alpha^{2n-2}}{u_{2n}} \pm \alpha^{2n} = 0. \tag{68}$$

Let $g_0 = 1$, $g_n = \pm 1$, then every term has the form

$$g_\nu u_{2n+2}\frac{\alpha^{2\nu}}{u_{2\nu+2}}.$$

Since u_{2n+2} is divisible by exactly $p^{\lambda_{n+1}(p)}$, it follows from our choice of r and s above that

$$u_{2n+2} \text{ is divisible by exactly } \mathfrak{p}^{\lambda_{n+1}(p)s}, \alpha^{2n} \text{ is divisible by exactly } \mathfrak{p}^{2nr}.$$

Since we don't know the divisors of g_ν, it follows that,

$$g_\nu u_{2n+2}\frac{\alpha^{2\nu}}{u_{2\nu+2}} \text{ is divisible by at least } \mathfrak{p}^{\lambda_{n+1}(p)s+2\nu r-\lambda_{\nu+1}(p)s}.$$

Suppose for all $\nu \geq 1$, $2\nu r > \lambda_{\nu+1}(p)s$, then every term except u_{2n+2} is divisible by a higher power of $\mathfrak{p}$ than u_{2n+2}, which from (68) cannot be true. It therefore follows that there exists at least one $\nu \geq 1$ such that

$$2\nu r \leq \lambda_{\nu+1}(p)s.$$

It follows from (67) that

$$2\nu \leq \lambda_{\nu+1}(p)k \tag{69}$$

for some $\nu \geq 1$. From Lemma 4, it follows that

$$2\nu < \frac{2\nu+2}{p}k, \tag{70}$$

and from (69) we know that $\lambda_{\nu+1}(p) \geq 1$ and therefore

$$2\nu + 2 > p. \tag{71}$$

Suppose $p > k+1$ i.e. $k \leq p-2$, then it follows from (70) that

$$2\nu p < (2\nu+2)(p-2) = 2\nu p + 2p - 4\nu - 4$$

but this implies that $p > 2\nu + 2$ which from (71) cannot be true. Therefore

$$p \leq k+1. \tag{72}$$

We have shown that if $p \geq 3$ is a prime divisor of a_k, then $p \leq k+1$. It follows then, that for $k < 2$, a_k has no prime factors and must therefore be equal to ± 1.

Part 2

Let us rewrite $G(x)$ as

$$G(x) = \pm x^{2n} + g_{n-1}(2n+1)x^{2n-2} + g_{n-2}(2n+1)(2n-1)x^{2n-4} + \cdots . \tag{73}$$

Similar to the proof of Theorem 2, we introduce a parameter l. Then, if $q \geq 3$ is a prime divisor of $(2n-2l+3)$, then $G(x) \mod q$ will be divisible by $x^{2n-2l+2}$. It follows that if $q \geq 3$ is a prime divisor of any of the following l numbers

$$2n-2l+3,\ 2n-2l+5, \ldots, 2n+1 \quad (l \geq 1)$$

then $G(x) \mod q$ is divisible by at least $x^{2n-2l+2}$.
Suppose that

$$2n-2l+2 > 2n-k \quad (2l < k+2) \tag{74}$$

For the polynomial

$$B(x) = \pm x^{2n-k} + b_1 x^{2n-k-1} + \cdots + b_{2n-k},$$

$B(x) \mod q$ can be at most divisible by x^{2n-k} (in the case $b_1, \ldots b_{2n-k}$ are all divisible by q) so from (74), $A(x) \mod q$ must be divisible by at least x. Therefore, a_k must be divisible by q and from (72) $q \leq k+1$.
In particular, if q is a prime divisor of $2n+1$ (the case $l = 1$) then q must divide a_k. Therefore all prime divisors of $2n+1$ are also prime divisors of a_k. Since $n > 1$, $2n+1 > 3$ so that a_k cannot be equal to ± 1 and therefore $k < 2$ cannot be true. We therefore only consider $k \geq 2$.

Let $k \geq 2$, then for $c \geq 1$, $k = 2c$ if k even or $2c + 1$ if k odd, we therefore represent k as

$$k = 2c + \epsilon, \quad \epsilon = 0 \text{ or } 1. \tag{75}$$

It follows that the largest value of l such that (74) holds must be of the form

$$l = c + \epsilon. \tag{76}$$

Using the fact that $n \geq k$ and the above forms of k and l, we know that

$$2n - 2l + 3 \geq 2k - 2l + 3 = 2c + 3 > 2c + 1. \tag{77}$$

Since $q \leq k + 1$ and $\epsilon = 0$ if k even and $\epsilon = 1$ if k odd, we know that

$$q \leq k + 1 = 2c + 1 + \epsilon$$

which since q is odd implies that

$$q \leq 2c + 1. \tag{78}$$

In conclusion, if $G(x)$ is reducible over $\mathbb{Z}$, then we must have a sequence of $l = c + \epsilon$ odd numbers which are all greater than $2c + 1$ (from (77)) and are only divisible by prime numbers $q \leq 2c + 1$ (from (78)). It follows from Corollary 1 that this is impossible for $c > 2$.

The case $c = 1$ and $\epsilon = 1$ would be a sequence of 2 consecutive odd numbers $(2n - 1, 2n + 1)$, that are both greater than 3 and are only divisible by odd prime numbers $q \leq 3$. It is impossible that two powers of 3 are consecutive odd numbers and therefore there exists no such sequence. The case $c = 1$ and $\epsilon = 0$ would be a sequence of 1 odd number $(2n + 1)$, which is greater than 3 and only divisible by 3, so if $2n + 1 = 3^r > 3$ then such a sequence could exist and $G(x)$ could have an irreducible factor $A(x)$. Since, in this case $c = 1$ and $\epsilon = 0$, from (75), $k = 2$ and $A(x)$ would be a quadratic polynomial.

