Brocard's problem and variations

A thesis

submitted in partial fulfilment

of the requirements for the Degree

of

Master of Science

at the

University of Waikato

by

Yi Liu

THE UNIVERSITY OF
WAIKATO
Te Whare Wānanga o Waikato

University of Waikato

2013

Abstract

This thesis examines the work which has been done on Brocard's problem which is to study solutions to

$$n! + 1 = x^2,$$

and related problems of the form

$$n! = f(x) \text{ or } n! = f(x, y),$$

where f is a polynomial with integer coefficients. I also consider problems of the form

$$n! = f(x),$$

where there are apparently no solutions.

Acknowledgements

I would like to thank Professor Kevin Broughan, who has the attitude and the substance of a genius. Without his guidance and persistent help this thesis would not have been possible. During the whole year, I received plenty of academic advice from him, which made some proofs in my thesis more complete and better. Professor Kevin has also helped and shown me how to use Mathematica 8.0 in spite of his busy schedule. He did not only had a heavy load of responsibility in my thesis but also concern in my life. Specifically, I was given the information about the Zulauf scholarship initially from him. Also Professor Kevin has helped me to polish many of the English phrases in the thesis. My special thanks also to Associate Professor Stephen Joe, who assisted me in using LaTeX. He could always solve the problems when LaTeX was in error. If anyone is looking for help with LaTeX, I highly recommend him. I also thank Dr Daniel Delbourgo for giving me helpful suggestions to improve my thesis. I would like to express the deepest appreciation to the Department of Mathematics of Waikato University for providing a congenial working environment for me. Not only all professors, also other graduate students and dear Glenys Williams from Mathematics Reception, made me feel welcome all the time. Finally, I take this opportunity to acknowledge my parents and my partner and I appreciate the support that they gave to me, both in the substance and in the spirit.

Contents

Chapter 1

Introduction

1.1 Overview

In this chapter, I give an overview of the thesis, all notations I applied including the symbols and the functions, as well as preliminary results in my thesis.

1.2 Thesis overview

This thesis is a study of Brocard's problem, namely to show that the equation

$$n! + 1 = x^2$$

has at most a finite number of solutions in integers (n, x). These are

$$\begin{aligned} 4! + 1 &= 5^2, \\ 5! + 1 &= 11^2, \\ 7! + 1 &= 71^2. \end{aligned}$$

This problem was posed by Henri Brocard in a pair of articles in 1876 [4] and 1885 [5]. I have studied most of the related diophantine equations and how they might contribute ideas to proving Brocard's problem. One of my purposes is to make these methods clearer and more accessible to readers. I hope to create a reasonably complete reference for people who will work on this problem.

While working on this material during 2012, I learned, in late September, of a proposed proof of the ABC conjecture. I am not able to check this proof, since it is over 500 pages long, and contains many ideas which I would need to understand to check it is correct. However, if the proof is correct, then, through the work of Luca described in Chapter 4, EACH of the equations $n! = f(x)$, for $f(x) \in \mathbb{Z}[X]$, has at most a finite number of solutions.

According to different angles to explore this problem, my thesis can be divided into 6 parts. Here is a brief description of each chapter.

Chapter 2 discusses the equations where $n!$ is expressed as a linear form, and gives a necessary condition on $a,\ b$ such that $n! = ax + by$ has a solution.

This chapter also considers the result of Dabrowski who treated the equation $n! = x^2 - A$, for A not a square, and proved the finiteness of solutions of it. I give many more details which do not appear in Dabrowski's work.

Chapter 3 begins with results from De Koninck and Luca who proved, following Erdös, that the equation $n! = x^p + y^p$ has at most a finite number of solutions, where p is an odd prime.

This chapter also introduces the method of Erdös and Obláth, who worked on the equation $n! = x^p \pm y^p$. The method involves the estimation of special subsets of factors of $n!$.

This chapter also tries to discover where there are a finite number of solutions for other related diophantine equations. These are $n! = x^2 - y^2$, $n! = x^2 + y^2 + z^2$ and $n! = x^2 + y^2$. The method used is to discuss the particular known patterns of the right side of these equations.

This chapter also gives two explicit examples where I show $n! = x^8 - y^8$ and $n! = x^3 - 1$ both have no solutions respectively.

Chapter 4 begins with the statement of Mason's Theorem, which is the source of the ABC conjecture.

Next, this chapter introduces the ABC conjecture and Szpiro's conjecture, and shows how to use the ABC conjecture to deal with Fermat's Last Theorem and Catalan's conjecture which is now named as Mihailescu's theorem. Also, I introduce another formulation of the ABC conjecture and some good abc examples,

which involve the function called *quality*, $q(a, b, c)$, of the triple (a, b, c).

One of the main purposes of this chapter is to show how Brocard's problem is proved by Overholt using Szpiro's conjecture. Another purpose is to show how to apply the ABC conjecture and solve the more general diophantine equation $n! = f(x)$, as originally done by Luca, which form includes Brocard's problem.

Chapter 5 is devoted to the result of Pollack and Shapiro. It takes a different route from Erdös and Obláth for proving that the equation $n! = x^4 - 1$ has no integer solutions. There I need to analyze the equation in two cases, $n \geq 27182.8$ and $n < 27182.8$, respectively by different methods. The latter case will be a little easier and treated by computer, while the case that $n \geq 27182.2$ will be the main focus.

Chapter 6 covers the results from Berend who studied the equation $P(x) = H_n$ and proved that for some various classes of polynomials these equations have only finitely many solutions. Here (H_n) represents several highly divisible sequences including the case $H_n = n!$. By the study of part of theorems in his paper, I give some examples and show for what cases the introduced theorems can work or not. The classes of polynomials I am going to pose are divisible by quadratic polynomials with the form of $(x^2 - A)$ or have so-called overloaded factors. For the latter case, I introduce the ideas of applying the density of primes and show an useful theorem.

Finally, in this chapter I establish some examples. I give a new method to show that $P(x) = n!$ has no solutions or has finitely many solutions, where $P(x) = x(x+3)$ and $P(x) = x(x+1)(x+2)$. Even though this method works for particular values of n, I suspect it can be made to work for all n.

In Chapter 6, I give some concluding remarks regarding how Brocard's problem might or might not be eventually solved.

Here is a list of what I believe is NEW work in this thesis. I do not claim all of it is really significant, but some of it might be. I do not include improvements to existing proofs.

This thesis introduces a smaller lower bound for n such that $n! = ax + by$ has a solution, compared with the other lower bound, i.e. the greatest common divisor

of a and b. There Section 2.2 shows a clear and brief proof for the smaller lower bound. In addition, Lemma 2.3 makes Dabrowski's work explicit, and therefore is an improvement.

Moreover, an infinite set of factorials which cannot be expressed as the sum of three integer squares is included in this thesis, particularly those $m!$ where $m = 3 \cdot 2^n$ with $n \geq 2$.

Also, in Chapter 6, I analyze two polynomials, $P(x) = x(x+3)$ and $P(x) = x(x+1)(x+2)$ as examples, and I give a new method to show that $P(x) = n!$ has no solutions or has finitely many solutions. For the first case, the method I give works for particular values of n, however, I suspect it can be made to work for all n. As for the second case, the one important observation is that I give the pattern of the power of prime factors in $x(x+1)(x+2)$ using Mathematica, which I think is quite useful information for me or people who work on this polynomial.

1.3 Notation

This is a list of symbols used in my thesis.

$\mathbb{N}$	The set of positive integers
$\mathbb{Z}[X]$	The set of polynomials in X with coefficients in the ring of integers
$\sum$	Summation
$\sum_{d\|n}$	Sum over divisors function
$\prod$	Product
$n!$	Factorial
$a \mid b$	Divides
$a \nmid b$	Does not divide
$(a_1, a_2, \ldots, a_n)$	Greatest common divisor (of n integers)
$\max(x, y)$	Maximum
$a \equiv b \bmod m$	Congruent
$a \not\equiv b \bmod m$	Incongruent
$(a \mid n)$	Jacobi symbol
$\binom{a}{b}$	Binomial coefficient
O	Big O notation
o	Little o notation
B	Mertens constant
$\square$	Any number which is a square
$f(x) \ll g(x)$	The growth of f is asymptotically bounded by g
$\lfloor x \rfloor$	The largest integer smaller or equal to x
$\{x\}$	The fractional part of x
$\lceil x \rceil$	The smallest integer greater or equal to x
$sf(A)$	The square-free part of A

$p^a \parallel b$	Exact divisibility
$p_{a,b}$	The smallest prime congruent to a modulo b
$n(q)$	The least positive quadratic nonresidue of q
χ	One of Dirichlet characters which are certain arithmetic functions

Here is a list of functions used in my thesis.

$\nu_p(n)$	The exact power of p dividing n
$\alpha_p(n) = \alpha_p = \sum_{j \geq 1} \left\lfloor \frac{n}{p^j} \right\rfloor$	The exact power of p dividing $n!$
$\pi(n) = \sum_{p \leq x} 1$	The number of prime numbers less than x
$\pi(n; a, b)$	The number of prime numbers $p \leq n$ with $p \equiv a \bmod b$
$\sum_{p \leq x} \frac{1}{p} = \log\log x + B + O\left(\frac{1}{\log x}\right)$	Mertens formula
$\phi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$	Euler's totient or phi function
$T(n, a, b) = \prod_{q \equiv b \bmod a} q^{\alpha_q(n)}$	A factor of $n!$ produced by the primes with $q \equiv a \bmod b$
$rad(f)$	The polynomial of minimum degree
$deg(rad(f))$	The number of distinct roots of f
$R(n) = \prod_{p \mid n} p$	The largest square-free divisor of n
$\psi(x) = \sum_{p^\alpha \leq x} \log p = \sum_{m \leq x} \Lambda(m)$	Chebshev function
$\mu(n)$	Mobius function
$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$	Dirichlet L-series
$q(a, b, c) = \frac{\log(c)}{\log(R(abc))}$	The quality of the triple (a, b, c)

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for some primes } p \text{ and integers } k \geq 1 \\ 0 & \text{otherwise} \end{cases}$$

1.4 Preliminary results

Lemma 1.1 (Linnik's theorem) *[22][23] Let $a + nb$, $n \in \mathbb{N}$ be an arithmetic progression with $(a, b) = 1$. Then the smallest prime p in this progression satisfies $p < b^L$ where $L = 5.5$ is Linnik's constant.*

Theorem 1.2 (Dirichlet's prime number theorem) *[9] If $a, b > 0$ are integers with $(a, b) = 1$ then there are an infinite number of primes $p = a + nb$ for some $n \in \mathbb{N}$, i.e. an infinite number of primes in the arithmetic progression generated by a and b.*

Theorem 1.3 (Chinese remainder theorem) *[18] If $m_1, \ldots, m_n$ are positive integers which are pairwise coprime, then for every set of residues $r_1, \ldots r_n$ there is an integer x with $0 \leq x < m_1 \cdots m_n$ and $x \equiv r_i \bmod m_i$ for all i with $1 \leq i \leq n$.*

Theorem 1.4 (Brun-Titchmarsh Theorem) *[19] The BrunTitchmarsh theorem gives an upper bound on the distribution of prime numbers in arithmetic progression. It states that, if $\pi(x; a, b)$ counts the number of primes p congruent to a modulo b with $p \leq x$, then*

$$|\{p \leq x : p \equiv a \bmod b\}| = \pi(x; a, b) \leq \frac{2x}{\phi(b) \log(x/b)},$$

for all $b < x$.

Theorem 1.5 (Abel's identity) *[1] For any arithmetical function $a(n)$ let*

$$A(x) = \sum_{n \leq x} a(n),$$

where $A(x) = 0$ if $x < 1$. Assume f has a continuous derivative on the interval $[y, x]$, where $0 < y < x$. Then we have

$$\sum_{y < n \leq x} a(n) f(n) = A(x) f(x) - A(y) f(y) - \int_y^x A(t) f'(t) dt.$$

Lemma 1.6 *[19] For fixed $b > 0$*

$$\sum_{\substack{p \le x \\ p \equiv a \bmod b}} \frac{\log p}{p} = \frac{\log x}{\phi(b)} + O_b(1),$$

where $O_b(1) = C \cdot g(b)$, and C is a constant, $g(b)$ represents some functions of b.

Proposition 1.7 *$R(n)$ is multiplicative and $R(n) \cdot R(m) = R(nm) \cdot R((n,m))$, where the radical $R(a)$ is the largest square-free divisor of a. i.e. $R(a) := \prod_{p|a} p$.*

Theorem 1.8 (Möbius inversion formula) *[1] If α is completely multiplicative we have*

$$G(x) = \sum_{n \le x} \alpha(n) F\left(\frac{x}{n}\right),$$

if and only if

$$F(x) = \sum_{n \le x} \mu(n)\alpha(n) G\left(\frac{x}{n}\right).$$

Theorem 1.9 (Partial summation) *[27] Let $f(n)$ and $g(n)$ be arithmetic functions. Consider the sum function*

$$F(x) = \sum_{n \le x} f(n).$$

Let a and b be nonnegative integers with $a < b$. Then

$$\sum_{n=a+1}^{b} f(n)g(n) = F(b)g(b) - F(a)g(a+1) - \sum_{n=a+1}^{b-1} F(n)(g(n+1) - g(n)).$$

In particular, if $x \ge 2$ and $g(t)$ is continuously differentiable on $[1, x]$, then

$$\sum_{n \le x} f(n)g(n) = F(x)g(x) - \int_1^x F(t)g'(t)dt.$$

ABC Conjecture [28][25] $\forall \varepsilon > 0$, there exists a constant $K_\varepsilon > 0$ that depending only on ε, such that if a, b, c are relatively prime and non-zero integers with $a + b = c$, then

$$max(|a|, |b|, |c|) \le K_\varepsilon R(abc)^{1+\varepsilon}.$$

Szpiro's Conjecture [33][34] There exists a constant $s > 0$ such that if a, b, c are relatively prime and non-zero integers with $a + b = c$, then the inequality

$$|abc| \leq R(abc)^s$$

holds.

Chapter 2

An elaboration of Dabrowski's work

2.1 Overview

In this chapter, I will first give a proof that includes a sufficient condition for the equation $n! = ax + by$ to have a solution. Next I focus on Dabrowski's work that shows the equation $n! = x^2 - A$ has at most a finite number of solutions, where A is not a square. There is a simple proof given in [8]. I will give a complete, much more explicit proof in Section 2.3. In Chapter 6, I explore values of A numerically and isolate some candidates where there are, apparently, no solutions.

2.2 Linear forms

Let a, b be integers and consider $n! = ax + by$. If this has a solution then we need $m := (a, b) \mid n!$ and this will certainly be true if $n \geq m$, so we get an infinite number of solutions. But given a positive integer m, can we get a smaller lower bound for n, so $m \mid n!$? Yes.

Proposition 2.1 *If $m = \prod_{i=1}^{I} p_i^{\beta_i}$, then for all $n \geq \max\{p_i\beta_i : 1 \leq i \leq I\}$ the equation $n! = ax + by$ has a solution.*

Proof. As is well known, the exact power of p_i dividing $n!$ is given by

$$\alpha_{p_i} = \sum_{j \geq 1} \left\lfloor \frac{n}{p_i^j} \right\rfloor = \left\lfloor \frac{n}{p_i} \right\rfloor + \left\lfloor \frac{n}{p_i^2} \right\rfloor + \left\lfloor \frac{n}{p_i^3} \right\rfloor + \dots .$$

Let $m = \prod_{i=1}^{I} p_i^{\beta_i}$ be written as its prime factorization. Since we are given $\max\{p_i\beta_i : 1 \leq i \leq I\} \leq n$, for a fixed i we have

$$p_i\beta_i \leq n \Rightarrow \beta_i \leq \frac{n}{p_i}.$$

But β_i is an integer, so

$$\beta_i \leq \left\lfloor \frac{n}{p_i} \right\rfloor \leq \sum_{j \geq 1} \left\lfloor \frac{n}{p_i^j} \right\rfloor = \alpha_{p_i}.$$

So $\beta_i \leq \alpha_{p_i}$, and then $p_i^{\beta_i} \leq p_i^{\alpha_{p_i}}$, for $1 \leq i \leq l$.
Therefore, $m = \prod_{i=1}^{I} p_i^{\beta_i} \mid \prod_{i=1}^{I} p_i^{\alpha_{p_i}} \mid n!$, and the equation $n! = ax + by$ has a solution. This completes the proof. □

Even though it is a new result, and easy to prove, it is hard to see how it could be improved.

2.3 Dabrowski's work

Consider the equation $n! = x^2 - A$. The nice aspect to the result of Dabrowski is that when A is not a square, there are, for given A, at most a finite number of solutions. Here I give his proof and find an explicit upper bound for the number of solutions. To compute the upper bound, I will show that there exists a prime p, such that $(A \mid p) = -1$, which implies $n < p$, i.e. there is an upper bound for n.

The following Lemma 2.2 is an old result of Vinogradov [35]. There have been a number of more recent improvements and extensions. For any odd prime p let $n(p)$ be the least positive quadratic nonresidue of p. Then $n(p) > 1$ and must be a prime.

Lemma 2.2 *[35] For all odd primes p we have $n(p) < p^{\frac{1}{2\sqrt{e}}} \log^2 p$.*

Table 2.1 shows odd primes with $p \leq 100$, explicit values for $n(p)$ and the numerical upper bound of $n(p)$, $p^{\frac{1}{2\sqrt{e}}} \log^2 p$ given in Lemma 2.2.

p	$n(p)$	$p^{\frac{1}{2\sqrt{e}}} \log^2 p$	p	$n(p)$	$p^{\frac{1}{2\sqrt{e}}} \log^2 p$
3	2	1.7	43	2	44.
5	2	4.2	47	5	48.
7	3	6.8	53	2	53.
11	2	12.	59	2	57.
13	2	14.	61	2	59.
17	3	19.	67	2	63.
19	2	21.	71	7	66.
23	5	25.	73	5	68.
29	2	31.	79	3	72.
31	3	33.	83	2	75.
37	2	39.	89	3	79.
41	3	43.	97	5	84.

Table 2.1: Odd primes p with $p \leq 100$ and computed values of $n(p)$.

There are a few very ancient references for the Chinese Remainder Theorem. As a chinese person, let me introduce one of famous stories about this theorem, which is called "Han Xin selects his troops", and let us see how a military general applied it in ancient times.

During the Chu-Han contention, there were many battles between the Chu Dynasty and the Han Dynasty. Han Xin (died 196 BC) was a military general in the Han Dynasty. One day he was in a hurry for selecting his troops and counting the accurate number. Then he assembled his army of approximately 1000 people and asked every three of them to queue in a line, then there were two more soldiers remaining; then every five in a line, three more remaining while every seven in a line, two more remaining. Immediately, Han Xin declared to and encouraged the army that he had 1073 soldiers, and it was strong enough to fight.

Now let me share with you how he worked this out. Since 23 is the least positive integer number which satisfies the following system of congruences.

$$\begin{aligned} x &\equiv 2 \bmod 3, \\ x &\equiv 3 \bmod 5, \\ x &\equiv 2 \bmod 7. \end{aligned}$$

Also the least common multiple is $3 \cdot 5 \cdot 7 = 105$, and then the only thing we need to do is to find the numbers between 1000 and 1500 satisfying $23 + 105n$, where n is natural number. At last, we get 1073, 1283 and 1493.

The following lemma enables the result of Dabrowski's work to be made explicit. I believe this is new.