The case $c = 2$ and $\epsilon = 1$ would be a sequence of 3 consecutive numbers $(2n-3, 2n-1, 2n + 1)$, that are all greater than 5 and of the form $3^\alpha 5^\beta$ which we have already shown in the proof of Theorem 1.2 to not be possible. The case $c = 2$ and $\epsilon = 0$ would be a sequence of 2 consecutive odd numbers $(2n - 1, 2n + 1)$, that are greater than 5 and of the form $3^\alpha 5^\beta$, for which there exists just one sequence according to Corollary 1, namely 25, 27. So, if $2n + 1 = 27$ then such a sequence could exist and $G(x)$ could have an irreducible factor $A(x)$. Since, in this case $c = 2$ and $\epsilon = 0$, from (75), $k = 4$ and $A(x)$ would be a polynomial of degree 4.

It follows therefore that $G(x)$ and therefore $g(x)$ is irreducible over $\mathbb{Q}$ except for if $2n + 1 = 3^r > 3$ in which case there could exist a quadratic factor or if $2n + 1 = 27$

in which case there could exist a polynomial factor of degree 4. It is left to determine if such polynomial factors exist.

Part 3

We begin by investigating the case $2n+1 = 3^r > 3$, it follows that

$$2n = 3^r - 1 \geq 3^2 - 1 = 8.$$

We suppose that a quadratic polynomial

$$A(x) = x^2 + a_1 x + a_2$$

is an irreducible factor of $G(x)$. As discussed above, we know that a_2 is divisible by every prime divisor of $2n+1$, it therefore follows that

$$a_2 = \pm 3^\rho, \quad \rho \geq 1.$$

We now wish to prove by contradiction that $a_1 = 0$. Suppose a_1 is non-zero, then $A(x)$ is a non-even factor of the even polynomial $G(x)$, meaning that $A(-x)$ is a second factor of $G(-x) = G(x)$. This means that

$$G(x) = A(x)A(-x)C(x)$$

where $C(x)$ is some polynomial

$$C(x) = \pm x^{2n-4} + c_1 x^{2n-5} + \dots. \tag{79}$$

From (73) we know that if q is a prime divisor of $2n-1$, then $G(x) \mod q$ is divisible by at least x^{2n-2} and $C(x) \mod q$ is at most divisible by x^{2n-4} (from (79)), so

$$A(x)A(-x) = x^4 + (2a_2 - a_1^2)x^2 + a_2^2$$

must be divisible $\mod q$ by at least x^2 meaning that a_2 must be divisible by q. Since

$$a_2^2 = \pm 3^{2\rho}$$

is only divisible by 3, it is not true that any prime factor of $2n-1 = 3^r - 2$ will be a prime divisor of a_2^2 and so there cannot exist a second quadratic factor. It follows, that $a_1 = 0$.

Part 4

Since $a_1 = 0$, the quadratic factor of $G(x)$ (if it exists) is of the form $A(x) = x^2 \pm 3^\rho$. It is left to find for which values of ρ, $A(x)$ would be a factor of $G(x)$. In other words, for $h_1, h_2, \dots$ where $h_\nu = g_\nu$ if $A(x) = x^2 - 3^\rho$ and $h_\nu = -g_\nu$ if $A(x) = x^2 + 3^\rho$, for which values of ρ does

$$u_{2n+2} + h_1 u_{2n+2}\frac{3^\rho}{u_4} + h_2 u_{2n+2}\frac{3^{2\rho}}{u_6} + \dots + h_{n-1}u_{2n+2}\frac{3^{(n-1)\rho}}{u_{2n}} \pm 3^{n\rho} = 0 \tag{80}$$

hold? Since we can rearrange (80), we can equate $u_{2n+2} \pm 3^{n\rho}$ with all other terms of (80). It therefore follows that the greatest common divisor of

$$\frac{3^{\rho}u_{2n+2}}{u_4}, \frac{3^{2\rho}u_{2n+2}}{u_6} \ldots, \frac{3^{(n-1)\rho}u_{2n+2}}{u_{2n}} \tag{81}$$

must also divide $u_{2n+2} \pm 3^{n\rho}$. Clearly, the last number of (81) is equal to

$$(2n+1) \cdot 3^{(n-1)\rho} = 3^{(n-1)\rho+r},$$

since we are investigating the case $2n + 1 = 3^r$. The greatest common divisor is therefore of the form 3^{δ} where δ is to be found. The ν^{th} number in (81) is divisible by

$$3^{\nu\rho-\lambda_{\nu+1}(3)+\lambda_{n+1}(3)}.$$

Therefore, δ is the smallest of

$$\nu\rho - \lambda_{\nu+1}(3) + \lambda_{n+1}(3) \;\; \nu = 1, 2, \ldots, n-1.$$

From Lemma 4, it follows that for $\nu \geq 2$, $\rho \geq 1$

$$\begin{aligned} \lambda_{\nu+1}(3) &< \frac{2\nu+2}{3} \\ &= \frac{2\nu}{3} + \frac{2}{3} \\ &\leq \frac{2\nu}{3} + \frac{\nu}{3} \\ &= \nu. \end{aligned} \tag{82}$$

Since $\nu \geq 2 > 1$, it follows that

$$\rho\nu - \nu > \rho - 1.$$

Therefore,

$$\nu < \rho\nu - \rho + 1,$$

and it follows from (82) that

$$\lambda_{\nu+1}(3) < \rho\nu - \rho + 1, \tag{83}$$

for $\nu \geq 2$, whereas for $\nu = 1$

$$\rho\nu - \lambda_{\nu+1}(3) = \rho - \lambda_2(3) = \rho - 1.$$

Therefore, from (83) for $\nu \geq 2$, the value of $\rho\nu - \lambda_{\nu+1}(3)$ is always smaller than for when $\nu = 1$, so that,

$$\delta = \rho - 1 + \lambda_{n+1}.$$

On the other hand, it also follows from Lemma 4 that for $\rho \geq 1$,

$$\lambda_{n+1}(3) < \frac{2n+2}{3} < n \leq \rho n.$$

Therefore $x_{2n+2} \pm 3^{n\rho}$ is divisible by exactly $3^{\lambda_{n+1}}$ which can only be true if

$$\rho - 1 + \lambda_{n+1}(3) \leq \lambda_{n+1}(3).$$

It follows that $\rho = 1$ is the only possible value of ρ. In conclusion, if $2n = 3^r - 1 \geq 8$, then the polynomial $g(x)$ admits one irreducible quadratic factor of the form $x^2 \pm 3$ and no other quadratic factor. In this case $g(x) = (x^2 \pm 3)g_1(x)$ where $g_1(x)$ is irreducible over $\mathbb{Q}$.

Part 5

Next, we investigate the case $2n = 26$. It was stated that in this case, an irreducible polynomial $A(x)$ of degree 4 could be a factor of $G(x)$, we will however show that no such $A(x)$ exists.
Let q be a prime factor of $2n - 3 = 23$, then from (73) we know that

$$G(x) \mod q = \pm x^{26} + g_{12}(2n+1)x^{24} + g_{11}(2n+1)(2n-1)x^{22}.$$

Therefore, $G(x) \mod q$ is divisible by at least x^{22}. In particular, since $2n - 3 = 23$ is prime, $G(x) \mod 23$ is divisible by at least x^{22}. We suppose that a polynomial of degree 4

$$A(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$$

is an irreducible factor of $G(x)$. We now wish to prove by contradiction that $a_1 = a_3 = 0$. Suppose a_1 and a_3 are not both equal to zero, then $A(x)$ is a non-even factor of the even polynomial $G(x)$, meaning that $A(-x)$ is a second factor of $G(-x) = G(x)$. This means that

$$G(x) = A(x)A(-x)C(x) \tag{84}$$

where $C(x)$ is some polynomial

$$C(x) = \pm x^{18} + c_1x^{17} + \dots$$

and it follows that $C(x) \mod 23$ is divisible by at most x^{18} (in the case $c_1, c_2, \dots$ are all divisible by 23), so

$$A(x)A(-x) = x^8 + \dots + a_4^2$$

must be divisible $\mod 23$ by at least x^4 meaning that a_4^2 must be divisible by 23. (i.e. a_4 must be divisible by 23 and therefore a_4^2 must be divisible by 23^2) Since a_4^2 is the constant term of $A(x)A(-x)$, which is a factor of $G(x)$, a_4^2 must divide the

constant term of $G(x)$ where $2n = 26$, which is u_{28}. Since u_{28} is not divisible by 23^2, $A(x)A(-x)$ cannot be a factor of $G(x)$, in fact there cannot exist more than one polynomial factor of degree 4 of $G(x)$. It follows that $A(x)$ is an even polynomial and the only possible factor of $G(x)$. If $G(x)$ has a factor, it must therefore be of the form

$$A(x) = x^4 + a_2x^2 + a_4.$$

Part 6

By letting $x^2 = y$ we can represent $G(x)$ and $A(x)$ as

$$K(y) = u_{28} + g_1u_{28}\frac{y}{u_4} + \cdots + g_{12}u_{28}\frac{y^{12}}{u_{26}} \pm y^{13} \tag{85}$$

and

$$D(y) = y^2 + b_1y + b_2 \tag{86}$$

and we suppose that $D(y)$ is an irreducible quadratic factor of $K(y)$. Since

$$\frac{u_{28}}{u_{26}} = 27 \tag{87}$$

it follows that

$$\frac{u_{28}}{u_{2\nu+2}} \quad \nu = 1, 2, \ldots, 24 \tag{88}$$

are all divisible by 3 and therefore

$$K(y) \equiv \pm y^{13} \mod 3. \tag{89}$$

If $D(y)$ were a factor of $K(y)$, then b_1 and b_2 must therefore be divisible by 3.

Part 7

We will now show that b_2 is not divisible by 9.

Suppose that b_2 is divisible by 9. Then, if we let $y = 3z$,

$$D(3z) = 9E(z) = 9(z^2 + c_1z + c_2)$$

where c_1 and c_2 are integers.
It follows from

$$\lambda_2(3) = \lambda_3(3) = \lambda_4(3) = 1 \tag{90}$$

that

$$u_4, u_6, u_8$$

are divisible by 3 and therefore

$$\frac{(3z)^\nu}{u_{2\nu+2}} \tag{91}$$

is divisible by $3^{\nu-1}$ for $\nu = 1, 2, 3$.
It follows from

$$\lambda_5(3) = \lambda_6(3) = \lambda_7(3) = 3 \tag{92}$$

that (91) is divisible by $3^{\nu-3}$ for $\nu = 4, 5, 6$.
It follows from

$$\lambda_8(3) = \lambda_9(3) = \lambda_{10}(3) = 4 \tag{93}$$

that (91) is divisible by $3^{\nu-4}$ for $\nu = 7, 8, 9$.
It follows from

$$\lambda_{11}(3) = \lambda_{12}(3) = \lambda_{13}(3) = 5 \tag{94}$$

that (91) is divisible by $3^{\nu-5}$ for $\nu = 10, 11, 12$.
It follows from

$$\lambda_{14}(3) = 8 \tag{95}$$

that (91) is divisible by $3^{\nu-5}$ for $\nu = 13$.
It follows from (95) that u_{28} is divisible by 3^8 and therefore

$$K(3z) = 3^8 L(z)$$

and it follows from (90)-(95) that $L(z)$ is of the form

$$\begin{aligned} L(z) = l_0 + l_1 z + 3l_2 z^2 + 3^2 l_3 z^3 + 3l_4 z^4 + 3^2 l_5 z^5 + 3^3 l_6 z^6 \\ + 3^3 l_7 z^7 + 3^4 l_8 z^8 + 3^5 l_9 z^9 + 3^5 l_{10} z^{10} + 3^6 l_{11} z^{11} + 3^7 l_{12} z^{12} \pm 3^5 z^{13} \end{aligned} \tag{96}$$

where l_ν are integers for all ν and l_0 is not divisible by 3. Since $K(y)$ is a factor of $D(y)$, we know that $L(z)$ is a factor of $E(z)$, i.e. there exists $H(z)$ such that

$$L(z) = E(z)H(z).$$

We will now prove that $H(z)$ is an integer polynomial. Suppose that $H(z)$ is not an integer polynomial, where

$$H(z) = h_0 + h_1 z + \cdots + h_{11} z^{11}.$$

Then, at least one of h_ν is non-integer. Let ν_* be the greatest ν for which h_ν is non-integer, then