Lemma 2.3 *Let $N > 1$ be a natural number, which is not a square. Then the least odd prime p which satisfies $(N \mid p) = -1$ is less than $f(N) := (4N)^L$.*

Proof. We can assume, without loss of generality, that N is square-free. Since if $N = ab^2$ with a square-free, provided p is an odd prime and $p \nmid N$, then $(N \mid p) = (ab^2 \mid p) = (a \mid p)(b \mid p)^2 = (a \mid p)$. Now let N be square-free.
If $N = 2$, let $p = 3$. Then $(N \mid p) = (2 \mid 3) = (-1)^{\frac{3^2-1}{8}} = -1$ and $3 < f(2) = 16^{5.5}$.
If $N = p_1 p_2 \cdots p_l$ is odd, consider the congruences

$$\begin{aligned} x &\equiv 1 \bmod p_i \ 1 \le i \le l-1 \\ x &\equiv 1 \bmod 4. \end{aligned}$$

By Theorem 1.3, there is a solution x with $0 \le x < 4p_1 p_2 \cdots p_{l-1} \le 4N \le (4N)^{5.5}$. Since

$$x \equiv 1 \bmod 4p_l p_2 \cdots p_{l-1}$$

and

$$(x, 4p_1 p_2 \cdots p_{l-1}) = (1, 4p_1 p_2 \cdots p_{l-1}) = 1,$$

by Theorem 1.1, we can find a prime value p for x with $p \equiv x < (4N)^{5.5}$. By Quadratic Reciprocity, for each i with $1 \le i \le l-1$, we have

$$\begin{aligned} (p_i \mid p) &= (p \mid p_i)(-1)^{\frac{(p_i-1)(p-1)}{4}} \\ &= (p \mid p_i) \ \text{ as } p \equiv x \equiv 1 \bmod 4 \text{ and } p_i \text{ is an odd prime} \\ &= (1 \mid p_i) = 1 \ \text{ as } p \equiv x \equiv 1 \bmod p_i. \end{aligned}$$

By Lemma 2.2 there exists a positive integer $n(p_l) < p_l$ such that $(n(p_l) \mid p_l) = -1$.

If the odd prime p satisfies $p \equiv n(p_l) \bmod p_l$, we get

$$\begin{aligned}(p_l \mid p) = (p \mid p_l)(-1)^{\frac{(p_l-1)(p-1)}{4}} &= (p \mid p_l) \ \text{ as } p \equiv x \equiv 1 \bmod 4 \\ &= (n(p_l) \mid p_l) \\ &= -1.\end{aligned}$$

Thus, with the solution of

$$\begin{aligned}p &\equiv 1 \bmod p_i \ 1 \le i \le l-1, \\ p &\equiv 1 \bmod 4, \\ p &\equiv n(p_l) \bmod p_l,\end{aligned}$$

the least odd prime p satisfies $(N \mid p) = (p_1 \mid p) \cdots (p_{l-1} \mid p)(p_l \mid p) = 1 \cdot (-1) = -1$ and is less than $f(N) = (4N)^L$.

If N is even, write $N = 2p_1p_2 \cdots p_l$ and we can assume $l \ge 1$.

If $p_i \equiv 1 \bmod 4$ let $i \in I_1$. If $p_i \equiv 3 \bmod 4$ let $i \in I_3$. So $I_1 \cup I_3 = \{1, 2, \ldots, l\}$.

Now let us consider solutions to the joint congruences

$$\begin{aligned}x &\equiv 1 \bmod p_i, \\ x &\equiv n(p_i) \bmod p_i, \\ x &\equiv 3 \bmod 8.\end{aligned}$$

By Theorem 1.3, we have

$$\begin{aligned}(N \mid p) &= (2p_1p_2 \cdots p_l \mid p) \\ &= (2 \mid p) \cdot \prod_{i \in I_1} (p_i \mid p) \cdot \prod_{i \in I_3} (p_i \mid p) \\ &= (-1)^{\frac{p^2-1}{8}} \cdot \prod_{i \in I_1} (p \mid p_i)(-1)^{\frac{(p-1)(p_i-1)}{4}} \cdot \prod_{i \in I_3} (p \mid p_i)(-1)^{\frac{(p-1)(p_i-1)}{4}} \\ &= (-1) \cdot \prod_{i \in I_1} (1 \mid p_i) \cdot (-1)^{\frac{(2+8q_1)(4q_2)}{4}} \cdot \prod_{i \in I_3} (n(p_i) \mid p_i)(-1)^{\frac{(2+8q_1)(2+4q_3)}{4}} \\ &= (-1) \cdot \prod_{i \in I_1} (1 \mid p_i) \cdot (-1)^{2(1+4q_1)(q_2)} \cdot \prod_{i \in I_3} (n(p_i) \mid p_i)(-1)^{(1+4q_1)(1+2q_3)}\end{aligned}$$

$$= (-1) \cdot \prod_{i \in I_1} (1 \cdot 1) \prod_{i \in I_3} ((-1) \cdot (-1))$$

$$= (-1) \cdot 1 \cdot 1,$$

where $q_1, q_2, q_3 \in \mathbb{N}$. This completes the proof. □

But we can do much better than this using work of Granville, Mollin and Williams [15], improved by Trevino [32]. However, their qualification "a finite number of exceptions "spoils its application, as can be seen in Table 2.2.

Lemma 2.4 *[32] Let N be a square-free integer. Then, other than a finite number of exceptions, there is an odd prime $p < (4N)^{0.45}$ such that $(N \mid p) = -1$.*

Here I give Table 2.2 that shows the first 32 square-free numbers A, for each A, the smallest odd prime p such that $(A \mid p) = -1$ as well as the upper bound $(4A)^{0.45}$ and $(4A)^{5.5}$ for p. Also, we can find out a few exceptions that $p > (4N)^{0.45}$ from this table.

A	p	$(4A)^{0.45}$	$(4A)^{5.5}$	A	p	$(4A)^{0.45}$	$(4A)^{5.5}$
2	3	2.54912	92681.9	29	3	8.49129	$2.26214 \cdot 10^{11}$
3	5	3.05937	861979.	30	11	8.62247	$2.72582 \cdot 10^{11}$
5	3	3.85002	$1.43108 \cdot 10^{7}$	31	7	8.75064	$3.26452 \cdot 10^{11}$
6	7	4.17922	$3.90087 \cdot 10^{7}$	33	5	9.00033	$4.60423 \cdot 10^{11}$
7	5	3.85002	$9.10687 \cdot 10^{7}$	34	7	9.12205	$5.4258 \cdot 10^{11}$
10	7	5.25929	$6.47634 \cdot 10^{8}$	35	3	9.24182	$6.36362 \cdot 10^{11}$
11	3	5.48976	$1.09393 \cdot 10^{9}$	37	5	9.47584	$8.63852 \cdot 10^{11}$
13	5	5.91836	$2.74169 \cdot 10^{9}$	38	5	9.59024,	$1.00032 \cdot 10^{12}$
14	3	6.11906	$4.1213 \cdot 10^{9}$	39	11	9.703	$1.15395 \cdot 10^{12}$
15	13	6.31202	$6.02326 \cdot 10^{9}$	41	7	9.92384,	$1.51929 \cdot 10^{12}$
17	3	6.67773	$1.19894 \cdot 10^{10}$	42	5	10.032	$1.73461 \cdot 10^{12}$
19	7	7.02047	$2.21042 \cdot 10^{10}$	43	5	10.1388	$1.97427 \cdot 10^{12}$
21	11	5.48976	$3.83298 \cdot 10^{10}$	46	11	10.4512	$2.86087 \cdot 10^{12}$
22	5	4.79924	$4.95056 \cdot 10^{10}$	47	5	10.5529	$3.22009 \cdot 10^{12}$
23	3	7.65076	$6.32169 \cdot 10^{10}$	51	11	10.948	$5.04622 \cdot 10^{12}$
26	3	8.08472	$1.24075 \cdot 10^{11}$	53	5	11.1391	$6.23515 \cdot 10^{12}$

Table 2.2: The first 32 square-free numbers, the smallest odd prime p such that $(A \mid p) = -1$ and the value of $(4A)^{0.45}$ and $(4A)^{5.5}$.

Definition Let A be a positive integer. Then the square-free part of A, written $\mathrm{sf}(A)$ is the product of all primes which divide A to an odd power, or 1 if $A = 1$. We can write $A = \mathrm{sf}(A)\square$.

Proposition 2.5 *Let $A \in \mathbb{N}$ be not a square. Then $n! = x^2 - A$ has at most finitely many solutions, indeed any solution satisfies $n \leq (4 \cdot \mathrm{sf}(A))^{0.45}$, other than a finite number of exceptions, in which $n \leq (4 \cdot \mathrm{sf}(A))^{0.45}$.*

Proof. Using Lemma 2.3 choose a prime p which is such that $(A \mid p) = -1$. Note that we can find such a prime with $p < (4 \cdot \mathrm{sf}(A))^{0.45}$. Then $n! = x^2 - A$ with $n \geq p$, implies $x^2 \equiv A \pmod{p}$ which is impossible. Thus if the equation has a solution we must have $n < p < (4 \cdot \mathrm{sf}(A))^{0.45}$. □

Chapter 3

The result of Erdös and Obláth

3.1 Overview

In this chapter I work with the result of Erdös and Obláth given in [13], that

$$n! = x^p + y^p$$

has no solutions when $(x, y) = 1$ and p is an odd prime. Part of their proof was given in the recently published book by Jean-Marie De Koninck and Florian Luca [19], but the proof was incomplete. Firstly, I introduce some preliminary results which will be employed for the proof. Then I will prove a restricted form of their result, Theorem 3.1 in Section 3.3. Moreover, I have made their proof explicit in two special cases in Section 3.5. One is when $p = 3$ and $y = -1$, the other case is when $p = 8$. The first case comes close to the original Brocard's problem. In Section 3.4, I consider some other related equations. Note that in Section 3.4.3, I show $n! = x^2 + y^2$ has only 3 solutions. This is an easy exercise and includes $2!-1 = 1^2$, showing that the case $n!-1 = x^2$ is trivial corresponding with Brocard's original problem.

Theorem 3.1 *[13] Let $p > 2$ be a fixed odd prime. Let x, y be coprime integers with $\max\{|x|, |y|\} > 1$. Then the diophantine equation $n! = x^p + y^p$ has at most a finite number of solutions.*

Erdös and Obláth actually proved that the given equation has **no** integer solutions. I use some well-known prelimary results, like Brun-Titchmarsh Theorem and Abel's Identity. These are needed for proving Theorem 3.2. There follow some formulas and results that play a key role in the proof of Theorem 3.1.

3.2 Preliminary results

Theorem 3.2 *[19] If a and b are coprime positive integers with $b > 1$, and $p_{a,b}$ is the smallest prime congruent to a modulo b, then we have*

$$\sum_{\substack{p \le x \\ p \equiv a \bmod b}} \frac{1}{p} \ll \frac{1}{p_{a,b}} + O\left(\frac{\log\log x}{\phi(b)}\right)$$

uniformly for $x \ge 3$ and $1 \le a < b$.

Proof. We may assume that $b \ge 3$, since otherwise the desired estimate follows from Mertens formula [31]

$$\sum_{p \le x} \frac{1}{p} = \log\log x + B + O\left(\frac{1}{\log x}\right),$$

where B, named as Mertens constant, is approximately 0.26 and O is the Landau symbol.

If $3 \le x \le 3b$, then

$$\begin{aligned}
\sum_{\substack{p \le x \\ p \equiv a \bmod b}} \frac{1}{p} &= \frac{1}{p_{a,b}} + \frac{1}{a+b} + \frac{1}{a+2b} \\
&< \frac{1}{p_{a,b}} + \frac{1}{b} + \frac{1}{2b} \\
&\le \frac{1}{p_{a,b}} + \frac{3}{2\phi(b)} \\
&= \frac{1}{p_{a,b}} + C_1\left(\frac{\log\log x}{\phi(b)}\right) \quad \text{where } C_1 \text{ is a constant} \\
&\ll \frac{1}{p_{a,b}} + O\left(\frac{\log\log x}{\phi(b)}\right),
\end{aligned}$$

since $\phi(b) \le b$ and $\log\log 3 > 0$.

Now we assume that $x > 3b$ and let $a_n = 1$ if n is a prime $> 3b$ that is congruent

to a modulo b and 0 otherwise. Then using Theorem 1.4 and Theorem 1.5 show that

$$A(x) = \sum_{n \le x} a_n \le \pi(x; a, b) \le \frac{2x}{\phi(b)\log(x/b)}.$$

Now with $f(t) = 1/t$ we have

$$\begin{aligned}
\sum_{\substack{p \le x \\ p \equiv a \bmod b}} \frac{1}{p} &\le \frac{1}{p_{a,b}} + \sum_{\substack{b < p \le x \\ p \equiv a \bmod b}} \frac{1}{p} \\
&< \frac{1}{p_{a,b}} + \frac{1}{b} + \frac{1}{2b} + \sum_{3b < n \le x} a_n f(n) \\
&= \frac{1}{p_{a,b}} + \frac{3}{2b} + \frac{A(x)}{x} + \int_{3b}^{x} \frac{A(t)}{t^2} dt \\
&\le \frac{1}{p_{a,b}} + \left(\frac{3}{2b} + \frac{2x}{\phi(b)\log(x/b)x} \right) + \left(\int_{3b}^{x} \frac{2t}{\phi(b)\log(t/b)t^2} dt \right) \\
&\le \frac{1}{p_{a,b}} + \frac{1}{\phi(b)} \left(\frac{3}{2} + \frac{2}{\log(x/b)} \right) + \frac{1}{\phi(b)} \left(\int_{3b}^{x} \frac{2}{\log(t/b)t} dt \right) \\
&\le \frac{1}{p_{a,b}} + \frac{1}{\phi(b)} \left(\frac{3}{2} + \frac{2}{\log 3} \right) + \frac{1}{\phi(b)} \left(\int_{3b}^{x} \frac{2}{\log(t/b)t} dt \right) \\
&= \frac{1}{p_{a,b}} + C_2 \left(\frac{1}{\phi(b)} \right) + C_3 \left(\frac{1}{\phi(b)} \int_{3b}^{x} \frac{1}{\log(t/b)t} dt \right) \\
&\ll \frac{1}{p_{a,b}} + O\left(\frac{1}{\phi(b)} \right) + O\left(\frac{1}{\phi(b)} \int_{3b}^{x} \frac{1}{\log(t/b)t} dt \right) \\
&= \frac{1}{p_{a,b}} + O\left(\frac{\log\log x}{\phi(b)} \right),
\end{aligned}$$

where C_2 and C_3 are constants.

As for the integral, to evaluate this we made the change of variable $u = t/b$, getting $dt = bdu$, so that

$$\begin{aligned}
\int_{3b}^{x} \frac{1}{t\log(t/b)} dt = \int_{3}^{x/b} \frac{du}{u\log u} &= \log\log u|_{u=3}^{u=x/b} \\
&= \log\log(x/b) - \log(\log 3) < \log\log(x/b) \\
&< \log\log x.
\end{aligned}$$

This completes the desired estimate in the range $x \ge 3b$ and so we finish this proof. □

After redoing this derivation with $f(t) := \frac{\log t}{t}$, we can get Lemma 1.6, which is important when proving Theorem 3.1.

The following two results are very important, and particularly Lemma 3.4 is applied for the proof of Theorem 3.1.

Lemma 3.3 *Let p be an odd prime, and $x,\ y$ coprime integers with $\max\{|x|,|y|\} > 1$. If $p \mid x-y$, then we have $\nu_p\left(\frac{x^n-y^n}{x-y}\right) = \nu_p(n)$, where ν_p is the function that counts the exponent of p.*

Proof. Let $x,\ y$ be coprime with $\max\{|x|,|y|\} > 1$, and let p be a prime ≥ 3 with $p \nmid xy$. Assume that $p \mid x-y$ and $x = y + kp^e$, where $p \nmid k$. Next, by the binomial theorem, we can get

$$x^p = y^p + \binom{p}{1} y^{p-1} k p^e + \binom{p}{2} y^{p-2} k^2 p^{2e} + \cdots + k^p p^{pe}.$$

Because $p \mid \binom{p}{j}$ for any j with $1 \leq j \leq p-1$. We have

$$\nu_p\left(\binom{p}{j}\right) \geq 1,$$

and then we get

$$\nu_p\left(\binom{p}{j} y^{p-j} k^j p^{ej}\right) \geq 1 + ej.$$

As for the last term, $\nu_p(k^p p^{pe}) = pe$. So now we can conclude that the power of p in $x^p - y^p$ is $e+1$. i.e. $\nu_p(x^p - y^p) = e+1$. After repeating, take power of p to $x^p - y^p$ r times, we can work out $\nu_p\left(x^{p^r} - y^{p^r}\right) = e + r$.

Explicitly, since $\nu_p(x^p - y^p) = e+1$, then we can write $x^p = y^p + k_1 p^{e+1}$. After taking power of p to both sides, it gives $\nu_p\left(x^{p^2} - y^{p^2}\right) = (e+1) + 1 = e+2$. The result given above follows by induction.

Now let us consider $\nu_p\left(\frac{x^n-y^n}{x-y}\right)$, where $n = mp^r$ and $p \nmid m$. Say $x_1 = x^m$ and $y_1 = y^m$ then we have $p \nmid \frac{x^m-y^m}{x-y}$. Since if so,

$$p \mid \left(x-y, \frac{x^m-y^m}{x-y}\right) = \left(x-y, k_2(x-y) + my^{m-1}\right) = (x-y, m) \mid m,$$

which contradicts $p \nmid m$. Since $p \nmid \frac{x^m-y^m}{x-y}$, then $\nu_p\left(\frac{x^m-y^m}{x-y}\right) = 0$, and we can get $e = \nu_p(x-y) = \nu_p(x_1 - y_1) = \nu_p(x^m - y^m) \geq 1$. So $\nu_p\left(x_1^{p^r} - y_1^{p^r}\right) = e + r$.

Therefore, it gives

$$\nu_p\left(\frac{x_1^{p^r}-y_1^{p^r}}{x-y}\right)=(e+r)-e=r=\nu_p(n),$$

and that is

$$\nu_p\left(\frac{x^n-y^n}{x-y}\right)=\nu_p\left(\frac{x_1^{p^r}-y_1^{p^r}}{x-y}\right)=\nu_p(n).$$

That completes the proof. □

Lemma 3.4 *Let p be any prime. If x, y are coprime integers and $\frac{x^p-y^p}{x-y}=\delta m$, where $\delta\in\{1,p\}$, and then for all primes $q\mid m$, we have $q\equiv 1 \bmod p$.*

Proof. Let $\frac{x^p-y^p}{x-y}=h$ and suppose $p\mid x-y$ with $x=y+kp^e$ and $(p,k)=1$. By Lemma 3.3, we can get directly that

$$\nu_p(h)=\nu_p\left(\frac{x^p-y^p}{x-y}\right)=\nu_p(p)=1,$$

which implies $p\mid h$, then we write $h=pm$ but $p\nmid m$.

However, if $p\nmid x-y$, then $a:=xy^{-1}\not\equiv 1 \bmod p$, which gives the multiplicative order e of $a \bmod p$ is greater than 1. i.e. $a^e\equiv 1 \bmod p$ and e is minimal with $e>1$. But if $p\mid h$ in this case as well, then because $p\mid x^p-y^p$ definitely, there is $(xy^{-1})^p=a^p\equiv 1 \bmod p$. Hence $e\mid p$, and then $e=p$ since $e>1$ and p is a prime. But it leads to $p=e\mid p-1$, which is impossible. Therefore, it means $p\nmid h$ in this case.

In conclusion, we have

$$\frac{x^p-y^p}{x-y}=\delta m\begin{cases}\delta=1\Leftrightarrow p\nmid x-y\\ \delta=p\Leftrightarrow p\mid x-y\end{cases}\quad\text{with } p\nmid m.$$

Now let us consider another interesting fact, the property of m. Let q be any prime such that $q\mid m$. If also $q\mid x-y$, then by Lemma 3.3, $\nu_q\left(\frac{x^p-y^p}{x-y}\right)=\nu_q(p)=0$ as $(p,q)=1$. However $\nu_q(\delta m)\geq 1$ since $q\mid m$, which gives a contradiction. Therefore, this case does not exist. While consider if $q\nmid x-y$. Since $q\mid x^p-y^p$ always, then we have $(xy^{-1})^p=a^p\equiv 1 \bmod q$, and the multiplicative order of

$a \bmod q$ is $e > 1$. Therefore, $e = p \mid q - 1$, i.e. $q \equiv 1 \bmod p$.