$$\begin{aligned} h_{\nu_*} z^{\nu_*}(E(z)) &= h_{\nu_*} z^{\nu_*}(z^2 + c_1 + c_2) \\ &= h_{\nu_*} z^{\nu_*+2} + h_{\nu_*} c_1 z^{\nu_*+1} + h_{\nu_*} c_2 z^{\nu_*} \\ h_{\nu_*+1} z^{\nu_*+1}(E(z)) &= h_{\nu_*+1} z^{\nu_*+1}(z^2 + c_1 + c_2) \\ &= h_{\nu_*+1} z^{\nu_*+3} + h_{\nu_*+1} c_1 z^{\nu_*+2} + h_{\nu_*+1} c_2 z^{\nu_*+1} \\ h_{\nu_*+2} z^{\nu_*+2}(E(z)) &= h_{\nu_*+2} z^{\nu_*+2}(z^2 + c_1 + c_2) \\ &= h_{\nu_*+2} z^{\nu_*+4} + h_{\nu_*+2} c_1 z^{\nu_*+3} + h_{\nu_*+2} c_2 z^{\nu_*+2} \end{aligned}$$

so that

$$\begin{aligned} L(z) &= E(z)H(z) \\ &= \cdots + (h_{\nu_*} + h_{\nu_*+1}c_1 + h_{\nu_*+2}c_2)z^{\nu_*+2} + \cdots . \end{aligned}$$

Since h_{ν_*+1} and h_{ν_*+2} are integers by choice of ν_*, the coefficient of z^{ν_*+2} in $L(z)$ must be non-integer, contradicting the fact that $L(z)$ is an integer polynomial. Therefore, no such non-integer coefficient h_{ν_*} can exist and $H(z)$ must be an integer polynomial. Since $L(z)$, $E(z)$ and $H(z)$ are all integer polynomials, it must be true that

$$L(z) \equiv E(z)H(z) \mod 3$$

but from (96) we know that $L(z) \mod 3$ is a polynomial of degree at most 1, whilst $E(z) \mod 3$ is a polynomial of degree 2 so we have reached a contradiction and b_2 is therefore divisible by 3 but not by 9.

Part 8

Let β be a root of $D(y) = 0$. Then, it follows that

$$\beta(\beta - b_1) = -b_2$$

and therefore β divides b_2 and, as we stated earlier 3 divides b_2. Note that β is an algebraic integer and $\mathbb{Q}(\beta)$ is an algebraic field extension of degree 2. From Ideal Property 2, it follows that $\langle\beta\rangle$ and $\langle 3\rangle$ are both divisible by $\langle b_2\rangle$. We therefore know, from Ideal Property 3, that there exists a prime ideal $\mathfrak{p}$ which divides $\langle\beta\rangle$ and $\langle 3\rangle$. Let the highest power of $\mathfrak{p}$ which divides $\langle\beta\rangle$ and $\langle 3\rangle$, be $\mathfrak{p}^r$ and $\mathfrak{p}^s$ respectively. Clearly, $r \geq 1$ and $s \geq 1$ but it also follows from Lemma 3 that $s \leq 2$. Since $\mathfrak{p}^r$ divides β exactly, then

$$\beta^2 \text{ is divisible by exactly } \mathfrak{p}^{2r}. \tag{97}$$

Since b_2 is divisible by 3 exactly and $\langle 3\rangle$ is divisible by $\mathfrak{p}^s$ exactly,

$$b_2 \text{ is divisible by exactly } \mathfrak{p}^s. \tag{98}$$

Finally, since b_1 is divisible by at least 3,

$$b_1\beta \text{ is divisible by at least } \mathfrak{p}^{r+s}. \tag{99}$$

It follows from (98) and (99) that $b_1\beta + b_2$ is divisible by exactly $\mathfrak{p}^s$. From $D(\beta) = 0$, it follows that β^2 must therefore be divisible by exactly $\mathfrak{p}^s$, from (97) it follows that $s = 2r$. Since

$$r \geq 1,\ 1 \leq s \leq 2 \tag{100}$$

it follows that

$$r = 1,\ s = 2. \tag{101}$$

Since $r = 1$, β^{13} is divisible by exactly $\mathfrak{p}^{13}$.
From (90), we know that u_4 is divisible by 3 and from (95), we know that u_{28} is divisible by 3^8, therefore

$$g_1 u_{28} \frac{\beta}{u_4} \tag{102}$$

is divisible by

$$\frac{3^8}{3}\beta$$

and it follows from (101) that (102) is divisible by $\mathfrak{p}^{15}$.

From (90), we know that u_6 is divisible by 3 and from (95), we know that u_{28} is divisible by 3^8, therefore

$$g_2 u_{28} \frac{\beta^2}{u_6} \tag{103}$$

is divisible by

$$\frac{3^8}{3}\beta^2$$

and it follows from (101) that (103) is divisible by $\mathfrak{p}^{16}$.

From (90), we know that u_8 is divisible by 3 and from (95), we know that u_{28} is divisible by 3^8, therefore

$$g_3 u_{28} \frac{\beta^3}{u_8} \tag{104}$$

is divisible by

$$\frac{3^8}{3}\beta^3$$

and it follows from (101) that (104) is divisible by $\mathfrak{p}^{17}$.

Similarly, from (92), we know that u_{10}, u_{12}, u_{14} are divisible by 3^3 and from (95), we know that u_{28} is divisible by 3^8, therefore

$$g_4 u_{28} \frac{\beta^4}{u_{10}}, \quad g_5 u_{28} \frac{\beta^5}{u_{12}}, \quad g_6 u_{28} \frac{\beta^6}{u_{14}},$$

are divisible by $\mathfrak{p}^{14}$, $\mathfrak{p}^{15}$ and $\mathfrak{p}^{16}$.

From (93),

$$g_7 u_{28}\frac{\beta^7}{u_{16}},\quad g_8 u_{28}\frac{\beta^8}{u_{18}},\quad g_9 u_{28}\frac{\beta^9}{u_{20}},$$

are divisible by $\mathfrak{p}^{15}$, $\mathfrak{p}^{16}$, $\mathfrak{p}^{17}$.

From (94),

$$g_{10} u_{28}\frac{\beta^{10}}{u_{22}},\quad g_{11} u_{28}\frac{\beta^{11}}{u_{24}},\quad g_{12} u_{28}\frac{\beta^{12}}{u_{26}}$$

are divisible by $\mathfrak{p}^{16}$, $\mathfrak{p}^{17}$, $\mathfrak{p}^{18}$.

Finally, we also know that u_{28} is divisible by $\mathfrak{p}^{16}$.

If $D(y)$ is a factor of $K(y)$, then

$$K(\beta) = u_{28} + g_1 u_{28}\frac{\beta}{u_4} + \cdots \pm \beta^{13} \tag{105}$$

must vanish. We have just shown that every term of $K(\beta)$ except β^{13} is divisible by at least $\mathfrak{p}^{14}$, while β^{13} is divisible by at most $\mathfrak{p}^{13}$, meaning that $K(\beta)$ cannot vanish and therefore $D(y)$ is not a factor of $K(y)$. It follows then that $D(x^2) = A(x)$ is not a factor of $K(x^2) = G(x)$ and $G(x)$ must be irreducible over $\mathbb{Z}$ in this case.

In conclusion, $g(x)$ is irreducible over $\mathbb{Q}$ in every case except for when $2n = 3^r - 1$, then $g(x)$ has an irreducible factor $x^2 \pm 3$. □

8.3 Proof of Corollary 2

Corollary 2 (Corollary of Theorems 2 and 3)**.**
The m^{th} Hermite Polynomial

$$H_m(x) = (-1)^m e^{\frac{x^2}{2}} \cdot \frac{d^m e^{-\frac{x^2}{2}}}{dx^m}$$

is irreducible over $\mathbb{Q}$ for even $m > 2$ and irreducible after division by x for odd m.

Proof of Corollary 2.
The Hermite polynomials can be expressed as

$$H_m(x) = \sum_{\mu=0}^{\left[\frac{m}{2}\right]} (-1)^\mu \binom{m}{2\mu} \cdot u_{2\nu} \cdot x^{m-2\mu}$$

From this, we can find an expression for the even Hermite polynomials

$$\begin{aligned} H_{2n}(x) &= \sum_{\mu=0}^{n}(-1)^{\mu}\binom{2n}{2\mu}u_{2\mu}\cdot x^{2n-2\mu} \\ &= \sum_{\mu=0}^{n}(-1)^{\mu}\cdot\frac{(2n)!}{(2\mu)!(2(n-\mu))!}\cdot\frac{(2\mu)!}{2^{\mu}\mu!}\cdot x^{2n-2\mu} \\ &= \sum_{\mu=0}^{n}(-1)^{\mu}\cdot\frac{(2n)!}{(2(n-\mu))!\cdot 2^{\mu}\mu!}\cdot x^{2n-2\mu} \end{aligned}$$

Let $\nu = n-\mu$, then

$$\begin{aligned} H_{2n}(x) &= \sum_{\nu=0}^{n}(-1)^{n+\nu}\cdot\frac{(2n)!}{(2\nu)!\cdot 2^{n-\nu}(n-\nu)!}\cdot x^{2\nu} \\ &= \sum_{\nu=0}^{n}(-1)^{n+\nu}\cdot\frac{2^{n}n!\cdot u_{2n}}{2^{\nu}\nu!\cdot u_{2\nu}\cdot 2^{n-\nu}(n-\nu)!}\cdot x^{2\nu} \\ &= \sum_{\nu=0}^{n}(-1)^{n+\nu}\cdot\frac{n!\cdot u_{2n}}{\nu!\cdot u_{2\nu}\cdot(n-\nu)!}\cdot x^{2\nu} \\ &= \sum_{\nu=0}^{n}(-1)^{n+\nu}\binom{n}{\nu}\cdot\frac{u_{2n}}{u_{2\nu}}\cdot x^{2\nu} \end{aligned} \tag{106}$$

Similarly, we can also find an expression for the odd Hermite polynomials:

$$H_{2n+1}(x) = \sum_{\nu=0}^{n}(-1)^{n+\nu}\binom{n}{\nu}\cdot\frac{u_{2n+2}}{u_{2\nu+2}}\cdot x^{2\nu+1} \tag{107}$$

It follows from (106), that

$$H_{2n}(x) = (-1)^{n}\cdot u_{2n}\cdot f(x)$$

where $f(x)$ is a polynomial of the form

$$f(x) = 1 + g_1\frac{x^2}{u_2} + g_2\frac{x^4}{u_4} + \cdots + g_{n-1}\frac{x^{2n-2}}{u_{2n-2}} \pm \frac{x^{2n}}{u_{2n}}.$$

It follows therefore, from Theorem 2 that $H_{2n}(x)$ are irreducible over $\mathbb{Q}$ for $n > 1$. Similarly, it follows from (107), that

$$H_{2n+1}(x) = (-1)^{n}\cdot u_{2n+2}\cdot x\cdot g(x)$$

where $g(x)$ is a polynomial of the form

$$g(x) = 1 + g_1\frac{x^2}{u_4} + g_2\frac{x^4}{u_6} + \cdots + g_{n-1}\frac{x^{2n-2}}{u_{2n}} \pm \frac{x^{2n}}{u_{2n+2}}.$$

It follows therefore, from Theorem 3 that

$$\frac{H_{2n+1}(x)}{x}$$

is irreducible over $\mathbb{Q}$ except for the case $2n+1 = 3^r \geq 9$, for which there could exist a factor of the form $x^2 \pm 3$. It is left to show that even in the case $2n+1 = 3^r \geq 9$, the odd Hermite polynomials $H_{2n+1}(x)$ cannot admit a factor of the form $x^2 \pm 3$. It follows trivially from the fact that Hermite polynomials only admit real roots, that x^2+3 cannot be a factor of $H_{2n+1}(x)$. In the case that $2n+1 = 9$, x^2-3 is not a factor as

$$\begin{aligned} H_9(\pm\sqrt{3}) &= (\pm\sqrt{3})^9 - 36(\pm\sqrt{3})^7 + 378(\pm\sqrt{3})^5 - 1260(\pm\sqrt{3})^3 + 945(\pm\sqrt{3}) \\ &= (\pm 81\sqrt{3}) - 36(\pm 27\sqrt{3}) + 378(\pm 9\sqrt{3}) - 1260(\pm 3\sqrt{3}) + 945(\pm\sqrt{3}) \\ &= \mp 324\sqrt{3} \\ &\neq 0. \end{aligned}$$