This completes the proof. □

3.3 Proof of Theorem 3.1

Now we have laid these massive foundations in Section 3.2, we can set out the proof from [19], which I have improved.

Proof. Assume that $|x| > |y|$. Since $n! > 0$, we have that x is positive. Observe that the condition that x and y are coprime implies that no prime $q \leq n$ divides either x or y, which implies that $(x, q) = (y, q) = 1$ for any prime $q \leq n$. Thus, $x \geq n + 1$ and both x and y are odd.

If $y > 0$, then $n^n > n! > x^p \geq (n+1)^p$, while if $y < 0$, then

$$n^n > n! = x^p - |y|^p = (x - |y|)(x^{p-1} + x^{p-2}|y| + \ldots + |y|^{p-1}) > x^{p-1} \geq (n+1)^{p-1}.$$

In both cases therefore, $p < n$. Also note that

$$x^p + y^p = (x + y)\left(\frac{x^p + y^p}{x + y}\right). \tag{3.3.1}$$

Lemma 3.4 shows that

$$\frac{x^p + y^p}{x + y} = \delta m,$$

where $\delta \in \{1, p\}$ and all primes $q \mid m$ have the property that $q \equiv 1 \bmod p$.

If $y > 0$, then

$$m = \frac{x^p + y^p}{\delta(x + y)} > \frac{x^p}{\delta(2x)} \geq \frac{x^p}{2xp} = \frac{x^{p-1}}{2p},$$

while if $y < 0$, then

$$m = \frac{1}{\delta}\left(\frac{x^p - |y|^p}{x - |y|}\right) = \frac{1}{\delta}(x^{p-1} + x^{p-2}|y| + \ldots + |y|^{p-1}) > \frac{x^{p-1}}{\delta} \geq \frac{x^{p-1}}{p} > \frac{x^{p-1}}{2p}.$$

Thus, the inequality

$$m > \frac{x^{p-1}}{2p} = \frac{2x^{p-1}}{4p} = \frac{2(x^p)^{\frac{p-1}{p}}}{4p} > \frac{(2x^p)^{\frac{p-1}{p}}}{4p} > \frac{(n!)^{\frac{p-1}{p}}}{4p} \tag{3.3.2}$$

holds, where we used the fact that $n! = x^p + y^p < 2x^p$. Let M be the largest divisor of $n!$ amongst those composed only of prime factors $q \equiv 1 (\mathrm{mod}\ p)$. Then $m \mid M$, so $M \geq m > \frac{(n!)^{\frac{p-1}{p}}}{4p}$ by (3.3.2), which gives

$$\log M > \left(\frac{p-1}{p}\right) \log(n!) - \log(4p) > \left(\frac{p-1}{p}\right) n \log\left(\frac{n}{e}\right) - \log(4p), \qquad (3.3.3)$$

where we used the version of Stirling's formula $n! > \left(\frac{n}{e}\right)^n$ which is true for all $n \geq 1$. Now for each prime $q \leq n$, the exponent of q in $n!$ is

$$\left\lfloor \frac{n}{q} \right\rfloor + \left\lfloor \frac{n}{q^2} \right\rfloor \ldots < n \sum_{i \geq 1} \frac{1}{q^i} = \frac{n}{q-1}.$$

Then we can get,

$$M < \prod_{\substack{q \leq n \\ q \equiv 1 \bmod p}} q^{\frac{n}{q-1}},$$

and next

$$\log M < n \sum_{\substack{q \leq n \\ q \equiv 1 \bmod p}} \frac{\log q}{q-1}. \qquad (3.3.4)$$

By (3.3.3) and (3.3.4), we get that

$$\left(\frac{p-1}{p}\right) \log n - \frac{p-1}{p} - \frac{\log 4p}{n} < \sum_{\substack{q \leq n \\ q \equiv 1 \bmod p}} \frac{\log q}{q-1},$$

which implies, using the fact that $p < n$, that

$$\left(\frac{p-1}{p}\right) \log n \leq \sum_{\substack{q \leq n \\ q \equiv 1 \bmod p}} \frac{\log q}{q-1} + O(1). \qquad (3.3.5)$$

Using the trivial inequality

$$\sum_{\substack{q \leq n \\ q \equiv 1 \bmod p}} \frac{\log q}{q-1} \ll \frac{\log n}{p} \sum_{t \leq \frac{n}{p}} \frac{1}{t} \ll \frac{\log^2 n}{p},$$

we get that

$$\frac{2}{3} \log n \leq \left(\frac{p-1}{p}\right) \log n \ll \frac{\log^2 n}{p} + O(1),$$

which implies

$$\frac{2}{3} \leq \frac{C_1 \log n}{p} + \frac{C_2}{\log n} \text{ where } C_1, C_2 \text{ are constants.}$$

There exists n_0 so that for any $n \geq n_0$, $\frac{C_2}{\log n} \leq \frac{1}{3}$. So

$$\frac{1}{3} \leq \frac{C_1 \log n}{p},$$

$$p \leq (3C_1) \log n.$$

Therefore it implies

$$p \ll \log n.$$

In light of the relation

$$\sum_{\substack{p \leq x \\ p \equiv a \bmod b}} \frac{\log p}{p} \ll \frac{A \log x}{\phi(b)},$$

we get that for $p \ll \log n$,

$$\sum_{\substack{q \leq n \\ q \equiv 1 \bmod p}} \frac{\log q}{q} \ll \frac{\log n}{2p},$$

$$\sum_{\substack{q \leq n \\ q \equiv 1 \bmod p}} \frac{2 \log q}{q} \ll \frac{\log n}{p}.$$

However,

$$\sum_{\substack{q \leq n \\ q \equiv 1 \bmod p}} \frac{\log q}{q-1} \leq \sum_{\substack{q \leq n \\ q \equiv 1 \bmod p}} \frac{2 \log q}{q},$$

so it implies

$$\sum_{\substack{q \leq n \\ q \equiv 1 \bmod p}} \frac{\log q}{q-1} \ll \frac{\log n}{p}.$$

Thus the estimate (3.3.5) leads to

$$\frac{2}{3} \log n \leq \left(\frac{p-1}{p} \right) \log n \ll \frac{\log n}{p} + O(1),$$

$$\frac{2}{3} \ll \frac{1}{p} + \frac{O(1)}{\log n},$$

Then

$$\frac{2}{3} \leq \frac{C_3}{p} + \frac{C_4}{\log n},$$

where $C_3,\ C_4$ are constants. Again, choose n sufficiently large so that $\frac{C_4}{\log n} \leq \frac{1}{3}$, and then

$$\frac{1}{3} \leq \frac{C_3}{p},$$

$$p \leq 3C_3,$$

which shows that p is bounded. Now by Lemma 1.6,

$$\sum_{\substack{p \leq x \\ p \equiv a \bmod b}} \frac{\log p}{p} = \frac{\log x}{\phi(b)} + O_b(1),$$

we can get

$$\sum_{\substack{q \leq n \\ q \equiv 1 \bmod p}} \frac{\log q}{q} = \frac{\log n}{p-1} + O_p(1).$$

But

$$\sum_{\substack{q \leq n \\ q \equiv 1 \bmod p}} \frac{\log q}{q-1} + C_5 = \sum_{\substack{q \leq n \\ q \equiv 1 \bmod p}} \frac{\log q}{q} = \frac{\log n}{p-1} + C_6 f(p),$$

where C_5, C_6 are constants, and $f(p)$ represents some functions. Then it gives

$$\sum_{\substack{q \leq n \\ q \equiv 1 \bmod p}} \frac{\log q}{q-1} = \frac{\log n}{p-1} - C_5 + C_6 f(p),$$

so we have

$$\sum_{\substack{q \leq n \\ q \equiv 1 \bmod p}} \frac{\log q}{q-1} \leq \frac{\log n}{p-1} - C_5 + C_6 \cdot \ \max\{f(2), f(3), \cdots, f(B)\} \ \text{ where } B \in \mathbb{P},$$

as p is bounded and $p \in \{2, 3, \cdots, B\}$. Hence we conclude that

$$\sum_{\substack{q \leq n \\ q \equiv 1 \bmod p}} \frac{\log q}{q-1} = \frac{\log n}{p-1} + O(1).$$

So (3.3.5) implies that

$$\left(\frac{p-1}{p}\right)\log n \leq \frac{\log n}{p-1} + O(1),$$

then we have

$$\frac{p-1}{p} - \frac{1}{p-1} \leq \frac{O(1)}{\log n} = \frac{C_7}{\log n} \text{ where } C_7 \text{ is a constant,}$$

which in turn has only finitely many solutions n with $p \geq 3$. Because

$$\frac{1}{6} \leq \frac{p-1}{p} - \frac{1}{p-1} = \frac{p^2-3p+1}{p(p-1)} \leq \frac{C_7}{\log n},$$

and then

$$n \leq e^{6C_7}.$$

In conclusion, using $n^n > x^{p-1}$ as well as n and p are both bounded, we get that x is also bounded. This completes the proof. □

Corollary 3.5 *Let m be any positive odd number and x, y be coprime integers with $\max\{|x|,|y|\} > 1$. Then the diophantine equation $n! = x^m + y^m$ has at most a finite number of solutions.*

Corollary 3.6 *Let the positive integer m have an odd prime factor and x, y be coprime integers with $\max\{|x|,|y|\} > 1$. Then the diophantine equation $n! = x^{2m} \pm y^{2m}$ also has at most a finite number of solutions.*

Note: this does not cover the case $n! = x^{2^m} \pm y^{2^m}$, $m \geq 1$, which includes $n! = x^2 - 1$. Note also that we could, in theory, make all of the constants C_i in the proof of Theorem 3.1 explicit. But this is a large task and I was not able to complete it.

3.4 Other related equations

3.4.1 Overview

In this section, I will consider some other related equations. Firstly, I will discuss the equation $n! = x^2 - y^2$, and show there are no solutions when $n = 1, 2, 3$. Also,

I will describe the characterization of those even numbers, which can be expressed as the difference of two squares. For the equation $n! = x^2 + y^2 + z^2$, I will give some infinite sets of $n!$'s, and show that they can or cannot be expressed as the sum of three squares, respectively. Theorem 3.9 is new I think and depends on a fascinating discovery made of what happens to positive integers when the powers of 2 are removed. This idea has a lot of promise for other applications. Finally, I will discuss the equation $n! = x^2 + y^2$ and give the only three known solutions, $\{n, x, y\}$. Then I will give the characterization of a particular set of $n!$, such that they cannot be represented as the sum of two squares.

In Chapter 6, I consider equations $n! = f(x)$, different from these in that the right hand side is a function of just one variable.

3.4.2 The equation $n! = x^2 - y^2$

There are the classical Brocard's problem solutions

$$\begin{aligned} 4! &= 5^2 - 1^1, \\ 5! &= 11^2 - 1^2, \\ 7! &= 71^2 - 1^2, \end{aligned}$$

but I also found expressions for $6!,\ 8!,\ 9!$ and $10!$, so maybe **all** factorials, except for $1!,\ 2!$ and $3!$ can be expressed as the difference of two squares. Here is the proof that these three fail to have such a representation.

Without loss of generality, suppose $|x| > |y| > 0$. Obviously, $x^2+y^2 > x^2-y^2 \geq (y+1)^2 - y^2 \geq 3 > 1!$. Let us check $2!$ and $3!$ next. Since they are both even numbers, then $x,\ y$ are either both even or both odd. Therefore, we can get a similar relation as before, that is $x^2 + y^2 > x^2 - y^2 \geq (y+2)^2 - y^2 \geq 8$, which is larger than both $2!$ and $3!$. So we are done.

In addition, we can show that all odd positive integers can be expressed as the difference of two positive integer squares, but that only those even integers which are 8 or more, and divisible by 4 can be so expressed. Here we just pay attention to even integers since $n!$ with $n \neq 1$ is always even.

Now suppose that the even number m is expressible as the difference of two squares, $m = 2n = x^2 - y^2 = (x + y)(x - y)$. This relation tells that either $x + y$ or $x - y$ is divisible by 2. However, both terms have the same parity, so they are both even numbers, which gives $4 \mid m$, and also $x,\ y$ have the same parity. If $x,\ y$ are both even and then $x = 2x_1,\ y = 2y_1$, which gives $m = 2^2(x_1 - y_1)(x_1 + y_1)$. Since $x_1 + y_1 > x_1 - y_1 \geq 1$, then we have $m \geq 8$. If $x,\ y$ are both odd, and then $x = 2x_1+1,\ y = 2y_1+1$ with $x_1 > y_1 \geq 0$, which implies $m = 2^2(x_1-y_1)(x_1+y_1+1)$. So we still obtain $m \geq 8$. If $4 \mid n$, let $n = 4m = (m + 1)^2 - (m - 1)^2$, so any n which is divided by 4 and greater than 8 can be written as the difference of two squares. So if $n \geq 4$, $n! \geq 8$ and $n!$ is even, then $n! = x^2 - y^2$ has a solution.

3.4.3 The equation $n! = x^2+y^2+z^2$ with $x,\ y,\ z$ non-negative

Compare Lagrange's theorem, that any integer can be represented as the sum of four squares, it appears that *not every* factorial can be represented as the sum of three squares. Here is a lemma given in [17] giving the characterization of such numbers.

Lemma 3.7 *A number s can be represented as the sum of three squares if and only if $s \neq 4^e(8k + 7)$, for any $e \geq 0,\ k \geq 0$.*

Here I give a brief proof [10] about the representation. It is known that $(2m)^2 \equiv 0 \bmod 4$ and $(2m + 1)^2 \equiv 1 \bmod 8$. So, no matter what the parity of a number is, we have $x^2 \equiv 0,\ 1,\ 4 \bmod 8$, and thus $x^2 + y^2 + z^2 \not\equiv 7 \bmod 8$. Therefore, there is no number of the form $8m + 7$ expressible as the sum of three squares. In addition, if $x^2 + y^2 + z^2 \equiv 0 \bmod 4$, then $x,\ y,\ z$ are definitely even, so that we have $\frac{1}{4}(x^2 + y^2 + z^2) = \left(\frac{1}{2}x\right)^2 + \left(\frac{1}{2}y\right)^2 + \left(\frac{1}{2}z\right)^2$, which implies that no number $4^e(8k + 7)$ is the sum of three squares.

We used the computer to check and found quite a few factorials of the form $4^e(8k + 7)$. Here is the list of values n such that $n! = 4^e(8k + 7)$ with $n \leq 400$.

$$\begin{aligned} S &= \{10, 12, 24, 25, 48, 49, 54, 60, 78, 91, 96, 97, 107, 114, 120, 121, 142, 151, 167, \\ & 170, 172, 180, 192, 193, 212, 222, 226, 238, 240, 241, 246, 252, 270, 279, 301, \\ & 307, 309, 318, 327, 333, 344, 345, 357, 360, 361, 367, 375, 379, 384, 385\} \end{aligned}$$

Take 10 as an example, $10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7 = 4^4 \cdot 3^4 \cdot 5^2 \cdot 7 = 4^4(8k+7)$, where $k = 253$, then $10!$ cannot be expressed as the sum of three squares. Observe that if n is on this list and $8 \mid n$ then $n+1$ is also on the list. Observe also the subsequence $\{12, 24, 48, 96, 192, \ldots\} \subset S$. This suggests the following new Theorem 3.9 which I was able to prove. First a lemma.

Lemma 3.8 *If $n \geq 2$ the binomial coefficient*

$$\binom{3 \cdot 2^{n+1}}{3 \cdot 2^n}$$

is 4 times an odd number.

Proof. The only thing we need to check is the power of 2 in the binomial coefficient. Now let $m = 3 \cdot 2^n$ and we can write that

$$\begin{aligned} \nu_2\left(\binom{2m}{m}\right) &= \nu_2\left(\frac{(2m)!}{(m!)^2}\right) \\ &= \nu_2((2m)!) - 2\nu_2(m!) \\ &= \sum_{j \geq 1}\left(\left\lfloor \frac{2m}{2^j} \right\rfloor - 2\left\lfloor \frac{m}{2^j} \right\rfloor\right). \end{aligned}$$

By using $0 \leq \lfloor 2x \rfloor - 2\lfloor x \rfloor \leq 1$ and the result that $\lfloor 2x \rfloor - 2\lfloor x \rfloor$ is always an integer, we figure out with Mathematica an array of values of

$$\left\lfloor \frac{3 \cdot 2^{n+1}}{2^j} \right\rfloor - 2\left\lfloor \frac{3 \cdot 2^n}{2^j} \right\rfloor,$$

for $1 \leq j \leq 10$ and $2 \leq n \leq 10$. That is

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

As the array implies, $\left\lfloor \frac{3\cdot 2^{n+1}}{2^j} \right\rfloor - 2\left\lfloor \frac{3\cdot 2^n}{2^j} \right\rfloor = 1$ if and only if $j = n+1$ or $n+2$. Also $\left\lfloor \frac{3\cdot 2^{n+1}}{2^j} \right\rfloor - 2\left\lfloor \frac{3\cdot 2^n}{2^j} \right\rfloor = \frac{3\cdot 2^{n+1}}{2^j} - 2\left(\frac{3\cdot 2^n}{2^j}\right) = 0$ when $j < n+1$; while $\left\lfloor \frac{3\cdot 2^{n+1}}{2^j} \right\rfloor - 2\left\lfloor \frac{3\cdot 2^n}{2^j} \right\rfloor = 0 - 0$ when $j > n+2$, as $2^{n+3} > 3\cdot 2^{n+1} > 3\cdot 2^n$. In conclusion, the power of 2 dividing the binomial coefficient is 2 for any $n \geq 2$, i.e.

$$\binom{3\cdot 2^{n+1}}{3\cdot 2^n} = 4\cdot(2y+1) \text{ for some integers } y.$$

□

Theorem 3.9 *There is an infinite set of factorials which cannot be expressed as the sum of three integer squares. In particular $m!$ where $m = 3\cdot 2^n$ with $n \geq 2$.*

Proof. 1. First we show that when m is of the given form, $\nu_2(m!)$ is even. (For example, $a_n = 3\cdot 2^n$ and let $n = 2$. Then

$$\nu_2(a_2!) = \nu_2(12!) = \nu_2(479001600) = \nu_2(2^{10}\cdot 3^5\cdot 5^2\cdot 7\cdot 11) = 10$$

is even.) By Lemma 3.8

$$\binom{a_{n+1}}{a_n} = 4(2x+1)$$

for some integers x, so $a_{n+1}! = (a_n!)^2\cdot 4\cdot(2x+1)$. Therefore, by induction, $\nu_2(a_n!)$ is even for all $n \geq 2$. This means we can write $m! = 4^e\cdot o$ where o is an odd

number.

2. Next we make a preliminary calculation. Fix $n \geq 2$ and let

$$s_1 = (3 \cdot 2^n + 1,\ 3 \cdot 2^n + 2, \ldots, 3 \cdot 2^n + 3 \cdot 2^n).$$

Factor each element of s_1 in the form of $2^e \cdot o$, where o is an odd number. Then take the odd part and sort the resulting sequence to obtain

$$s_2 = (1, 3, 5, 7, \ldots, 3 \cdot 2^{n+1} - 1),$$

which, I **claim** is the initial sequence of $3 \cdot 2^n$ odd numbers.

To see this, fix an odd number $2x + 1$ in the range $1 \leq 2x + 1 \leq 3 \cdot 2^{n+1} - 1$, so $0 \leq x \leq 3 \cdot 2^n - 1$. Let $a \geq 0$ be the smallest integer such that

$$3 \cdot 2^n < 2^a(2x - 1),$$

and define $j := 2^a(2x+1) - 3 \cdot 2^n$. Then $3 \cdot 2^n + j = 2^a(2x+1)$ and $j \leq 1$. We need only check that $j \leq 3 \cdot 2^n$. If **not** $j > 3 \cdot 2^n$ and therefore $2^a(2x + 1) > 3 \cdot 2^{n+1}$. If it happened that $a = 0$ then we would get $3 \cdot 2^{n+1} - 1 \geq 2x + 1 > 3 \cdot 2^{n+1}$, which is false. Thus $a \geq 1$ and we can write $2^{a-1}(2x + 1) > 3 \cdot 2^n$, giving a contradiction since a would not be the smallest integer. We have shown $j \leq 3 \cdot 2^n$, and a little thought shows this is enough to verify the **claim**.

Now rewrite s_2 in the form

$$s_3 = ((1, 3, 5, 7), (8 + 1, 8 + 3, 8 + 5, 8 + 7), \ldots, (8x + 1, 8x + 3, 8x + 5, 8x + 7))$$

where $x := 1 + 3 \cdot 2^{n-2}$. After multiplying all of the elements of s_3 together modulo 8, we obtain a number congruent to 1.

3. Now let $n = 2$ and then

$$m! = (3 \cdot 2^2)! = 12! = 2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11 \equiv 7 \bmod 8.$$

According to the conclusion of part 2,

$$(3\cdot 2^3)! = (3\cdot 2^2)!\cdot((3\cdot 2^2+1)\cdot(3\cdot 2^2+2)\ldots(3\cdot 2^2+3\cdot 2^2)) \equiv (3\cdot 2^2)!\cdot 1 \equiv 7 \bmod 8.$$

By induction, $(3\cdot 2^n)! \equiv (3\cdot 2^2)!\cdot 1 \equiv 7 \bmod 8$. Therefore, we have completed the proof that $m!$ cannot be expressed as the sum of three integer squares when m is the form of $3\cdot 2^n$. □

Another potential subsequence I observed was $(60, 120, 240, 480, \ldots)$. The theorem falls short of giving a characterization of every n on the list, which is an interesting problem.

Of course there are an infinite number of factorials which can be expressed as the sum of three squares. According to the conclusion from above, we only need to ensure the power of 2 dividing a factorial is odd. For example, let $m = 2^n$ and it is easy to see that

$$\nu_2((2^n)!) = 2^n - 1$$

which is odd for all $n \geq 1$, giving an infinite set of expressible factorials. Take $n = 2$ as an example, $m! = (2^2)! = 4! = 2^3\cdot 3 = 24$, while $24 = 4^2 + 2^2 + 2^2$.

3.4.4 The equation $n! = x^2 + y^2$ with x and y non-negative

The following lemma is well known.

Lemma 3.10 *[14] A positive integer N cannot be represented as the sum of two squares if and only if in the standard prime factorization of N there occurs to an odd power a prime $p \equiv 3 \bmod 4$.*

Lemma 3.11 *[24] The interval $n < p < 4n/3$, for $n \geq 118$ always contains a prime of each of the forms*

$$12m+1,\ 12m+5,\ 12m+7,\ 12m+11$$

i.e. a prime in each of the possible $\phi(12) = 4$ residue classes modulo 12.

Theorem 3.12 *The only factorials which can be expressed as the sum of two squares of integers are* $1! = 1^2 + 0^2$, $2! = 1^2 + 1^2$ *and* $6! = 12^2 + 24^2$.

Proof. I used exhaustive search up to $N = 159$ and found only the 3 given solutions. I claim that for $n \geq 160$ there is always at least one prime to power 1 and congruent to 3 modulo 4 in the standard factorization of $n!$.

Any prime p with $\frac{3N}{4} < p < N$ has $\frac{N}{2} < p < N$, so appears to power 1 in the factorization of $N!$. But if we set $n := \frac{3N}{4}$, then $\frac{3N}{4} < p < N$ implies $n < p < \frac{4n}{3}$ and $N \geq 160$ implies $n \geq 120 > 118$. Thus there is at least one prime $p = 12m+7$, i.e. $p \equiv 3 \bmod 4$, appearing to power 1 in $N!$. The result now follows from Lemma 3.10 and Lemma 3.11. □

Corollary 3.13 *The equation* $n! - A^2 = x^2$ *has exactly three solutions,* $\{x, A\}$.

3.5 Estimation of some of the factors of $n!$

In this section, I will first establish Lemma 3.14 that proves the inequality

$$\nu_p(R(a,m)) \geq \nu_p(m!),$$

where $R(a,m) := (1+a)(1+2a)\dots(1+(m-1)a)$ with $a \geq 1$ and $p \nmid a$.

This is an essential condition used when I investigate the expression

$$P(m,a) := \prod_{p|a} p^{\lfloor \frac{m-1}{p-1} \rfloor} \left(\frac{(a+1)(2a+1)\dots((m-1)a+1)}{m!} \right),$$

while $P(m,a)$ is the main tool for estimating one set of factors of $n!$, i.e.

$$T(n,a,b) = \prod_{q \equiv b \bmod a} q^{\alpha_q(n)}.$$

Note that Lemma 3.14 is an improvement I made, so that the study of $T(n,a,b)$ becomes easier for readers to understand.

Continuing, I will reveal the process of estimation of $T(n,a,b)$ by translating the reference [13] and make it more complete.

Lemma 3.14 *Let* $R(a,m) := (1+a)(1+2a)\dots(1+(m-1)a)$ *with* $a \geq 1$. *If* $p \nmid a$, *then*

$$\nu_p(R(a,m)) \geq \nu_p(m!).$$

If $p \mid a$, *then* $\nu_p(R(a,m)) = 0$.

Before we prove this lemma, let us have a look at an example and see the relation between the prime factors of $R(a,m)$ and $m!$.
Let $m = 40$. Then

$$m! = 2^{38} \cdot 3^{18} \cdot 5^9 \cdot 7^5 \cdot 11^3 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23^1 \cdot 29^1 \cdot 31^1 \cdot 37^1.$$

If $a = 2$, then

$$\begin{aligned} R(2,40) &= (1+2)(1+2\cdot 2)\dots(1+2\cdot 39) \\ &= 3^{18} \cdot 5^{10} \cdot 7^7 \cdot 11^4 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23^2 \cdot 29^1 \cdot 31^1 \cdot 37^1 \\ &\quad \cdot 41^1 \cdot 43^1 \cdot 47^1 \cdot 53^1 \cdot 59^1 \cdot 61^1 \cdot 71 \cdot 67^1 \cdot 71^1 \cdot 73^1 \cdot 79^1. \end{aligned}$$

We see that the powers of all prime factors of $R(2,40)$ are larger than or equal to those of 40!, except for $p = 2$, since $p \mid a$ in this case. Moreover, for all of the primes that are larger than 37, the maximum prime factor of 40!, their powers are just 1 in $R(2,40)$. For $p = 13,\ 17,\ 19,\ 29,\ 31$ and 37, $\nu_p(R(2,40)) = \nu_p(40!)$. Otherwise, $\nu_p(R(2,40)) > \nu_p(40!)$ for all other prime factors of $R(2,40)$.
If $a = 5$, then

$$\begin{aligned} R(5,40) &= 2^{39} \cdot 3^{19} \cdot 7^7 \cdot 11^5 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23^2 \cdot 29^1 \cdot 31^2 \cdot 37^1 \cdot 41^1 \cdot 43^1 \\ &\quad \cdot 47^1 \cdot 53^1 \cdot 61^1 \cdot 71^1 \cdot 73^1 \cdot 83^1 \cdot 101^1 \cdot 131^1 \cdot 131^1 \cdot 151^1 \cdot 181^1 \cdot 191^1. \end{aligned}$$

We get $\nu_p(R(5,40)) \geq \nu_p(40!)$ for all prime factors of $R(5,40)$ and 40!, other than $p = 5$.

Proof. Let

$$v_r(m,p) := |\{j : 1 \leq j \leq m-1,\ \exists\, x \in \{0,1,\dots,a-1\},\ p^r x = 1 + ja\}|.$$

Note this counts the number of factors in $R(a,m)$ divisible by p^r. Let j_1 be the minimum value of j which satisfies the given equation, i.e. $p^r x_1 = 1 + aj_1$ with $j_1 \leq m-1$. Note that since $1 \leq x_1 < a$, then we must have $j_1 < p^r$.

Consider the case that $j_1 \leq (m-1) \bmod p^r$, the least positive residue. Since $p^r x = 1 + ja$ and $p^r y = 1 + ia$ for some $i > j$ implies $p^r(y-x) = a(i-j)$, because $(p,a) = 1$, then we must have $i \equiv j \bmod p^r$. So the number of solutions $v_r(m,p)$, is simply

$$\left\lfloor \frac{m-1}{p^r} \right\rfloor + 1 \geq \left\lfloor \frac{m}{p^r} \right\rfloor.$$

In particular, if $m-1 < m < p^r$, then $\left\lfloor \frac{m-1}{p^r} \right\rfloor = \left\lfloor \frac{m}{p^r} \right\rfloor = 0$ and

$$v_r(m,p) = \left\lfloor \frac{m-1}{p^r} \right\rfloor + 1 = 1 > \left\lfloor \frac{m}{p^r} \right\rfloor.$$

Moreover, if $p^r \alpha = m$ for some positive integers α, then

$$v_r(m,p) = \left\lfloor \frac{m-1}{p^r} \right\rfloor + 1 = \left\lfloor \frac{m}{p^r} \right\rfloor = \frac{m}{p^r} = \alpha.$$

Note that $\left\lfloor \frac{m-1}{p^r} \right\rfloor \neq \left\lfloor \frac{m}{p^r} \right\rfloor$ if and only if $p^r \alpha = m$ for some positive integers α. If it is the case that $j_1 > (m-1) \bmod p^r$ also, since we have

$$(m-1) \bmod p^r \equiv p^r \alpha - 1 - p^r \left\lfloor \frac{m-1}{p^r} \right\rfloor \geq 1,$$

then it implies

$$j_1 \geq p^r \left(\alpha - \left\lfloor \frac{m-1}{p^r} \right\rfloor \right) > p^r,$$

which is false. Hence if $j_1 > (m-1) \bmod p^r$, we must have $v_r(m,p) = \left\lfloor \frac{m-1}{p^r} \right\rfloor = \left\lfloor \frac{m}{p^r} \right\rfloor$.

So for any case, we can conclude that

$$v_r(m,p) \geq \left\lfloor \frac{m}{p^r} \right\rfloor,$$

and therefore

$$\nu_p(R(a,m)) = \sum_{r=1}^{\infty} v_r(m,p) \geq \sum_{r=1}^{\infty} \left\lfloor \frac{m}{p^r} \right\rfloor = \nu_p(m!).$$

This completes the proof of the lemma. □

3.5.1 A factor produced by just one prime in an arithmetic progression

The following work is based on that of [13], which I had to translate from German to English.

According to a classical theorem of Legendre, for each prime $q \leq n$, the exponent of q in $n!$ is

$$\alpha_q(n) := \left\lfloor \frac{n}{q} \right\rfloor + \left\lfloor \frac{n}{q^2} \right\rfloor + \left\lfloor \frac{n}{q^3} \right\rfloor + \dots . \tag{3.5.1}$$

Consider the prime q that is in an arithmetic progression $ak+b$, where $(a,\ b) = 1$, $0 < b < a$. Then it contributes to $n!$ a factor

$$T(n,a,b) = \prod_{q \equiv b \bmod a} q^{\alpha_q(n)} = \prod_{q \equiv b \bmod a} \prod_{r=1}^{\infty} q^{\lfloor \frac{n}{q^r} \rfloor}.$$

By taking logarithms, we get

$$\begin{aligned} \log T(n,a,b) &= \sum_{q \equiv b \bmod a} \sum_{r=1}^{\infty} \left\lfloor \frac{n}{q^r} \right\rfloor \log q \\ &= \sum_{q \equiv b \bmod a} \sum_{r=1}^{\infty} \sum_{1 \leq s \leq \frac{n}{q^r}} \log q \\ &= \sum_{s=1}^{\infty} \sum_{r=1}^{\infty} \sum_{\substack{q \equiv b \bmod a \\ q \leq \sqrt[r]{n/s}}} \log q. \end{aligned}$$

By setting

$$\Psi(x,a,b) := \prod_{r=1}^{\infty} \prod_{\substack{q \equiv b \bmod a \\ q \leq \sqrt[r]{x}}} q = \prod_{\substack{q \equiv b \bmod a \\ q \leq x}} q \prod_{\substack{q \equiv b \bmod a \\ q \leq \sqrt{x}}} q \prod_{\substack{q \equiv b \bmod a \\ q \leq \sqrt[3]{x}}} q \dots ,$$

we obtain

$$T(n,a,b)=\prod_{s=1}^{\infty}\Psi\left(\frac{n}{s},a,b\right)=\Psi(n,a,b)\Psi\left(\frac{n}{2},a,b\right)\Psi\left(\frac{n}{3},a,b\right)\ldots. \tag{3.5.2}$$

In the special case $b=1$, we write $T(n,a)$ and $\Psi(x,a)$ instead of $T(n,a,1)$ and $\Psi(x,a,1)$. We now estimate $\Psi(x,a)$ from above. For this purpose, we first investigate the expression, first given in [6]

$$P(m,a):=\prod_{p|a}p^{\lfloor\frac{m-1}{p-1}\rfloor}\left(\frac{(a+1)(2a+1)\ldots((m-1)a+1)}{m!}\right),$$

where m can be any positive integer and p is a prime. We have

$$\frac{ka+1}{k+1}\leq a\ (k=1,2,\ldots,m-1),$$

so an upper bound for $P(m,a)$ is

$$P(m,a)\leq\left(\prod_{p|a}p^{\frac{m-1}{p-1}}\right)a^{m-1}=(A_a)^{m-1}, \tag{3.5.3}$$

where

$$A_a:=a\prod_{p|a}p^{\frac{1}{p-1}}. \tag{3.5.4}$$

Furthermore, I claim $P(m,a)$ is a whole number. Let us consider the rational part of $P(m,a)$. Firstly, assume a prime $q\nmid a$, by Lemma 3.14 we have the relation that

$$\nu_q((1+a)(1+2a)\ldots(1+(m-1)a))\geq\sum_{r=1}^{\infty}\left\lfloor\frac{m}{q^r}\right\rfloor=\alpha_q(m).$$

i.e. for a prime q dividing the rational part of $P(m,a)$, its multiplicity appearing in the numerator is at least same as in the denominator. However in the second case that the primes $q\mid a$, we have

$$(q-1)\alpha_q(m)<(q-1)\left(\frac{m}{q}+\frac{m}{q^2}+\frac{m}{q^3}+\ldots\right)=m.$$

Then because $\alpha_q(m)$ is an integer, we can write

$$\begin{aligned}(q-1)\alpha_q(m) &\leq m-1\\ \alpha_q(m) &\leq \frac{m-1}{q-1}\\ \alpha_q(m) &\leq \Big\lfloor \frac{m-1}{q-1} \Big\rfloor.\end{aligned}$$

Therefore, we can say $P(m,a)$ is a whole number and the claim is correct.

Now consider primes q of the form of $ak+1$ belonging to one of the intervals $m < q < ma+1, \sqrt{m} < q < \sqrt{ma+1}, \sqrt[3]{m} < q < \sqrt[3]{ma+1}, \ldots$. These intervals can partly overlap, but q cannot be the intersection of two of these intervals, because then we would have

$$\sqrt[r]{m} < q < \sqrt[r+1]{ma+1}$$

and we would get

$$q = \frac{q^{r+1}}{q^r} < \frac{ma+1}{m} \leq a+1,$$

while $q \equiv 1 \bmod a$ implies $q \geq a+1$. Hence there is no such prime $q = ak+1$ in the intersection of two of these intervals.

Now if $\sqrt[s]{m} < q < \sqrt[s]{ma+1}$, then $v_s(m,q) = 1$. This is because we have $m < q^s < ma+1$, and we also have $q = ak+1$ and $q^s \equiv 1 \bmod a$. If there exists x satisfying $q^s x \equiv 1 \bmod a$, it must $x = 1$. Moreover we have $\left\lfloor \frac{m}{q^s} \right\rfloor = 0$ since $m < q^s$. We now have, in this situation,

$$\nu_q(R(a,m)) > \alpha_q(m) = \nu_q(m!),$$

i.e. $P(m,a)$ is divisible by q. Collecting all such primes q, we have

$$\begin{aligned}Q(m,a) &:= \prod_{r=1}^{\infty} \prod_{\substack{\sqrt[r]{m}<q<\sqrt[r]{ma+1}\\ q\equiv 1 \bmod a}} q\\ &= \prod_{m<q<ma+1} q \prod_{\sqrt{m}<q<\sqrt{ma+1}} q \prod_{\sqrt[3]{m}<q<\sqrt[3]{ma+1}} q \ldots\end{aligned}$$

is a divisor of $P(m,a)$, where q, as well as later in this section, runs through the primes of the form $ak+1$. Because of the relation (3.5.3), then

$$Q(m,a) \leq A^{m-1}.$$

Next we replace the number m successively by

$$m_1 = \left\lceil \frac{m}{a} \right\rceil,\ m_2 = \left\lceil \frac{m}{a^2} \right\rceil, \ldots, m_s = \left\lceil \frac{m}{a^s} \right\rceil = 1 \ \text{ if } a^{s-1} < m \leq a^s,$$

where $\lceil t \rceil$ is the smallest integer number $\geq t$. Next we multiply the resulting inequalities for the $Q(m,a)$ together and we have

$$\begin{aligned} \prod_{r=1}^{\infty} \prod_{q < \sqrt[r]{ma+1}} q &\leq Q(m,a)Q(m_1,a)Q(m_2,a)\ldots Q(m_s,a) \\ &\leq A^{m+m_1+m_2+\ldots+m_s-s-1}, \end{aligned} \tag{3.5.5}$$

where the left hand side of (3.5.5) followed the relation

$$am_{r+1} + 1 \geq a\frac{m}{a^{r+1}} + 1 = \frac{m}{a^r} + 1 > m_r,$$

where $r = 0, 1, 2, \ldots, s-1$ and $m_0 = m$.

Since $q < \sqrt[r]{ma+1}$, then $q^r < ma+1$ and $q^r \leq ma$, so $q \leq \sqrt[r]{ma}$ equivalently. Moreover

$$\begin{aligned} m + m_1 + m_2 \ldots + m_s &\leq m + \frac{m+a-1}{a} + \frac{m+a^2-1}{a^2} + \ldots + \frac{m+a^s-1}{a^s} \\ &= (m-1)\left(1 + \frac{1}{a} + \ldots + \frac{1}{a^s}\right) + s + 1 \\ &< (m-1)\left(\frac{a}{a-1}\right) + s + 1, \end{aligned}$$

therefore, (3.5.5) can be written as

$$\begin{aligned} \Psi(am,a) &= \prod_{q \leq am} q \prod_{q \leq \sqrt{am}} q \prod_{q \leq \sqrt[3]{am}} q \ldots \\ &\leq A_a^{m+m_1+m_2+\ldots+m_s-s-1} \end{aligned}$$

$$< A_a^{\left(\frac{a}{a-1}\right)(m-1)}.$$

Given $x > 0$ (but not necessarily whole number) and if m satisfies

$$a(m-1) < x \leq am,$$

then we have

$$\Psi(x,a) \leq A_a^{\frac{x}{a-1}}. \tag{3.5.6}$$

As an interesting special case, since $A_4 = 4 \cdot 2 = 8$ and we get

$$\Psi(x,4) = \prod_{r=1}^{\infty} \prod_{\substack{q \equiv 1 \bmod 4 \\ q \leq \sqrt[r]{x}}} q \leq 8^{\frac{x}{3}} = 2^x. \tag{3.5.7}$$

Now we apply (3.5.6) to estimate $T(n,a)$ formed from the prime factors of $n!$ with the form $ak+1$. Let q_0 denote the smallest prime of this form and notice that, for $x < q_0,\ \Psi(x,a) = 1$, since it is the empty product. The relation (3.5.2) becomes

$$T(n,a) = \prod_{s \leq \frac{n}{q_0}} \Psi\left(\frac{n}{s}, a\right) \leq A_a^{\frac{n}{a-1}\sum_{s \leq \frac{n}{q_0}} \frac{1}{s}}.$$

Since for all x, there is the inequality

$$\sum_{1 \leq s \leq x} \frac{1}{s} \leq \log x + 1,$$

then we have new estimate

$$T(n,a) \leq A_a^{\frac{n}{a-1}\left(\log \frac{n}{q_0} + 1\right)}. \tag{3.5.8}$$

This is a valuable estimate which may have many uses when studying $n!$, so I state it as a lemma.