Suppose that $2n+1 = 3^r > 9$, then, as we saw in Section 4 (Example 3), $2n, 2n+1$ cannot be $\{2,3\}$-smooth, so there must exist a prime factor $p \geq 5$ of $2n$.
We can see from our expression for $H_{2n+1}(x)$

$$H_{2n+1}(x) = \sum_{\mu=0}^{n} (-1)^{\mu} \binom{2n+1}{2\mu} u_{2\mu} \cdot x^{2n-2\mu+1}$$

that the coefficient of $x^{2n+1-2\mu}$ is divisible by

$$\binom{2n+1}{2\mu} \cdot u_{2\mu}.$$

For $2\mu \geq p+1$, $u_{2\mu}$ will be divisible by p.
For $0 < 2\mu \leq p-1$,

$$\binom{2n+1}{2\mu} = \frac{(2n+1)\cdot(2n)\cdots(2n+1-2\mu)}{1\cdot 2\cdots 2\mu}$$

will be divisible by p (as p divides $2n$ which appears in the numerator but p does not appear in the denominator). Therefore, the coefficient of every term of $H_{2n+1}(x)$ except x^{2n+1} is divisible by $p \geq 5$ so that

$$H_{2n+1}(x) \equiv x^{2n+1} \mod p.$$

It follows that any factorisation of $H_{2n+1}(x)$ into two integer polynomials, results in those two factors both having constant terms divisible by $p \geq 5$. As a result, x^2-3 cannot be a factor of $H_{2n+1}(x)$. □

9 A Modern Look At The Distribution Of Prime Numbers

Having been introduced to the distribution of prime numbers in Section 2, I felt it was important to revisit this subject as there have been many advances in our understanding of this subject since 1929. In this section, I present some better approximations found after Schur wrote his papers. I also talk about how one can use Maple to investigate the distribution of prime numbers and I present a method for finding more intervals containing prime numbers, inspired by Schur's proof of Lemma 1.

9.1 New Approximations

New Approximation 1 (Rosser and Schoenfeld [11])**.**

$$\pi(x) < 1.25506\frac{x}{\log x}$$

for $x > 1$.

New Approximation 2 (Dusart [3])**.**

$$\vartheta(x) < x + 151.3\frac{x}{\log^4(x)}$$
$$\vartheta(x) > x - 151.3\frac{x}{\log^4(x)}$$

for $x \geq 2$.

New Approximation 3 (Dusart [3])**.**

$$\psi(x) < x + 59.18\frac{x}{\log^4(x)}$$
$$\psi(x) > x - 59.18\frac{x}{\log^4(x)}$$

for $x \geq 2$.

9.2 Using Maple

With the use of the computer programming software Maple, it is very easy to find exact values for all of the functions defined in Section 2.1 using the Number Theory package. Below, you can find the relevant code for each function:

For the prime counting function $\pi(x)$, simply use

```
pi(x);
```

For the prime gaps function Δp, first define

```
delta(i):=ithprime(i+1)-ithprime(i);
```

then in order to find Δp for some $p \in \mathbb{P}$, type

```
delta(pi(p));
```

For the function $L(x)$, having defined delta(i) as above, define a sequence

```
m:=seq(delta(i),i=1..pi(p));
```

for a chosen $p \in \mathbb{P}$. This will give all prime gaps up to p, then in order to find the maximum prime gap up to p, type

```
M:=max(m);
```

The value of $L(p)$ is just one less than M. If instead you wish to find $L(x)$ for some $x \in \mathbb{N}$, then simply find $L(p_1)$ and $L(p_2)$ where p_1 and p_2 are consecutive primes either side of x, they are easily found using

```
p1:=prevprime(x);
p2:=nextprime(x);
```

If $L(p_1) = L(p_2)$ then they are equal to $L(x)$, otherwise $L(x)$ is the larger of $L(p_1)$ and $x - p_1$.

For the first Chebyshev function $\vartheta(x)$ use

```
vartheta:=x->sum(ln(ithprime(i)),i=1..pi(x)):
```

For the second Chebyshev function $\psi(x)$, use

```
varpsi:=x->sum((floor(log[ithprime(i)](x)))*ln(ithprime(i)),i=1..pi(x)):
```

9.2.1 Using Maple to find Prime Gaps

In Section 2.2, we saw some approximations for the prime gaps function Δp and the function $L(x)$ giving the length of the longest sequence of consecutive numbers, or equivalently, if we define $M(x)$ to be the maximum prime gap up to x, then

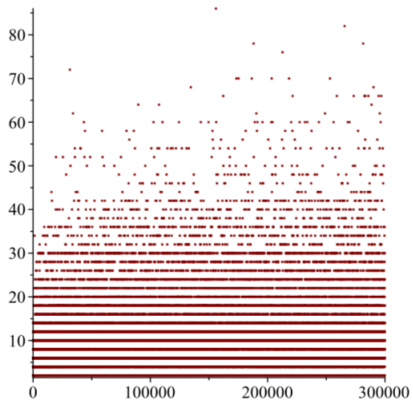

Figure 1: Graph showing Δp for all prime numbers $p \leq 300000$

$L(x) = M(x) - 1$. Using Maple, I plotted all prime gaps for $x \leq 300000$.

In Approximation 4, we saw that Schur approximated that $\Delta p < 1000$ for $p < 162754$, this is equivalent to saying that the maximum prime gap for $p < 16275$ is less than 1000. Using Maple, I find that the actual maximum prime gap for $p < 16275$ is 44. Similarly, I find that

$$M(4000) = 34$$
$$M(400) = 14$$

Note that, $M(400) = 14$ agrees with Approximation 4.