Lemma 3.15 *Let*

$$T(n,a) := \prod_{q \equiv 1 \bmod a} q^{\alpha_q(n)}$$

and

$$A_a := a \prod_{p|a} p^{\frac{1}{p-1}},$$

where both n and a are positive integers and greater than 1. Then

$$T(n,a) \leq A_a^{\frac{n}{a-1}\left(\log \frac{n}{q_0}+1\right)},$$

where q_0 is the smallest prime of the form $ak+1$.

3.6 Application of the method of Erdös and Obláth

I will now show how to apply particular factors $T(n,a,b)$ of $n!$, actually $T(n,8)$ and $T(n,6)$, to prove equation $n! = x^p - y^p$ has no solutions in the cases that $p = 8$ and $p = 3$.

For the applications, there are only two special cases, (1) $a = 2p$, p is an odd prime; (2) $a = 8$. In the first case, according to (3.5.4)

$$A_{2p} = 2p \cdot 2 \cdot p^{\frac{1}{p-1}} = 4p^{\frac{p}{p-1}}$$

and

$$q_0 \geq 2p+1 \geq 7,$$

thus

$$T(n,2p) \leq \left(4p^{\frac{p}{p-1}}\right)^{\frac{n}{2p-1}(\log n - \log 7 + 1)}; \tag{3.6.1}$$

in the second case

$$A_8 = 8 \cdot 2 = 16$$

and

$$q_0 = 17,$$

thus

$$T(n,8) \leq 16^{\frac{n}{7}(\log n - \log 17 + 1)}. \tag{3.6.2}$$

3.6.1 The case $p = 8$

Now, we are going to prove the equation

$$n! = x^8 - y^8, \tag{3.6.3}$$

where $(x,\ y) = 1$, has no solutions. Firstly let

$$B_1 = x^4 - y^4,\ B_2 = x^4 + y^4.$$

Because $B_1 < B_2$, we have

$$n! = B_1 B_2 < B_2^2. \tag{3.6.4}$$

Now if an odd prime $p \mid B_2$, then we have $x^4 \equiv -y^4 \bmod p$, which gives $u^4 \equiv -1 \bmod p$ has a solution. Therefore $p \equiv 1 \bmod 8$ follows. Moreover,

$$B_2 \leq 2T(n, 8). \tag{3.6.5}$$

We need the 2 because if x is even and y is odd, then B_2 is odd and $2 \nmid B_2$, while if both x and y are odd, then we have $x^4 + y^4 = 4z + 2$ and $2^1 \parallel B_2$. From (3.6.2) and (3.6.4), we have

$$n! < 4 \cdot 16^{\frac{2n}{7}(\log n - \log 17 + 1)}.$$

Applying the relation

$$2\left(\frac{n}{e}\right)^n < n!,$$

which follows because

$$2\frac{n^n}{n!} = \frac{n^{n-1}}{(n-1)!} + \frac{n^n}{n!} < e^n,$$

then we have

$$2\left(\frac{n}{e}\right)^n < n! < 4 \cdot 16^{\frac{2n}{7}(\log n - \log 17 + 1)},$$

$$\left(\frac{n}{e}\right)^n < 2 \cdot 16^{\frac{2n}{7}(\log n - \log 17 + 1)}.$$

Next taking logarithms, it gives

$$n \log n - n < \log 2 + \frac{8}{7} n \log 2 (\log n - \log 17 + 1).$$

After performing the numerical calculations

$$0.208 n \log n + 0.451 n < 0.694,$$

which is impossible for all $n > 2$. For $n = 1$, (3.6.3) has no solution. Therefore, the difference of the eighth powers of two relatively prime integers is never a factorial.

3.6.2 The case $p = 3$

At last, let us consider the case that $p = 3$ and the equation

$$n! = x^3 - 1, \tag{3.6.6}$$

where $x > 1$. Let

$$B_1 = (x - 1), \quad B_2 = (x^2 + x + 1).$$

In this case, we have

$$B_1^2 \leq B_2, \tag{3.6.7}$$

which is different from [13] and gives a much lower bound for B_1^2. Furthermore,

$$B_2 \leq 3T(n, 6). \tag{3.6.8}$$

Because for all $p \mid x^2+x+1$, we have $p \mid x^3-1$, then by Fermat's Little Theorem, it implies $p \equiv 1 \bmod 3$. However, B_2 is odd as x is odd, so we must have $p \equiv 1 \bmod 6$. As for $p = 3$, since $((x-1), (x^2+x+1)) = ((x-1), 3)$, then we have either their greatest common divisor is 1, which implies $3 \nmid x - 1$ and $3 \nmid x^2 + x + 1$ either, or the GCD is 3 and it implies $3 \mid x-1$ and then $3 \parallel x^2+x+1$ follows. Thus, (3.6.8) is given.

From (3.6.1), (3.6.7) and (3.6.8) we have

$$n!^2 = B_1^2 B_2^2 \leq B_2^3 \leq 3^3 \left(4 \cdot 3^{\frac{3}{2}}\right)^{\frac{3}{5}n(\log n - \log 7 + 1)}. \tag{3.6.9}$$

Again applying the relation

$$2\left(\frac{n}{e}\right)^n < n!,$$

we obtain

$$\frac{2n}{3}(\log n - 1) < \log 3 - \frac{\log 4}{3} + \frac{1}{5}\left(\log 4 + \frac{3}{2}\log 3\right) n(\log n - \log 7 + 1). \tag{3.6.10}$$

However, this is false for all $n \geq 12$. For $n < 12$, we can check and find out there are no solutions for (3.6.6). In conclusion, (3.6.6) has no solutions at all.

Chapter 4

Using the ABC conjecture

4.1 Overview

In this chapter I show how the ABC conjecture can be used to show that each member of a vast set of extensions to Brocard's problem has only a finite number of solutions. Of course the ABC conjecture is just a conjecture so we would say all of these results are **conditional**, i.e. conditional upon the conjecture being true.

While working on this material during 2012, I learned, in late September, of a proposed proof of the ABC conjecture. This is by Shinichi Mochizuki and relies on a lot of unpublished work, so I do not give any references. I am not able to check this proof, since it is over 1000 pages long, and contains many ideas which I would need to understand to check it is correct. However, if the proof is correct, then all of these conditional results will become (unconditional) theorems, with no more work. Through the work of Luca described in this chapter, EACH of the equations $n! = f(x)$, for $f(x) \in \mathbb{Z}[X]$, has at most a finite number of solutions, provided we assume the ABC conjecture.

In this chapter, firstly I state Mason's theorem for polynomials, which is where the idea for the conjecture comes from. Then I will give the statement of the conjecture and some examples of its use in classical problems, Fermat's Last Theorem and Catalan's conjecture. Then I will show how Brocard's problem is proved by Szpiro's conjecture, which is implied by the ABC conjecture, but is unproven yet either. Finally I will give Luca's proof that the equation $n! = f(x)$ where $f(x)$ is

any polynomial with integer coefficients, has at most a finite number of solutions.

4.2 Mason's Theorem

Mason's theorem is about polynomials, which is the polynomial version of the ABC conjecture.

Theorem 4.1 *[37] Let $a(x)$, $b(x)$ and $c(x)$ be three polynomials with no common factors such that*

$$a(x) + b(x) = c(x).$$

Then

$$max\{deg(a), deg(b), deg(c)\} \leq deg(rad(abc)) - 1,$$

where $rad(f)$ is the polynomial of minimum degree that has the same roots of f, so $deg(rad(f))$ gives the number of distinct roots of f.

4.3 the ABC conjecture

Definition The **radical**

$$R(n) := \prod_{p|n} p$$

is the largest square-free divisor of n, or the square-free **core** of n. In particular, $R(1) = 1$.

Definition The **quality** $q(a, b, c)$ of the triple (a, b, c) is

$$q(a, b, c) = \frac{\log(c)}{\log(R(abc))}.$$

A typical triple (a, b, c) of coprime positive integers with $a + b = c$ will have $c < R(abc)$, i.e. $q(a, b, c) < 1$. Triples with $q > 1$ are considered rather special, they consist of numbers divisible by high powers of small prime numbers. The ABC conjecture states that, for any $\varepsilon > 0$, there exist only finitely many triples (a, b, c) of coprime positive integers with $a + b = c$ such that $q(a, b, c) > 1 + \varepsilon$. Whereas it is known that there are infinitely many triples (a, b, c) of coprime positive integers

with $a + b = c$ such that $q(a, b, c) > 1$, the conjecture predicts that only finitely many of those have $q > 1.01$ or $q > 1.001$ or even $q > 1.0001$. Here I give a Table that shows some good examples for the ABC conjecture. The data is taken from [38].

No.	a	b	c	q
1	2	$3^{10} \cdot 109$	23^5	1.62991
2	11^2	$3^2 \cdot 5^6 \cdot 7^3$	$2^{21} \cdot 23$	1.62599
3	$19 \cdot 1307$	$7 \cdot 29^2 \cdot 31^8$	$2^8 \cdot 3^{22} \cdot 5^4$	1.62349
4	283	$5^{11} \cdot 13^2$	$2^8 \cdot 3^8 \cdot 17^3$	1.58076
5	1	$2 \cdot 3^7$	$5^4 \cdot 7$	1.56789
6	7^3	3^{10}	$2^{11} \cdot 29$	1.54708
7	$7^2 \cdot 41^2 \cdot 311^3$	$11^{16} \cdot 13^2 \cdot 79$	$2 \cdot 3^3 \cdot 5^{23} \cdot 953$	1.54443
8	5^3	$2^9 \cdot 3^{17} \cdot 13^2$	$11^5 \cdot 17 \cdot 31^3 \cdot 137$	1.53671
9	$13 \cdot 19^6$	$2^{30} \cdot 5$	$3^{13} \cdot 112 \cdot 31$	1.52700
10	$3^{18} \cdot 23 \cdot 2269$	$17^3 \cdot 29 \cdot 31^8$	$2^{10} \cdot 5^2 \cdot 7^{15}$	1.52216

Table 4.1: The top ten good *abc* examples.

Theorem 4.2 (Asymptotic Fermat Theorem) *[27] There exists $n_0 \in \mathbb{N}$ such that for $\forall n \geq n_0$,*

$$x^n + y^n = z^n$$

has no solutions where $gcd(x, y, z) = 1$.

Theorem 4.3 *[27] The ABC conjecture implies the Asymptotic Fermat Theorem.*

Proof. Let x, y, z be relatively prime. Then we have

$$R(x^n y^n z^n) = R(xyz) \leq xyz \leq z$$

since $x < z$ and $y < z$. Applying the ABC conjecture with $\varepsilon = 1$, then

$$z^n = max(x^n, y^n, z^n) \leq K_1 R(x^n y^n z^n)^2 \leq K_1 z^6,$$

by taking logarithms we have

$$n \log z \leq \log K_1 + 6 \log z,$$

which implies

$$n \leq 6 + \frac{\log K_1}{\log z} \leq 6 + \frac{\log K_1}{\log 3}.$$

Therefore, let $n_0 = 7 + \frac{\log K_1}{\log 3}$ and then for any $n > n_0$, there are no solutions for this diophantine equation. □

Theorem 4.4 *[7]* **Catalan Conjecture** *The only solution in the natural numbers of*

$$x^m - y^n = 1$$

for $x, m, y, n > 1$ is $x = 3, a = 2, y = 2, b = 3$. That is $3^2 - 2^3 = 1$, and 8 and 9 are the only consecutive powers.

Many special cases of this conjecture have been proved, for example: $x^2 - y^n = 1$ has only one solution, that is $x = n = 3$ and $y = 2$; $x^m - y^2 = 1$ has no solutions. So we need only focus on the case $m,\ n > 3$. The completion of the proof of Catalan's conjecture was done by Preda Mihailescu in April 2002 [26], so it is now sometimes called Mihailescu's theorem.

Theorem 4.5 *[27] The ABC conjecture implies the Catalan equation has only a finite number of solutions.*

Proof. Say (x, y, m, n) be a solution with $m,\ n \geq 3$. Then we have $(x, y) = 1$, if not, $p \mid x$ and $p \mid y$ lead to $p \mid 1$. Let $\varepsilon = \frac{1}{4}$ in the ABC conjecture, then there exists $K_{1/4}$, say K such that $max(|a|, |b|, |c|) \leq KR(abc)^{5/4}$. Since there is $x^m = 1 + y^n$, then we have

$$\begin{aligned} y^n < x^m &\leq KR(1 \cdot x^m \cdot y^n)^{5/4} \\ &= KR(xy)^{5/4} \\ &\leq K(xy)^{5/4}. \end{aligned}$$

By taking logarithms, it leads to

$$\begin{aligned} m \log x &\leq \log K + \frac{5}{4}(\log x + \log y), \\ n \log y &< \log K + \frac{5}{4}(\log x + \log y), \end{aligned}$$

and then we have

$$m\log x + n\log y \leq 2\log K + \frac{5}{2}(\log x + \log y),$$

$$(m - \frac{5}{2})\log x + (n - \frac{5}{2})\log y < 2\log K.$$

However, $x,\ y \geq 2$, so it gives

$$(m - \frac{5}{2})\log 2 + (n - \frac{5}{2})\log 2 < (m - \frac{5}{2})\log x + (n - \frac{5}{2})\log y < 2\log K,$$

thus we have

$$m + n < \frac{2\log K}{\log 2} + 5,$$

and $m + n$ is bounded. In conclusion, there are only finitely many exponents m and n for which $x^m - y^n = 1$ has a solution. Also it is known that, for fixed $m,\ n$ Catalan's equation has only a finite set of solutions x, y, therefore the number of set (x, y, m, n) is finite. □

4.4 The ABC conjecture applied to Brocard's problem and variations

First I give the simple proof that Szpiro's conjecture implies Brocard's problem has only a finite number of solutions. It is really an exercise.

Proposition 4.6 *[29] Assume that Szpiro's conjecture is true, then there are only a finite number of solutions of* $n! + 1 = m^2$.

Proof. Obviously, m is an odd number since $n!$ is always an even number except for $n = 1$, while there are no solutions for this equation when $n = 1$. So m can be written as $2k + 1$, which gives $n! = 4k(k + 1)$. Therefore, $n \geq 4$ since $k \geq 1$. Now let $a = 1,\ b = k,\ c = k + 1$ such that $a + b = c$, then the Szpiro's conjecture indicates that

$$n^n e^{-n} \leq \frac{n!}{4} = k(k + 1)$$

$$\begin{aligned} n^n e^{-n} &\leq (R(k(k+1)))^s \\ &= \left(R\left(\frac{n!}{4}\right)\right)^s = (\prod_{p\leq n} p)^s \\ &\leq 4^{ns}, \end{aligned}$$

Hence, $n \leq 4^s e$ and there is an upper bound for n. This completes the proof. □

Next we are going to generalize the result from above and show that, assuming the ABC conjecture, the diophantine equation

$$P(x) = n! \tag{4.4.1}$$

has only finitely many integer solutions (x, n), where $n > 0$ and $P(x)$ is an arbitrary polynomial with integer coefficients of degree $d \geq 2$. This is strong evidence that Brocard's equation, and each of the other equations considered in this thesis, have at most a finite number of solutions. By transforming and reducing a given general polynomial, I will rewrite the original polynomial. In the new equation, after making sure that the three terms $A,\ B,\ C$ are coprime, I will use the ABC conjecture and do some calculations, then find out an upper bound for n. This is more difficult than Proposition 4.6.

Proposition 4.7 *[21] Let $P(X) \in \mathbb{Z}[X]$ be a polynomial of degree $d \geq 2$. Assume the ABC conjecture is true. Then there are only a finite number of solutions (x, n) for $P(x) = n!$.*

Proof. Let $P(X)$ be given by

$$P(X) := a_0 X^d + a_1 X^{d-1} + \ldots + a_d \text{ where } a_i \in \mathbb{Z}. \tag{4.4.2}$$

Then (4.4.1) can be written as

$$a_0 x^d + a_1 x^{d-1} + \ldots + a_d = n!. \tag{4.4.3}$$

Let $c := d^d a_0^{d-1}$, $y := a_0 dx$ and $b_i := d^i a_0^{i-1} a_i$ for $i = 1, 2, \ldots, d$. Now multiply both sides of (4.4.3) by $d^d a_0^{d-1}$. Then the coefficient of the first term is 1 in a new

expression

$$y^d + b_1 y^{d-1} + \ldots + b_d = cn!. \tag{4.4.4}$$

If we change the variable into $z := y + a_1$ and then the second term with the power $d-1$ will disappear. So we can rewrite (4.4.4) as

$$z^d + c_2 z^{d-2} + \ldots c_d = cn!, \tag{4.4.5}$$

and then we have the polynomial $Q(X) \in \mathbb{Z}[X]$

$$Q(X) := X^d + c_2 X^{d-2} + \ldots + c_d, \tag{4.4.6}$$

where c_i represents some integers that depend on the a_i.

Now assume that $|z|$ is sufficiently large, then we have

$$\frac{|z|^d}{2} < |Q(z)| < 2|z|^d. \tag{4.4.7}$$

To see this, because

$$Q(z) := z^d + c_2 z^{d-2} + \ldots c_d = z^d + O(z^{d-2}),$$

using the O notation. Then there exists a positive number M such that

$$|z^d| - M|z^{d-2}| \leq |z^d + O(z^{d-2})| \leq |z^d| + M|z^{d-2}|,$$

$$|z|^d \left(1 - \frac{M}{|z|^2}\right) \leq Q(z) \leq |z|^d \left(1 + \frac{M}{|z|^2}\right),$$

when $|z|$ is sufficiently large, which leads to (4.4.7). Now by using (4.4.5), we get

$$\frac{|z|^d}{2} < |cn!| < 2|z|^d, \tag{4.4.8}$$

so

$$\frac{|z|^d}{2n!} < |c| < \frac{2|z|^d}{n!},$$

then take logarithms to get

$$\log(|z|^d) - \log(n!) - \log 2 < \log|c| < \log(|z|^d) - \log(n!) + \log 2,$$

therefore

$$\log\left(\frac{|c|}{2}\right) < \log(|z|^d) - \log(n!) < \log(2|c|).$$

As we know, $c := d^d a_0^{d-1}$ and $d \geq 2$. It then follows that there exist constants C_1 and C_2 such that for any $(z,\ n)$ as a solution of (4.4.5),

$$|d\log|z| - \log(n!)| < C_1 \text{ for } |z| > C_2. \tag{4.4.9}$$

From now on, we use C_i for $i = 1, 2, \ldots$ to represent positive constants depending directly or indirectly only on the coefficients a_i of the polynomial $P(X)$. We may also assume that C_2 is large enough with respect to C_1 such that whenever z and n are integers with $|z| > C_2$ satisfying (4.4.9), then $n > c$ by choosing C_2 sufficiently large. Briefly speaking, if $n \leq c$ follows in this case, (4.4.8) indicates that z has an upper bound. Provided that C_2 is any positive number but larger than this bound, then $n \leq c$ cannot be satisfied, so we can assume $c < n$. The reason for this assumption will become clear below.

Now let $Q_1(X) \in \mathbb{Z}[X]$ be a polynomial such that

$$Q(X) = X^d + Q_1(X). \tag{4.4.10}$$

If $Q_1(X) = 0$, then (4.4.5) reduces to

$$z^d = cn! \tag{4.4.11}$$

I claim that there are no integer solutions (z, n) when $n > 2c$. Because if $n > 2c$, then for any prime $p \in (n/2, n)$ we have $p > c$. Therefore, the exponent of such a prime can only be 1 and $cn!$ cannot be written as a perfect power ≥ 2. Hence, it implies that there exists an upper bound for n, i.e. $n \leq 2c$, and (4.4.1) has only finitely many solutions in this case.

Now let us pay attention to a more interesting case when $Q_1(X) \neq 0$. To make sure that the constant term of the polynomial $Q(X)$ or $Q_1(X)$ is not zero, divide both sides of (4.4.5) by z^{d-j} to get

$$z^j + c_2 z^{j-2} + \ldots + c_j = \frac{cn!}{z^{d-j}}, \tag{4.4.12}$$

where $2 \leq j \leq d$ is the largest integer with $c_j \neq 0$. Let $Q_2(X) \in \mathbb{Z}[X]$ be the polynomial

$$Q_2(X) := \frac{Q_1(X)}{X^{d-j}} = c_2 X^{j-2} + \ldots + c_j, \tag{4.4.13}$$

then (4.4.12) can be rewritten as

$$z^j + Q_2(z) = \frac{cn!}{z^{d-j}}. \tag{4.4.14}$$

In a similar way as we did before, we can get

$$|c_2 z^{j-2}| - M|z^{j-3}| < |Q_2(z)| \leq |c_2 z^{j-2}| + M|z^{j-3}|,$$

$$0 < |Q_2(z)| < C_3|z|^{j-2}, \quad \text{for } |z| > C_4 \geq C_2. \tag{4.4.15}$$

where we can take $C_3 := |c_2| + 1$.

Let $D := gcd(z^j, Q_2(z))$. Obviously, it implies that D divides z, so D must divide c_j in the equation (4.4.13). By dividing both sides of (4.4.14) by D, we get

$$\frac{z^j}{D} + \frac{Q_2(z)}{D} = \frac{cn!}{z^{d-j}D}. \tag{4.4.16}$$

Let $A := \frac{z^j}{D}, B := \frac{Q_2(z)}{D}$ and $C := \frac{cn!}{(z^{d-j}D)}$. Now by the ABC conjecture to (4.4.15), we get

$$\max(|A|, |B|, |C|) < C_5 R \left(\frac{z^j Q_2(z) cn!}{D^3 z^{d-j}} \right)^{1+\varepsilon}.$$

So we have

$$\frac{|z|^j}{D} < C_5 R \left(\frac{z^j Q_2(z) cn!}{D^3 z^{d-j}} \right)^{1+\varepsilon}, \tag{4.4.17}$$

where C_5 depends only on ε. Because we have the three inequalities as follow:

$$R\left(\frac{z^j}{D}\right) \leq R(z^j) \leq |z|; \tag{4.4.18}$$

$$R\left(\frac{Q_2(z)}{D}\right) \leq \frac{|Q_2(z)|}{D} < \frac{C_3|z|^{j-2}}{D}; \tag{4.4.19}$$

$$R\left(\frac{cn!}{Dz^{d-j}}\right) \leq R(cn!) = R(n!) = \prod_{p\leq n} p < 4^n, \text{ for } n > c. \tag{4.4.20}$$

The last of the chain of inequalities follows from Prime Counting Function $\pi(n) \approx \frac{n}{\log n}$. From (4.4.18)-(4.4.20), we have

$$R\left(\frac{z^j Q_2(z) cn!}{D^3 z^{d-j}}\right) \leq R\left(\frac{z^j}{D}\right) R\left(\frac{Q_2(z)}{D}\right) R\left(\frac{cn!}{Dz^{d-j}}\right) < \frac{C_3|z|^{j-1}4^n}{D}. \tag{4.4.21}$$

From (4.4.17) and (4.4.21), we get

$$\frac{|z|^j}{D} < C_6 \left(\frac{|z|^{j-1}4^n}{D}\right)^{1+\varepsilon},$$

where $C_6 := C_5 C_3^{1+\varepsilon}$. Then we have

$$|z|^j < C_6 \frac{(|z|^{j-1}4^n)^{1+\varepsilon}}{D^\varepsilon} \leq C_6 |z|^{(j-1)(1+\varepsilon)} 4^{n(1+\varepsilon)},$$

which implies

$$|z|^{1+\varepsilon-\varepsilon j} < C_6 4^{n(1+\varepsilon)}. \tag{4.4.22}$$

Since ε can be any positive number, then we suppose $\varepsilon := \frac{1}{2d} \leq \frac{1}{2j}$. Next we get the following inequalities

$$0 < \varepsilon \leq \frac{1}{2j} \leq \frac{1}{2},$$
$$-\frac{1}{2} \leq -\varepsilon j < 0 \text{ as } \varepsilon > 0,\ j \geq 1.$$

Now it gives (4.4.22) a lower bound, that is

$$|z|^{1/2} < |z|^{1+\varepsilon-\varepsilon j} < C_6 4^{n(1+\varepsilon)}.$$

By taking logarithms, we get

$$\log|z| < C_7 n + C_8, \tag{4.4.23}$$

where $C_7 := 2(1+\varepsilon)\log 4$ and $C_8 := 2\log C_6$. Now multiply both sides by d to get,

$$d\log|z| < C_9 n + C_{10}, \tag{4.4.24}$$

where $C_9 := dC_7$ and $C_{10} := dC_8$. Combining (4.4.9) and (4.4.24), we get

$$\log(n!) < C_1 + d\log|z| < C_9 n + C_{11},$$

where $C_{11} := C_1 + C_{10}$. The inequality $n\log n - n < \log n!$ satisfying the Stirling's formula is applied here, which implies that

$$n\log n - n < C_9 n + C_{11}.$$

Therefore, $n < C_{12}$, i.e. n has an upper bound. And $|z| < C_{13}$ follows. Therefore both n and z do have an upper bound, so it follows that (4.4.1) has only finitely many integer solutions (x, n). □

Chapter 5

The work of Pollack and Shapiro

5.1 Overview

In this chapter I will describe the work of Richard Pollack and Harold Shapiro given in [30]. In fact, it is indicated in [13] that the diophantine equation

$$n! = x^4 - y^4 \tag{5.1.1}$$

has no solutions, which is proved in a similar way as the case $p = 8$. Briefly speaking, since we have

$$n! = (x^2 + y^2)(x^2 - y^2),$$

then

$$B_2 := x^2 + y^2 \leq 2T(n, 4, 1)$$

and

$$B_1 := x^2 - y^2 \geq 2^{\alpha_2(n)-1} T(n, 4, 3)$$

follow. Also because $B_1 < B_2$, we have

$$2^{\alpha_2(n)} T(n, 4, 3) < 4T(n, 4, 1),$$

After some more work, it implies that

$$n \log 2 - \log 8n < n \sum_{q^r \leq n} \frac{\chi(q^r) \log q}{q^r} + \sum_{\substack{q \equiv 3 \bmod 4 \\ q^r \leq n}} \log q, \tag{5.1.2}$$

where q is a prime and $\chi(q^r)$ is defined later. The first sum of the right side of (5.1.2) is negative when n is sufficiently large, which will be shown below, and the second sum is approximately $\frac{n}{2}$, which gives a contradiction when n becomes sufficiently large. Therefore, we have (5.1.1) has no solutions only for sufficiently large n. It follows that, we have

$$n! = x^4 - 1 \tag{5.1.3}$$

has no solutions for sufficiently large n. But we do not have any bound on the number of solutions to (5.1.3) by the conclusion of Erdös and Obláth, because we cannot have an explicit value for n. Pollack and Shapiro showed that (5.1.3) had no solutions at all. Their work is quite sophisticated, and it also relies on the "second order" difference in the number of primes in the two progressions $(4n + 1)$ and $(4n + 3)$. The reader will recall that, by Dirichlet's theorem, there are asymptomatically up to $x > 0$, $\pi(x)/2$ in each of these progressions as $x \to \infty$. Its all set out in [30].

Note that

$$\sum_{q^r \leq n} \frac{\chi(q^r) \log q}{q^r} = -\left(\frac{\log 3}{3} - \frac{\log 5}{5}\right) - \left(\frac{\log 7}{7} - \frac{\log 9}{9}\right) - \ldots < 0, \tag{5.1.4}$$

which illustrates the first sum of (5.1.2).

5.2 Dirichlet L-functions

A Dirichlet L-function is a series of the form

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

where χ is a Dirichlet Character and s is a complex variable with real part greater than 1. A Dirichlet Character is a completely multiplicative function $\chi : \mathbb{Z} \to \mathbb{C}$, with a fixed modulus $k > 1$, such that $\chi(n) = 0$ if $(n, k) \neq 1$, and $|\chi(n)| = 1$ for all n with $(n, k) = 1$ as well as $\chi(n + k) = \chi(n)$.

The Dirichlet L-function that is applied in the proof of Richard Pollack and Harold Shapiro is

$$L_1 = \sum_n \frac{\chi(n)}{n}, \tag{5.2.1}$$

where the Dirichlet character in this case has $\mathbb{R}$ values and $k = 4$. It is defined by

$$\chi(n) = \begin{cases} 0 & \text{if } n \text{ is even,} \\ 1 & \text{if } n \equiv 1 \bmod 4, \\ -1 & \text{if } n \equiv 3 \bmod 4. \end{cases}$$

Note that as n goes to infinity, the Dirichlet L-series L_1 is a well-known alternating series, the Leibniz series, which is convergent to $\frac{\pi}{4}$. In brief,

$$\begin{aligned} \frac{\pi}{4} = \arctan(1) &= \int_0^1 \frac{1}{1+x^2}\,dx \\ &= \int_0^1 \left(\sum_{k=0}^{n} (-1)^k x^{2k} + \frac{(-1)^{n+1} x^{2n+2}}{1+x^2} \right) dx \\ &= \sum_{k=0}^{n} \frac{(-1)^k}{2k+1} + (-1)^{n+1} \int_0^1 \frac{x^{2n+2}}{1+x^2}\,dx. \end{aligned}$$

As for the integral in the last line, we have:

$$0 < \int_0^1 \frac{x^{2n+2}}{1+x^2}\,dx \;<\; \int_0^1 x^{2n+2}\,dx \;=\; \frac{1}{2n+3} \;\to\; 0 \quad \text{as } n \to \infty.$$

Therefore, as $n \to \infty$ we are left with the Leibniz series

$$\sum_{k=0}^{\infty} \frac{(-1)^k}{2k+1} \;=\; \frac{\pi}{4}.$$

5.3 Preliminary results

Before we prove that $n! + 1 = x^4$ has no integer solutions, there is a long road we need to travel, that is to understand some preliminary results which are interesting and definitely important to our purpose. I will show how each lemma ingeniously leads on to the next one, and also give more explanation that do not appear in their article, which may be more straightforward to understand, and thus easier for readers.

5.3.1 A lower bound for a special character sum

Now follow me and start our first goal— to derive a constant C which is the lower bound in the inequality

$$L_1 \sum_{n \le x} \frac{\chi(n)\mu(n)}{n} \ge C, \tag{5.3.1}$$

where x needs to be sufficiently large. The following lemmas show how this can be done.

Lemma 5.1 *If we define*

$$Q(x) := \sum_{\substack{n \le x \\ (n,2)=1}} |\mu(n)|, \tag{5.3.2}$$

then we have, for all $x \ge 10^4$*,*

$$\frac{Q(x)}{x} \le \frac{4}{\pi^2} + 0.0075 = \beta. \tag{5.3.3}$$

Proof. Using a well-known formula for $|\mu(n)|$, we have

$$\begin{aligned} Q(x) &= \sum_{\substack{n \le x \\ (n,2)=1}} \left(\sum_{d^2 | n} \mu(d) \right) \\ &= \sum_{\substack{d \le \sqrt{x} \\ (d,2)=1}} \mu(d) \left(\left\lfloor \frac{x}{d^2} \right\rfloor - \left\lfloor \frac{x}{2d^2} \right\rfloor \right), \end{aligned}$$

Since $\{z\}$ denotes the fractional part of z, we have

$$\left| \{z\} - \left\{ \frac{1}{2} z \right\} \right| \le \frac{1}{2},$$

which gives

$$\begin{aligned}
Q(x) &= \sum_{\substack{d\le\sqrt{x}\\(d,2)=1}} \mu(d)\left(\left(\frac{x}{d^2}-\left\{\frac{x}{d^2}\right\}\right)-\left(\frac{x}{2d^2}-\left\{\frac{x}{2d^2}\right\}\right)\right)\\
&= \sum_{\substack{d\le\sqrt{x}\\(d,2)=1}} \mu(d)\left(\left(\frac{x}{d^2}-\frac{x}{2d^2}\right)-\left(\left\{\frac{x}{d^2}\right\}-\left\{\frac{x}{2d^2}\right\}\right)\right)\\
&= \frac{x}{2}\sum_{\substack{d\le\sqrt{x}\\(d,2)=1}} \frac{\mu(d)}{d^2}-\sum_{\substack{d\le\sqrt{x}\\(d,2)=1}} \mu(d)\left(\left\{\frac{x}{d^2}\right\}-\left\{\frac{x}{2d^2}\right\}\right)\\
&\le \frac{x}{2}\sum_{\substack{d\le\sqrt{x}\\(d,2)=1}} \frac{\mu(d)}{d^2}+\frac{1}{2}\sum_{\substack{d\le\sqrt{x}\\(d,2)=1}} \mu(d)\\
&\le \frac{x}{2}\sum_{\substack{d\le\sqrt{x}\\(d,2)=1}} \frac{\mu(d)}{d^2}+\frac{1}{2}Q(\sqrt{x}). \qquad (5.3.4)
\end{aligned}$$

Also, since

$$\begin{aligned}
\sum_{\substack{d\le\sqrt{x}\\(d,2)=1}} \frac{\mu(d)}{d^2} &= \sum_{\substack{d\ge1\\(d,2)=1}} \frac{\mu(d)}{d^2}-\sum_{\substack{d>\sqrt{x}\\(d,2)=1}} \frac{\mu(d)}{d^2}\\
&= \sum_{d\ge1} \frac{\mu(d)}{d^2}-\sum_{\substack{d\ge1\\(d,2)=1}} \frac{\mu(d)}{d^2}-\sum_{\substack{d>\sqrt{x}\\(d,2)=1}} \frac{\mu(d)}{d^2}\\
&= \sum_{d\ge1} \frac{\mu(d)}{d^2}-\sum_{\substack{d\ge1\\(d,2)=1}} \frac{\mu(2d)}{(2d)^2}-\sum_{\substack{d>\sqrt{x}\\(d,2)=1}} \frac{\mu(d)}{d^2}\\
&= \sum_{d\ge1} \frac{\mu(d)}{d^2}-\sum_{\substack{d\ge1\\(d,2)=1}} \frac{\mu(2)\mu(d)}{4d^2}-\sum_{\substack{d>\sqrt{x}\\(d,2)=1}} \frac{\mu(d)}{d^2}\\
&= \sum_{d\ge1} \frac{\mu(d)}{d^2}+\frac{1}{4}\sum_{\substack{d\ge1\\(d,2)=1}} \frac{\mu(d)}{d^2}-\sum_{\substack{d>\sqrt{x}\\(d,2)=1}} \frac{\mu(d)}{d^2}\\
&= \frac{6}{\pi^2}+\frac{1}{4}\sum_{\substack{d\ge1\\(d,2)=1}} \frac{\mu(d)}{d^2}-\sum_{\substack{d>\sqrt{x}\\(d,2)=1}} \frac{\mu(d)}{d^2}\\
&= \frac{8}{\pi^2}-\sum_{\substack{d>\sqrt{x}\\(d,2)=1}} \frac{\mu(d)}{d^2}, \qquad (5.3.5)
\end{aligned}$$

where I used the known sum $\sum_{d\ge1}\frac{\mu(d)}{d^2}=\frac{1}{\zeta(2)}=\frac{6}{\pi^2}$.

Also because

$$\Big|\sum_{\substack{d>\sqrt{x}\\(d,2)=1}}\frac{\mu(d)}{d^2}\Big| \le 2\int_{\sqrt{x}}^{\infty}\frac{Q(u)}{u^3}du, \tag{5.3.6}$$

where we use Theorem 1.5. Then divide (5.3.4) by x and apply (5.3.5), (5.3.6). We get

$$\begin{aligned}\frac{Q(x)}{x} &\le \frac{1}{2}\sum_{\substack{d\le\sqrt{x}\\(d,2)=1}}\frac{\mu(d)}{d^2}+\frac{1}{2}\frac{Q(\sqrt{x})}{x}\\ &\le \frac{4}{\pi^2}-\frac{1}{2}\sum_{\substack{d>\sqrt{x}\\(d,2)=1}}\frac{\mu(d)}{d^2}+\frac{1}{2}\frac{Q(\sqrt{x})}{x}\\ &\le \frac{4}{\pi^2}+\int_{\sqrt{x}}^{\infty}\frac{Q(u)}{u^3}du+\frac{1}{2}\frac{Q(\sqrt{x})}{x}. \end{aligned}\tag{5.3.7}$$

Because of the estimate $Q(u)\le\frac{1}{2}u$ that is valid for $u\ge 4$, (5.3.7) can be written as

$$\frac{Q(x)}{x}\le\frac{4}{\pi^2}+\frac{3}{4\sqrt{x}}, \tag{5.3.8}$$

Hence for all $x\ge 10^4$, we can have the inequality (5.3.3). □

Lemma 5.2 *For any real number $x\ge 1$,*

$$\Big|\sum_{n\le x}\frac{\chi(n)}{n}-L_1\Big|<\frac{1}{x}. \tag{5.3.9}$$

Proof. Since

$$L_1=\sum_{n}\frac{\chi(n)}{n}=\sum_{n\le x}\frac{\chi(n)}{n}+\sum_{n>x}\frac{\chi(n)}{n},$$

and also

$$\begin{aligned}\Big|\sum_{n>x}\frac{\chi(n)}{n}\Big| &= \Big|\sum_{n>\lfloor x\rfloor}\frac{\chi(n)}{n}\Big|\\ &= \Big|\frac{\pi}{4}-\sum_{n\le\lfloor x\rfloor}\frac{\chi(n)}{n}\Big|\\ &= \Big|\frac{\pi}{4}-1+\frac{1}{3}-\ldots\pm\frac{\chi(\lfloor x\rfloor)}{\lfloor x\rfloor}\Big|\\ &\le \frac{1}{\lfloor x\rfloor+1}\\ &< \frac{1}{x},\end{aligned}$$

which followed from Leibniz's test. Therefore we have

$$\Big|\sum_{n\le x}\frac{\chi(n)}{n}-L_1\Big|=\Big|\sum_{n>\lfloor x\rfloor}\frac{\chi(n)}{n}\Big|<\frac{1}{x}.$$

□

Now, using Lemma 5.1 and Lemma 5.2, let us derive the upper bound and achieve our objective.

Lemma 5.3 *For all $x \ge 10^4$, we have*

$$L_1\sum_{n\le x}\frac{\chi(n)\mu(n)}{n}\ge 1-\beta, \tag{5.3.10}$$

for the value of β given by (5.3.3).