In Approximation 5, we saw that Schur gave upper bounds for $L(x)$. Using Maple I can find the exact value of $L(x)$, they are as follows

$$L(300000) = 85$$
$$L(100000) = 71$$
$$L(50000) = 71$$
$$L(5000) = 33$$

I conclude this section by presenting some graphs that compare approximations of the prime counting function and Chebyshev functions with their actual values up to 1000.

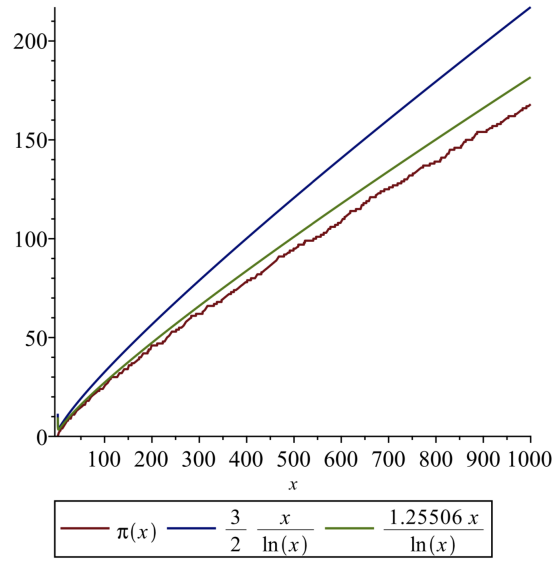

Figure 2: Graph comparing two different upper bounds for $\pi(x)$ with the actual values of $\pi(x)$.

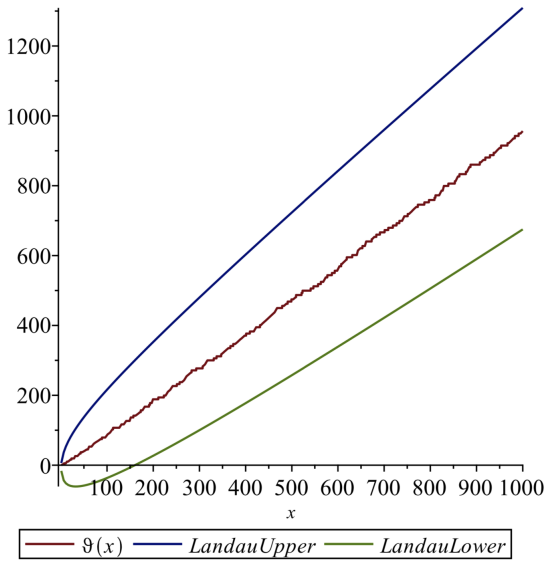

Figure 3: Graph comparing Landau's upper and lower bounds for $\vartheta(x)$ with the actual values of $\vartheta(x)$.

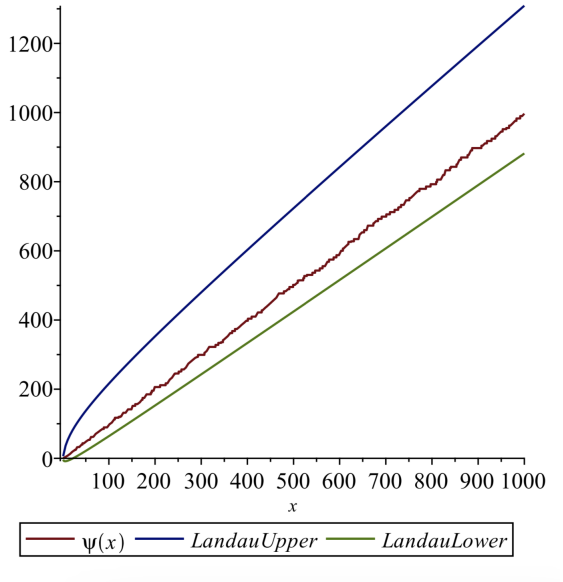

Figure 4: Graph comparing Landau's upper and lower bounds for $\psi(x)$ with the actual values of $\psi(x)$.

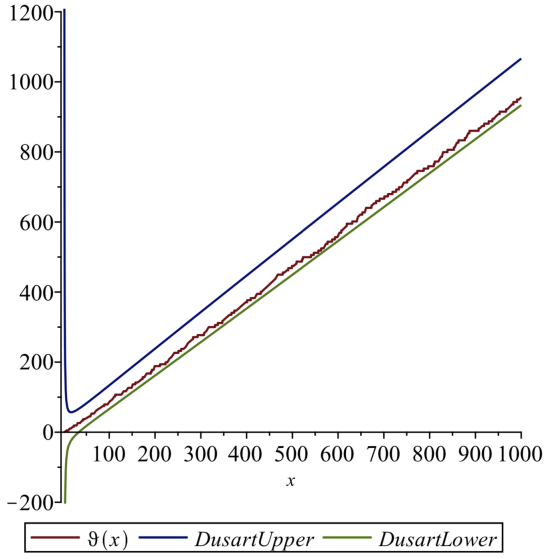

Figure 5: Graph comparing Dusart's upper and lower bounds for $\vartheta(x)$ with the actual values of $\vartheta(x)$.

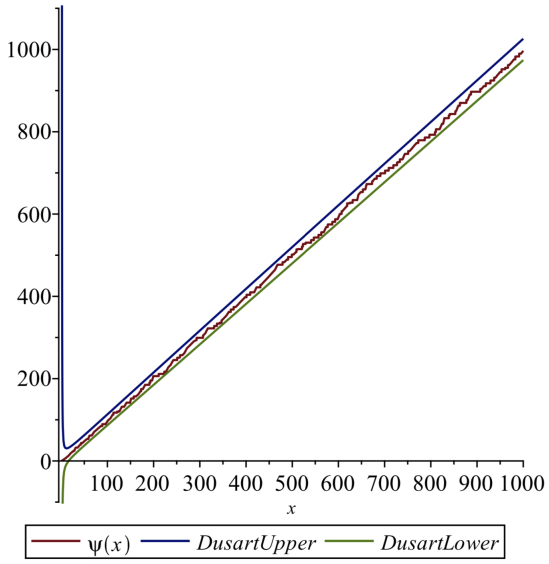

Figure 6: Graph comparing Dusart's upper and lower bounds for $\psi(x)$ with the actual values of $\psi(x)$.