Proof. Define

$$\alpha(n):=\frac{\chi(n)}{n}$$

and

$$G(x):=\sum_{n\le x}\frac{\chi(n)}{n}.$$

Also let $F(x)$ be the identity function, so

$$F(x):=1.$$

By Theorem 1.8, we have

$$F(x)=\sum_{n\le x}\mu(n)\alpha(n)G\left(\frac{x}{n}\right),$$

so there follows the equation

$$\sum_{n\le x}\alpha(n)\mu(n)G\left(\frac{x}{n}\right)=\sum_{n\le x}\frac{\chi(n)\mu(n)}{n}\sum_{m\le x/n}\frac{\chi(m)}{m}=1. \tag{5.3.11}$$

Applying (5.3.9) and (5.3.3), we have

$$\begin{aligned}\sum_{n\le x}\frac{\chi(n)\mu(n)}{n}\sum_{m\le x/n}\frac{\chi(m)}{m} &\le \sum_{n\le x}\frac{\chi(n)\mu(n)}{n}\left(L_1+\frac{n}{x}\right)\\ &\le L_1\sum_{n\le x}\frac{\chi(n)\mu(n)}{n}+\frac{1}{x}\sum_{n\le x}\chi(n)\mu(n)\\ &\le L_1\sum_{n\le x}\frac{\chi(n)\mu(n)}{n}+\frac{1}{x}\sum_{\substack{n\le x\\(n,2)=1}}|\mu(n)|\\ &= L_1\sum_{n\le x}\frac{\chi(n)\mu(n)}{n}+\frac{1}{x}Q(x)\\ &\le L_1\sum_{n\le x}\frac{\chi(n)\mu(n)}{n}+\beta.\end{aligned}$$

Therefore we have

$$1\le L_1\sum_{n\le x}\frac{\chi(n)\mu(n)}{n}+\beta,$$

$$1-\beta\le L_1\sum_{n\le x}\frac{\chi(n)\mu(n)}{n}. \tag{5.3.12}$$

This completes the proof. □

5.3.2 Preparing to estimate a sum

The objective of this section is to obtain an upper bound for the sum

$$\sum_{n\le x}\frac{\Lambda(n)\chi(n)}{n},$$

where $\Lambda(n)=\log p$, if $n=p^k$ for some primes p and integers $k\ge 1$, and $\Lambda(n)=0$ otherwise. This is called the von Mangoldt function after German mathematician Hans von Mangoldt discovered it. As the Dirichlet character $\chi(n)$ is defined at Section 5.2, which is sorted according to a number congruent to 1 or 3 modulo 4, then I will show that for $n\equiv 1 \bmod 4$, there is an upper bound for the sum

$$\sum_{\substack{n\le x\\ n\equiv 1 \bmod 4}}\frac{\Lambda(n)}{n},$$

which is followed by the upper bound for $\sum_{n\le x}\frac{\Lambda(n)\chi(n)}{n}$.

Lemma 5.4 *For all integers $x \geq 10^4$, we have*

$$\frac{1}{x} \sum_{\substack{n \leq x \\ (n,2)=1}} |\mu(n)| \log\left(\frac{x}{n}\right) \leq \beta + 0.0075 \tag{5.3.13}$$

where β is given in (5.3.3).

Proof. Let

$$f(n) := |\mu(n)| \quad \text{where } n \text{ is odd,}$$

then

$$Q(x) = \sum_{\substack{n \leq x \\ (n,2)=1}} f(n) = \sum_{\substack{n \leq x \\ (n,2)=1}} |\mu(n)|.$$

Also let

$$g(n) := \log n.$$

By Theorem 1.9, we have, if x is a positive integer

$$Q(x)\log(1+\frac{1}{x}) + \sum_{\substack{n \leq x \\ (n,2)=1}} |\mu(n)| \log\left(\frac{x}{n}\right) = \sum_{d=1}^{x} Q(d) \log\left(1+\frac{1}{d}\right) \tag{5.3.14}$$

for all positive integers x. Because

$$\log(1+t) \leq t \quad \text{for } 0 < t \leq 1,$$

then it yields

$$\sum_{d=1}^{x} Q(d) \log\left(1+\frac{1}{d}\right) \leq \sum_{d=1}^{x} \frac{Q(d)}{d}.$$

Therefore (5.3.14) can be written as

$$\begin{aligned} \sum_{\substack{n \leq x \\ (n,2)=1}} |\mu(n)| \log\left(\frac{x}{n}\right) &= \sum_{d=1}^{x-1} Q(d) \log\left(1+\frac{1}{d}\right) \\ &< \sum_{d=1}^{x} Q(d) \log\left(1+\frac{1}{d}\right) \\ &\leq \sum_{d=1}^{x} \frac{Q(d)}{d}. \end{aligned} \tag{5.3.15}$$

For $x \geq 10^4$, using (5.3.8), it gives

$$\begin{aligned}\sum_{d=1}^{x} \frac{Q(d)}{d} &\leq \sum_{d=1}^{x} \left(\frac{4}{\pi^2} + \frac{3}{4\sqrt{d}}\right) \\ &\leq \frac{4}{\pi^2}x + \frac{3}{2}\sqrt{x} \\ &\leq x(\beta + 0.0075).\end{aligned}$$

Then (5.2.11) follows and we complete this proof. □

Lemma 5.5 *The sum*

$$M = \sum_{n=1}^{\infty} \frac{\chi(n)\log n}{n} \tag{5.3.16}$$

converges, and

$$\left|M - \sum_{n\leq x} \frac{\chi(n)\log n}{n}\right| < \frac{\log x}{x} \tag{5.3.17}$$

for all real $x \geq e$.

Proof. Since $\sum_{n=1}^{\infty} \frac{\chi(n)\log n}{n}$ is an alternating series, where $\frac{\log n}{n}$ is non-negative and approaches 0 as n approaches infinity, as well as the absolute value of the sequence $\frac{\log n}{n}$ is monotonically decreasing, then by employing Leibniz's test we get,

$$\left|M - \sum_{n\leq x} \frac{\chi(n)\log n}{n}\right| < \frac{\log(\lfloor x\rfloor + 1)}{\lfloor x\rfloor + 1} < \frac{\log x}{x}.$$

□

Now applying Lemma 5.4 and Lemma 5.5, let us prove the following lemma and achieve our first goal.

Lemma 5.6 *For all integers $x \geq e \cdot 10^4$, we have*

$$\sum_{n\leq x} \frac{\Lambda(n)\chi(n)}{n} \leq 0.277. \tag{5.3.18}$$

Proof. Since

$$\Lambda(n) = \sum_{d|n} \mu(d)\log\frac{n}{d},$$

then we have

$$\sum_{n\le x}\frac{\Lambda(n)\chi(n)}{n}=\sum_{d\le x}\frac{\mu(d)\chi(d)}{d}\sum_{m\le x|d}\frac{\chi(m)\log m}{m}. \tag{5.3.19}$$

Noting that, for $z\le e$,

$$\sum_{m\le z}\frac{\chi(m)\log m}{m}=0.$$

So for (5.3.19), it is valid only when for $\frac{x}{d}\ge e$, then apply (5.3.17), we have

$$\sum_{m\le x/d}\frac{\chi(m)\log m}{m}<M+\frac{\log(x/d)}{x/d},$$

and (5.3.19) can be written as

$$\begin{aligned}\sum_{n\le x}\frac{\Lambda(n)\chi(n)}{n}&<\sum_{d\le x}\frac{\mu(d)\chi(d)}{d}\left(M+\frac{\log(x/d)}{x/d}\right)\\&<M\sum_{d\le x|e}\frac{\mu(d)\chi(d)}{d}+\frac{1}{x}\sum_{\substack{d\le x|e\\(d,2)=1}}|\mu(d)|\log\frac{x}{d}.\end{aligned} \tag{5.3.20}$$

Applying (5.3.13) and (5.3.10) for the first and second sum of (5.3.20), respectively, we have for $x\ge e\cdot 10^4$,

$$\sum_{n\le x}\frac{\Lambda(n)\chi(n)}{n}\le\frac{M}{L_1}(1-\beta)+\beta+0.0075. \tag{5.3.21}$$

Note that $M<0$ and (5.1.4) has shown it.

Since $3.1415924\le\pi\le 3.1415928$ and $L_1=\frac{1}{4}\pi$, then we have

$$0.7853981\le L_1\le 0.7853982. \tag{5.3.22}$$

As for the estimate for M, [30] shows that allowing for possible round off errors, it is a conservative estimate that

$$M<-0.192. \tag{5.3.23}$$

Next consider β, since $0.40528470 \leq \frac{4}{\pi^2} \leq 0.40528476$, then we have

$$0.41278470 \leq \beta \leq 0.41278476,$$

so

$$1 - \beta \geq 0.58721524.$$

Therefore by calculating, we have

$$\sum_{n \leq x} \frac{\Lambda(n)\chi(n)}{n} \leq \frac{M}{L_1}(1-\beta) + \beta + 0.0075 \leq 0.277, \tag{5.3.24}$$

which completes the proof of (5.3.18). □

Next, we are going to consider the numbers n such that $n \equiv 1 \bmod 4$ and explore the upper bound for the sum using the von Mangoldt function.

Lemma 5.7 *For all integers $x \geq e \cdot 10^4$, we have*

$$2 \sum_{\substack{n \leq x \\ n \equiv 1 \bmod 4}} \frac{\Lambda(n)}{n} \leq \sum_{n \leq x} \frac{\Lambda(n)}{n} - 0.41609. \tag{5.3.25}$$

Proof. Since

$$2 \sum_{\substack{n \leq x \\ n \equiv 1 \bmod 4}} \frac{\Lambda(n)}{n} = \sum_{\substack{n \leq x \\ (n,2)=1}} \frac{\Lambda(n)}{n} + \sum_{n \leq x} \frac{\chi(n)\Lambda(n)}{n},$$

consider the first term on the right hand side, and then we have

$$\begin{aligned}
\sum_{\substack{n \leq x \\ (n,2)=1}} \frac{\Lambda(n)}{n} &= \sum_{n \leq x} \frac{\Lambda(n)}{n} - \left(\frac{1}{2} + \frac{1}{2^2} + \ldots + \frac{1}{2^\alpha}\right) \log 2 \\
&= \sum_{n \leq x} \frac{\Lambda(n)}{n} - \left(1 - \frac{1}{2^\alpha}\right) \log 2 \\
&= \sum_{n \leq x} \frac{\Lambda(n)}{n} - \log 2 + \frac{\log 2}{2^\alpha},
\end{aligned}$$

where $2^\alpha \leq x$. Apply (5.3.18) to the second term, so we have

$$2\sum_{\substack{n\le x\\ n\equiv 1 \bmod 4}}\frac{\Lambda(n)}{n} \le \sum_{n\le x}\frac{\Lambda(n)}{n} - \log 2 + 0.000052 + 0.277$$
$$\le \sum_{n\le x}\frac{\Lambda(n)}{n} - 0.41609,$$

for all integers $x \ge e\cdot 10^4$. □

Next Pollack and Shapiro give a transformation of (5.3.25), that will be required in the next section.

Lemma 5.8 *For all integers $x \ge e\cdot 10^4$, we have*

$$2\sum_{\substack{n\le x\\ n\equiv 1 \bmod 4}}\frac{\Lambda(n)}{n} \le \frac{1}{x}\sum_{n\le x}\left\{\frac{x}{n}\right\}\Lambda(n) + \frac{\log x!}{x} - 0.41609. \tag{5.3.26}$$

Proof. For positive integers x, we have

$$\log x! = \sum_{n\le x}\Lambda(n)\left[\frac{x}{n}\right]. \tag{5.3.27}$$

Apply $z = [z] + \{z\}$ and replace $\left[\frac{x}{n}\right]$ in (5.2.25) into $\frac{x}{n} - \left\{\frac{x}{n}\right\}$, which gives

$$\log x! = x\sum_{n\le x}\frac{\Lambda(n)}{n} - \sum_{n\le x}\left\{\frac{x}{n}\right\}\Lambda(n).$$

Divide it by x, we have

$$\frac{\log x!}{x} = \sum_{n\le x}\frac{\Lambda(n)}{n} - \frac{1}{x}\sum_{n\le x}\left\{\frac{x}{n}\right\}\Lambda(n),$$

so

$$\sum_{n\le x}\frac{\Lambda(n)}{n} = \frac{\log x!}{x} + \frac{1}{x}\sum_{n\le x}\left\{\frac{x}{n}\right\}\Lambda(n). \tag{5.3.28}$$

Now apply (5.3.28) to (5.3.25), then (5.2.24) follows and we complete the proof. □

5.3.3 The imbalance in the distribution of primes

The assumption that (5.1.3) has a solution produces an imbalance in the distribution of primes less than n. This imbalance is quantified by the following lemma.

Lemma 5.9 *If $n! + 1 = x^4$, and $n \geq e \cdot 10^4$, then*

$$\frac{1}{n} \sum_{m \leq n} \left\{ \frac{n}{m} \right\} \Lambda(m) \geq 0.854. \tag{5.3.29}$$

Proof. As we know,

$$n! = \prod_{p \leq n} p^{\alpha_p}, \tag{5.3.30}$$

and (5.1.3) can be written as

$$(x^2 - 1)(x^2 + 1) = n!.$$

Also we have

$$x^2 - 1 \geq 2^{\alpha_2 - 1} \prod_{\substack{p \leq n \\ p \equiv -1 \bmod 4}} p^{\alpha_p}, \tag{5.3.31}$$

and

$$x^2 + 1 \leq 2 \prod_{\substack{p \leq n \\ p \equiv 1 \bmod 4}} p^{\alpha_p}. \tag{5.3.32}$$

Since $x^2 - 1 \leq x^2 + 1$, then we have

$$2^{\alpha_2 - 1} \prod_{\substack{p \leq n \\ p \equiv -1 \bmod 4}} p^{\alpha_p} \leq 2 \prod_{\substack{p \leq n \\ p \equiv 1 \bmod 4}} p^{\alpha_p}.$$

Take logarithms to it, then we obtain

$$(\alpha_2 - 1) \log 2 + \sum_{\substack{p \leq n \\ p \equiv -1 \bmod 4}} \alpha_p \log p \leq \log 2 + \sum_{\substack{p \leq n \\ p \equiv 1 \bmod 4}} \alpha_p \log p. \tag{5.3.33}$$

Add $\sum_{\substack{p \leq n \\ p \equiv 1 \bmod 4}} \alpha_p \log p$ to both sides of (5.3.33) we have

$$\alpha_2 \log 2 + \sum_{\substack{p \leq n \\ p \neq 2}} \alpha_p \log p \leq \log 4 + 2 \sum_{\substack{p \leq n \\ p \equiv 1 \bmod 4}} \alpha_p \log p,$$

or

$$\log n! \le \log 4 + 2 \sum_{\substack{p \le n \\ p \equiv 1 \bmod 4}} \alpha_p \log p. \tag{5.3.34}$$

Since

$$\begin{aligned} \alpha_p &= \sum_{p^\nu \le n} \left\lfloor \frac{n}{p^\nu} \right\rfloor \\ &\le n \sum_{p^\nu \le n} \frac{1}{p^\nu}, \end{aligned}$$

then (5.3.34) can be written as

$$\log n! \le \log 4 + 2n \sum_{\substack{p \le n \\ p \equiv 1 \bmod 4}} \left(\sum_{p^\nu \le n} \frac{1}{p^\nu} \right) \log p.$$

Divide it by n, then we have

$$\begin{aligned} \frac{\log n!}{n} &\le \frac{\log 4}{n} + 2 \sum_{\substack{p \le n \\ p \equiv 1 \bmod 4}} \sum_{p^\nu \le n} \frac{\log p}{p^\nu} \\ &\le \frac{\log 4}{n} + 2 \left(\sum_{\substack{m \le n \\ m \equiv 1 \bmod 4}} \frac{\Lambda(m)}{m} - \sum_{\substack{p^{2\nu} \le n \\ p \equiv -1 \bmod 4}} \frac{\log p}{p^{2\nu}} \right), \end{aligned} \tag{5.3.35}$$

which follows as there is the case that $m = p^{2\nu} \equiv 1 \bmod 4$ with $p \equiv -1 \bmod 4$.

Consider the second sum of (5.3.35). We have for $n \ge e \cdot 10^4$,

$$2 \sum_{\substack{p^{2\nu} \le n \\ p \equiv -1 \bmod 4}} \frac{\log p}{p^{2\nu}} \ge 2 \sum_{\substack{p \le 59 \\ p \equiv -1 \bmod 4}} \frac{\log p}{p^2 - 1} - 2 \sum_{\substack{p \le 59 \\ p \equiv -1 \bmod 4 \\ p^{2\nu} > n}} \frac{\log p}{p^{2\nu}}.$$

Since

$$\begin{aligned} \sum_{\substack{p \le 59 \\ p \equiv -1 \bmod 4 \\ p^{2\nu} > n}} \frac{\log p}{p^{2\nu}} &\le \sum_{\substack{p \le 59 \\ p \equiv -1 \bmod 4 \\ p^{2\nu} > e \cdot 10^4}} \frac{\log p}{p^{2\nu}} \\ &\le \sum_{\substack{p \le 59 \\ p \equiv -1 \bmod 4 \\ p^{2\nu} > e \cdot 10^4}} \frac{\log p}{e \cdot 10^4} \end{aligned}$$

$$
\begin{aligned}
&< \sum_{\substack{p\le 59\\ p\equiv -1 \bmod 4}} \frac{\log p}{e\cdot 10^4} \\
&< e^{-1}10^{-4} \sum_{\substack{p\le 59\\ p\equiv -1 \bmod 4}} \left(1+\frac{1}{p^2-1}\right)\log p \\
&= e^{-1}10^{-4} \sum_{\substack{p\le 59\\ p\equiv -1 \bmod 4}} \frac{p^2}{p^2-1}\log p \\
&\le 0.00107,
\end{aligned}
$$

and also we have

$$
2 \sum_{\substack{p\le 59\\ p\equiv -1 \bmod 4}} \frac{\log p}{p^2-1} \ge 0.44088.
$$

Then they yield

$$
2 \sum_{\substack{p\equiv -1 \bmod 4\\ p^{2\nu}\le n}} \frac{\log p}{p^{2\nu}} \ge 2 \sum_{\substack{p\le 59\\ p\equiv -1 \bmod 4}} \frac{\log p}{p^2-1} - \sum_{\substack{p\le 59\\ p\equiv -1 \bmod 4\\ p^{2\nu}> n}} \frac{\log p}{p^{2\nu}} \ge 0.438. \tag{5.3.36}
$$

By (5.3.36) and (5.3.26), (5.3.35) can be written as for $n \ge e\cdot 10^4$,

$$
\begin{aligned}
\frac{\log n!}{n} &\le \frac{\log 4}{n} + \left(\frac{1}{n}\sum_{m\le n}\left\{\frac{n}{m}\right\}\Lambda(m) + \frac{\log n!}{n} - 0.41609\right) - 0.438 \\
&\le \frac{1}{n}\sum_{m\le n}\left\{\frac{n}{m}\right\}\Lambda(m) + \frac{\log n!}{n} - 0.41609 - 0.438 + 0.00006.
\end{aligned}
$$

Therefore there follows

$$
\frac{1}{n}\sum_{m\le n}\left\{\frac{n}{m}\right\}\Lambda(m) \ge 0.854.
$$

□

5.4 Proof that there are no solutions for the equation $n! = x^4 - 1$

5.4.1 The case $n \ge 27182.8$

To prove (5.1.3) has no solutions, we need to derive a contradiction to the inequality (5.3.29), Lemma 5.9. To attain this objective, we need to estimate $\left\{\frac{n}{m}\right\}$ and the

Chebyshev function $\psi(x)$ to deal with $\sum_{m\leq n}\Lambda(m)$. Finally, the Prime Number Theorem will be employed to give the contradiction.