9.3 Revisiting the Problem of Finding Intervals Containing Primes

Schur's proof of Lemma 1 involved using Approximation 1 to show that $\vartheta(\frac{5x}{4})-\vartheta(x) > 0$ for $x > e^{12}$ and then verifying that there exists a prime number in every interval $x < p \leq \frac{5}{4}x$ for $29 \leq x \leq e^{12}$.
In 1952 it was proven (see [9]) that there always exists a prime number in the interval $x < p \leq \frac{6x}{5}$ for $x \geq 25$. Nagura's proof used upper and lower bounds of $\psi(x)$ to show that $\vartheta(\frac{6x}{5})-\vartheta(x) > 0$ for $x \geq 2103$ and then verified that there exists a prime number in every interval $x < p \leq \frac{6}{5}$ for $25 \leq x < 2103$.
This led me to thinking about other intervals of the form

$$x < p \leq \frac{n+1}{n}x. \tag{108}$$

It follows from the Prime Number Theorem that for all n, there must exist an X such that for all $x > X$, the interval (108) contains a prime number. Using Dusart's approximations for $\vartheta(x)$, I have found a method for finding such an X.

Theorem 4.
For some $n \geq 1$, there exists a prime number in the interval

$$x < p \leq \frac{n+1}{n} \cdot x$$

for $x \geq X$, where

$$X = e^{\sqrt[4]{151.3 \cdot (2n+1)}}.$$

Proof of Theorem 4.
Using the new approximations for the first Chebyshev function, found by Dusart in [3], we can find a lower bound for $\vartheta(\frac{n+1}{n}x) - \vartheta(x)$.

$$\vartheta\left(\frac{n+1}{n}x\right) - \vartheta(x) > \frac{x}{n} - \frac{n+1}{n} \cdot \frac{151.3 \cdot x}{\log^4(\frac{n+1}{n} \cdot x)} - \frac{151.3 \cdot x}{\log^4(x)}$$

for $x \geq 2$.
We also know that

$$\frac{1}{\log^4(\frac{n+1}{n} \cdot x)} < \frac{1}{\log^4(x)} \tag{109}$$

for $x \geq 2$.
Therefore,

$$\begin{aligned}\vartheta\left(\frac{n+1}{n}x\right) - \vartheta(x) &> \frac{x}{n} - \frac{n+1}{n} \cdot \frac{151.3 \cdot x}{\log^4(x)} - \frac{151.3 \cdot x}{\log^4(x)} \\ &= \frac{x}{n} - \frac{(2n+1) \cdot 151.3 \cdot x}{n \log^4(x)} \\ &= \frac{x}{n}\left(1 - \frac{151.3 \cdot (2n+1)}{\log^4(x)}\right)\end{aligned}$$

It follows that for some $n \geq 1$, if

$$\log^4(x) \geq 151.3 \cdot (2n+1),$$

then $\vartheta(\frac{n+1}{n}x) - \vartheta(x) > 0$. □

From Theorem 4, it follows that for:

$n = 6$ there exists a prime number p in the interval (108) for $x \geq e^{\sqrt[4]{1966.9}} = 780.207\ldots$
$n = 7$ there exists a prime number p in the interval (108) for $x \geq e^{\sqrt[4]{2269.5}} = 994.381\ldots$
$n = 8$ there exists a prime number p in the interval (108) for $x \geq e^{\sqrt[4]{2572.1}} = 1238.316\ldots$
$n = 9$ there exists a prime number p in the interval (108) for $x \geq e^{\sqrt[4]{2874.7}} = 1513.697\ldots$

Using Maple, I can verify that there exists a prime in every interval 108 for small x.
It therefore follows that there exists a prime number p in the following intervals:

$$x < p \leq \frac{7}{6}x \qquad \forall x \geq 32$$

$$x < p \leq \frac{8}{7}x \qquad \forall x \geq 33$$

$$x < p \leq \frac{9}{8}x \qquad \forall x \geq 48$$

$$x < p \leq \frac{10}{9}x \qquad \forall x \geq 115$$

10 References

[1] Keith Conrad, *Pell's Equation II*, https://kconrad.math.uconn.edu/blurb/, Accessed 2020.

[2] ———, *Stirling's Formula*, https://kconrad.math.uconn.edu/blurb/, Accessed 2020.

[3] Pierre Dusart, *Explicit Estimates of Some Functions Over Primes*, The Ramanujan Journal **45** (2018), 227–251.

[4] Michael Jacobson, Jr and Hugh Williams, *Solving the Pell Equation*, Springer-Verlag New York, 2009.

[5] Edmund Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, vol. 1, Leipzig B.G. Teubner, 1909.

[6] Derrick Henry Lehmer, *On the Multiple Solutions of the Pell Equation*, Annals of Mathematics **30** (1928), 66–72.

[7] ———, *On a problem of Størmer*, Illinois J. Math. **8** (1964), 57–79.

[8] Keith Matthews, *The Diophantine Equation* $x^2 - Dy^2 = N, D > 0$, Expositiones Mathematicae **18** (2000), 323–332.

[9] Jitsuro Nagura, *On The Interval Containing At Least One Prime Number*, Proc. Japan Acad. **28** (1952), 177–181.

[10] Oskar Perron, *Über eine Anwendung der Idealtheorie auf die Frage nach der Irreduzibilität algebraischer Gleichungen*, Mathematische Annalen **60** (1905), 448–458.

[11] J. Barkley Rosser and Lowell Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.

[12] Issai Schur, *Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen I*, Sitzungsberichte der Preussischen Akademie der Wissenschaft (1929), 125–136.

[13] ———, *Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen II*, Sitzungsberichte der Preussischen Akademie der Wissenschaft (1929), 370–391.

[14] Carl Størmer, *Quelques théorèmes sur l'équation de Pell* $x^2 - dy^2 = \pm 1$ *et leurs applications*, Christiania Videnskabsselskabs Skrifter (1897), 3–48.

[15] Gabor Szegö, *Orthogonal Polynomials*, American Mathematical Society, 1959.