Let $r \geq 1$ be fixed and for given $n \in \mathbb{N}$, m satisfies

$$\frac{n}{1+1/r} < m < \frac{n}{1+1/(r+1)}, \tag{5.4.1}$$

then we have

$$1 + \frac{1}{r+1} < \frac{n}{m} < 1 + \frac{1}{r}.$$

Therefore, we obtain the estimation

$$\left\{\frac{n}{m}\right\} \leq \frac{1}{r}. \tag{5.4.2}$$

Apply the Chebyshev function

$$\psi(x) = \sum_{p^\alpha \leq x} \log p = \sum_{m\leq x} \Lambda(m),$$

we have

$$\sum_{m\leq n}\left\{\frac{n}{m}\right\}\Lambda(m) \leq \sum_{r=1}^{\infty}\frac{1}{r}\left(\psi\left(\frac{r+1}{r+2}\cdot n\right) - \psi\left(\frac{r}{r+1}\cdot n\right)\right) + \psi(\frac{1}{2}n). \tag{5.4.3}$$

Since the right hand side can be written as

$$\begin{aligned} &1\cdot(\psi(\frac{2}{3}n) - \psi(\frac{1}{2}n)) + \frac{1}{2}\cdot(\psi(\frac{3}{4}n) - \psi(\frac{2}{3}n)) + \frac{1}{3}\cdot(\psi(\frac{4}{5}n) - \psi(\frac{3}{4}n)) + \ldots + \psi(\frac{1}{2}n) \\ &= \sum_{r=1}^{\infty}\psi\left(\frac{r+1}{r+2}\cdot n\right)\frac{1}{r(r+1)}, \end{aligned}$$

then we have

$$\sum_{m\leq n}\left\{\frac{n}{m}\right\}\Lambda(m) \leq \sum_{r=1}^{\infty}\psi\left(\frac{r+1}{r+2}\cdot n\right)\frac{1}{r(r+1)}. \tag{5.4.4}$$

Suppose that for all $x \geq x_0$, we have

$$\psi(x) \leq Ax. \tag{5.4.5}$$

Since $\left(\frac{r+1}{r+2}\right) \cdot n \geq \frac{2}{3} \cdot n$, then for all $\frac{2}{3}n \geq x_0$, it yields

$$\begin{aligned}\sum_{r=1}^{\infty} \psi\left(\frac{r+1}{r+2} \cdot n\right) \frac{1}{r(r+1)} &\leq \sum_{r=1}^{\infty} \left(A\left(\frac{r+1}{r+2} \cdot n\right)\right)\left(\frac{1}{r(r+1)}\right) \\ &= An \sum_{r=1}^{\infty} \frac{1}{(r+2)r} \\ &= \frac{A}{2} n \sum_{r=1}^{\infty} \left(\frac{1}{r} - \frac{1}{r+2}\right) \\ &= \frac{A}{2} n(1+\frac{1}{2}),\end{aligned}$$

therefore (5.4.5) can be written as

$$\sum_{m \leq n} \left\{\frac{n}{m}\right\} \Lambda(m) \leq \frac{3}{4} An. \tag{5.4.6}$$

By Lemma 5.9, for all $n \geq max\{e \cdot 10^4, \frac{3}{2}x_0\}$

$$0.854n \leq \sum_{m \leq n} \left\{\frac{n}{m}\right\} \Lambda(m) \leq \frac{3}{4} An,$$

so

$$1.1386 \leq A. \tag{5.4.7}$$

Now, it is equivalent to Lemma 5.9 that (5.4.7) should be satisfied if $n! = x^4 - 1$ has a solution. However, the prime number theorem indicates that there exists an x_0 when $A < 1.1386$, so our purpose is to give an explicit estimation of x_0, which makes a contradiction to Lemma 5.9. Assume then for $x \geq 1$, we have

$$\psi(x) \leq \frac{6}{5} ax + (3 \log x + 5)(\log x + 1) \quad \text{where } a \leq 0.9213 \tag{5.4.8}$$

which is shown in [20]. Then we have

$$\begin{aligned}\psi(x) &\leq (1.1056)x + (3 \log x + 5)(\log x + 1) \\ &\leq \left(1.1056 + \frac{(3 \log x + 5)(\log x + 1)}{x}\right) x.\end{aligned}$$

To the purpose

$$A < 1.1386,$$

that is to make sure

$$\psi(x) \leq \left(1.1056 + \frac{(3\log x + 5)(\log x + 1)}{x}\right) x < 1.1386x,$$

then we have

$$x \geq \frac{2}{3}e \cdot 10^4.$$

Therefore, let $x_0 = \frac{2}{3}e \cdot 10^4$, then for all

$$n \geq e \cdot 10^4 = 27182.8,$$

we have

$$A < 1.1386,$$

which contradicts to Lemma 5.9. Therefore, (5.1.3) has no solutions for all $n \geq e \cdot 10^4 = 27182.8$.

5.4.2 The case $n < 27182.8$

What we remain is the case that $n \leq 27182$, which is also interesting to think about. After that, we will finish the proof of the nonexistence of solutions to (5.1.3). In this case, we are going to do the calculation and prove it by computers.

Divide (5.3.34) by $2n$, we have

$$\begin{aligned} \frac{\log n!}{2n} &\leq \frac{\log 2}{n} + \sum_{\substack{p \leq n \\ p \equiv 1 \bmod 4}} \frac{\alpha_p}{n} \log p \\ &\leq \frac{\log 2}{n} + \sum_{\substack{p \leq n \\ p \equiv 1 \bmod 4}} \frac{\log p}{p-1}, \end{aligned} \tag{5.4.9}$$

which follows as

$$\sum_{\substack{p \leq n \\ p \equiv 1 \bmod 4}} \frac{\alpha_p}{n} \log p = \sum_{\substack{p \leq n \\ p \equiv 1 \bmod 4}} \frac{1}{n}\left(\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \dots\right) \log p$$

$$\leq \sum_{\substack{p\leq n \\ p\equiv 1 \bmod 4}} \frac{1}{n}\left(\frac{n}{p}+\frac{n}{p^2}+\ldots\right)\log p$$
$$= \sum_{\substack{p\leq n \\ p\equiv 1 \bmod 4}} \frac{\log p}{p-1}.$$

By Stirling's formula given in [36],

$$\frac{\log n!}{n} > \left(1+\frac{1}{2n}\right)\log(n+1) - 1 + \frac{(\frac{1}{2}\log(2\pi)-1)}{n}, \tag{5.4.10}$$

then (5.4.9) and (5.4.10) imply

$$\frac{1}{2}\left(1+\frac{1}{2n}\right)\log(n+1) - 0.5 - \frac{0.734}{n} < \frac{\log n!}{2n} \leq \sum_{\substack{p\leq n \\ p\equiv 1 \bmod 4}} \frac{\log p}{p-1}, \tag{5.4.11}$$

where

$$\frac{(\frac{1}{2}\log(2\pi)-1)}{2n} - \frac{\log 2}{n} = -\frac{0.734}{n}.$$

By the observation

$$\frac{1}{4}\log(n+1) \geq 0.734$$

for $n \geq 18$. Then (5.4.11) implies

$$\frac{1}{2}\log(n+1) - 0.5 < \sum_{\substack{p\leq n \\ p\equiv 1 \bmod 4}} \frac{\log p}{p-1} \tag{5.4.12}$$

for $n \geq 18$.

For the case that $18 \leq n \leq 27182$, it is shown that the left side of (5.4.12) is always greater than the right by using Mathematica. Thus, we conclude that (5.1.3) has no solutions in this case, either. As for $n \leq 17$, we can check it by hand, and we get the same conclusion. Therefore, (5.1.3) has no solutions at all.

This is a great research which cannot be improved. However there might be an easier or shorter proof yet to be discovered.

5.5 The next to next to last case

This is the equation $n! = x^8 - 1$. It covers all powers of two on the right, $n! = x^{2^m} - 1$ for $m \geq 3$, since we have

$$x^{2^m} - 1 = \left(x^{2^{m-3}}\right)^8 - 1.$$

Lemma 5.10 *If p is an odd prime which divides $x^4 + 1$, then $p \equiv 1 \bmod 8$.*

Proof. Suppose p divides $x^4 + 1$, then we have

$$\begin{aligned} x^4 &\equiv -1 \bmod p, \\ (x^2)^2 &\equiv -1 \bmod p. \end{aligned} \tag{5.5.1}$$

This implies $(-1 \mid p) = 1$, so we get $p \equiv 1 \bmod 4$. But then

$$p \equiv 1 \bmod 8 \quad \text{or} \quad p \equiv 5 \bmod 8.$$

Assume $p \equiv 5 \bmod 8$. Since $p \nmid x$, then we have $x^{p-1} \equiv 1 \bmod p$. Because $p = 5 + 8q$, we get

$$\begin{aligned} x^{4+8q} &\equiv 1 \bmod p \\ (x^4)^{1+2y} &\equiv 1 \bmod p. \end{aligned}$$

By the congruence (5.5.1), we obtain

$$-1 = (-1)^{1+2y} \equiv 1 \bmod p,$$

which implies $p \mid 2$. Then we have $p = 2$, which is false. Thus $p \equiv 1 \bmod 8$ and we complete the proof. □

Theorem 5.11 *The equation $n! = x^8 - 1$ has no solutions in positive integers (n, x).*

Proof. Note that we can assume $n > 1$ so x is odd. We write

$$x^8 - 1 = (x^2 - 1)(x^2 + 1)(x^4 + 1),$$

and note that any odd prime p which satisfies $p \mid x^2+1$ or $p \mid x^4+1$, has $(-1 \mid p) = (-1)^{(p-1)/2} = 1$. This is the case if and only if $p \equiv 1 \bmod 4$. So for a given n satisfying $n! = x^8 - 1$ more than x^6 worth of the prime powers have their primes congruent to 1 modulo 4. This is too many, since $n!$ includes all of the primes up to n, and we expect about half of them to be congruent to 3 modulo 4.

1. Let

$$n! = x^8 - 1 = (x^4-1)(x^4+1) =: B_1 B_2 < B_2^2.$$

and note that for $n > 1$ we must have x odd.

2. Note that if an odd $p \mid B_2$ then $p \equiv 1 \bmod 8$ and that for x odd $2 \mid x^4+1$.

3. Note we employ Lemma 3.15.

$$T(n,a) \;:=\; \prod_{s \le n/q_0} \Psi(\frac{n}{s}, a) \le A^{\frac{n}{a-1}\sum_{s \le n/q_0} \frac{1}{s}} \le A^{\frac{n}{a-1}(\log \frac{n}{q_0})}.$$

4. This next is the key step: by 2. we get $B_2 \le 2T(n,8)$.

5. Stirling's approximation for the factorial gives $2(n/e)^n < n!$ for all $n \ge 1$.

Using 3. and 4. with $a = 8$ and $q_0 = 17$ gives

$$2n^n e^{-n} < n! < B_2^2 < 4T(n,8)^2 \le 4 \cdot 16^{\frac{2n}{7}(\log n - \log 17)},$$

so

$$n \log n - n \le \log 2 + \; n(\log n - \log 17),$$

Thus $n < 2$. □

Again, this is a great result which cannot be improved. We have described most of the literature which gives **no** solutions for

$$n! + 1 = x^m$$

for all $m \ge 3$, leaving only $n! + 1 = x^2$, which does of course have at least 3 solutions. The reader might compare this situation with Fermat's Last Theorem/ Wiles-Taylor's Theorem

$$x^m + y^m \ne z^m$$

except for $m = 2$, where there are an infinite number of primitive solutions.

Chapter 6

Related diophantine equations

6.1 Overview

In Chapter 4, I have already shown that, assuming the ABC conjecture, for any polynomial $P(x)$ of degree 2 or more with integer coefficients, the equation

$$P(x) = n! \tag{6.1.1}$$

has only a finite number of solutions $(x,\ n)$. In this chapter, I will consider the results of Daniel and Jorgen given in [2] and show that for some classes of polynomials $P(x)$, the number of solutions of (6.1.1) is finite. For different classes of polynomials, different methods will be introduced.

First I take some examples of $P(x) = x^2 - A$ and show $x^2 - A = n!$ has finitely many solutions, where A is a square-free integer. A different track from the one applied in Chapter 2 is introduced in [2]. Then by applying the same method, I show one class of reducible polynomials that can be factored as $(x^2 - a_1)(x^2 - a_2)\dots(x^2 - a_m)$ and solve (6.1.1). Next, I will take a few reducible polynomials as examples and introduce a method that involves the density of primes. Furthermore, I give the case where the polynomial is divisible by the mth cyclotomic polynomial Φ_m. By the property of the natural density of the subset of primes $S(\Phi_m)$, I will prove that $P(x) = n!$ has only finitely many solutions for some given polynomials. Finally, I give two examples, and give a method to show that there are no solutions when $P(x) = x(x+3)$ or $P(x) = x(x+1)(x+2)$. This

method may lead to a complete proof with more work.

Note that all methods introduced later depend on the fact that the numbers $n!$ are highly divisible by many primes. That is, we need n to be sufficiently large.

6.2 Quadratic factors with the form $(x^2 - A)$

Suppose $P(x) = n!$ has infinitely many solutions. Then it implies that the congruence

$$P(x) \equiv 0 \bmod m \tag{6.2.1}$$

always has a solution x for every positive integer m, or for every prime power $m = p^k$. Equivalently, if there exists an integer m such that (6.2.1) has no solutions, then it implies that (6.1.1) has finitely many solutions. Our results in this section will rely on this observation. First of all, consider a type of polynomials of the form $P(x) = x^2 - A$, where $A \in \mathbb{N}$ and is square-free. I show how it can be explained using that observation.

Example 6.1. Given $P(x) = x^2 - 3$, then

$$x^2 - 3 = n!$$

has only finitely many solutions. Since for any $n \geq 5$, $5 \mid n!$, but there is no solution for

$$x^2 - 3 \equiv 0 \bmod 5.$$

For $n < 5$, the only solution is $(3, 3)$. For a given square-free integer A, to find out the least integer m such that

$$x^2 - A \equiv 0 \bmod m$$

has no solutions, we can consider the system of quadratic nonresidue modulo m instead. If m is a prime, we can employ the law of quadratic reciprocity

$$(A \mid p) = (p \mid A) \text{ if } A \equiv 1 \bmod 4,$$

$$(A \mid p) = (p \mid A) \text{ if } A \equiv 3 \bmod 4, p \equiv 1 \bmod 4,$$

$$(A \mid p) = -(p \mid A) \text{ if } A \equiv 3 \bmod 4, p \equiv 3 \bmod 4.$$

For example, let $A = 13$. Since $A = 13 \equiv 1 \bmod 4$, then we have $(13 \mid p) = (p \mid 13)$. Therefore, we can list the primes

$$p \equiv 1, 3, 4, 9, 10 \text{ or } 12 \bmod 13,$$

such that $(13 \mid p) = 1$. Also we obtain some primes such that $(13 \mid p) = -1$ and the congruence $x^2 - 13 \equiv 0 \bmod p$ has no solutions. Say $p = 5$, $(13 \mid 5) = -1$. So for $n \geq 5$, $x^2 - 13 = n!$ has no solutions. In fact, there are no solutions for $n < 5$, either. Thus, $x^2 - 13 = n!$ has no solutions at all.

I did some numerical experiments on the type of polynomials, $P(x) = x^2 - A$. The following Table 6.1 gives some values of $A \leq 50$ such that $x^2 - A = n!$ has no solutions, and the least integers m such that $x^2 - A \equiv 0 \bmod m$ has no solutions, which can account for the former result.

Here I give a theorem that is about irreducible polynomials and the cases discussed could be covered by it.

Theorem 6.1 *[2] If $P \in \mathbb{Z}[X]$ is irreducible over $\mathbb{Q}$ and the degree of P is greater than or equal to 2, then the equation $P(x) = n!$ has only finitely many solutions.*

This works, in fact, not just for irreducible polynomials. The method of Theorem 6.1 works also on some kinds of reducible polynomials. In order to illustrate that, let us consider and analyze some examples below. For instance,

$$(x^2 - 5)(x^2 - 6)(x^2 - 30) = n!$$

has only finitely many solutions. This is because when $m = 8 = 2^3$, there are no solutions for the congruence $(x^2 - 5)(x^2 - 6)(x^2 - 30) \equiv 0 \bmod 8$, even though the associated congruence has a solution for $p = 2$. This can be found by explicit numerical calculation. More generally, consider the polynomial $P(x) = (x^2 -$

A	$x^2 - A$	$\min\{m\|(A \mid m) = -1\}$
5	$x^2 - 5$	3
6	$x^2 - 6$	4
11	$x^2 - 11$	3
13	$x^2 - 13$	5
17	$x^2 - 17$	3
18	$x^2 - 18$	4
20	$x^2 - 20$	3
21	$x^2 - 21$	8
22	$x^2 - 22$	4
26	$x^2 - 26$	3
27	$x^2 - 27$	4
28	$x^2 - 28$	5
29	$x^2 - 29$	3
31	$x^2 - 31$	4
32	$x^2 - 32$	3
33	$x^2 - 33$	5
37	$x^2 - 37$	5
38	$x^2 - 38$	3
39	$x^2 - 39$	4
41	$x^2 - 41$	3
42	$x^2 - 42$	4
44	$x^2 - 44$	3
45	$x^2 - 45$	7
46	$x^2 - 46$	4
50	$x^2 - 50$	3

Table 6.1: Some values of $A \leq 50$, $x^2 - A$ and the least integers m with $(A \mid m) = -1$

$r)(x^2 - s)(x^2 - rs)$, where r and s are some integers such that each factor is irreducible. Note that in this section, we do not discuss the case where there exist linear factors arising from quadratic reducible factors. Since there is always a solution for (6.2.1) and the method in this section will not be working. There is no doubt that for any prime p, there is at least one of r, s and rs which is quadratic residue modulo p, which leads to the congruence

$$(x^2 - r)(x^2 - s)(x^2 - rs) \equiv 0 \bmod p \tag{6.2.2}$$

has a solution. However, by the observation we mentioned from the start, we also need to check if the congruence has a solution for any prime power. In fact, different choices of r and s in $(x^2 - r)(x^2 - s)(x^2 - rs)$ lead to different results.

For instance, when $r = 2$, $s = 7$,

$$(x^2 - 2)(x^2 - 7)(x^2 - 14) \equiv 0 \bmod m$$

has solutions modulo any integer, i.e. any prime power $p^k = m$ only except for $p = 2$, therefore the equation has only finitely many solutions. While if $r = 13$, $s = 17$, $(x^2-13)(x^2-17)(x^2-221) \equiv 0 \bmod m$ has a solution x for every positive integer m. However, we cannot give a conclusion that there are an infinite number of solutions only because this condition is met. We need to keep checking if for such x that $(x^2-13)(x^2-17)(x^2-221) \equiv 0 \bmod m$ has a solution for every $m \leq n$, each divisor of $(x^2 - 13)(x^2 - 17)(x^2 - 221)$ is also the divisor of $n!$.

6.3 Overloaded factors

6.3.1 Density of primes

In this section, we focus on the case where $P(x)$ is a reducible polynomial which is made up of general factors, rather than only factors of degree 2 as in the preceding cases. Therefore, the method in the last section may not be applied and we need to explore other methods.

Example 6.2: The equation

$$n! = x(x^2 + 1)$$

has only a finite number of solutions.

We are not able to verify the number of solutions of the equation $x(x^2+1) = n!$ by previous methods. However, based on the assumption that n is sufficiently large, we may estimate the order of magnitude of x as $\sqrt[3]{n!}$, so that x^2+1 is approximately $\sqrt[3]{n!^2}$. In terms of the factor (x^2+1), we can apply the law of quadratic reciprocity, which gives the congruence

$$x^2 + 1 \equiv 0 \bmod p \quad \text{where } p \text{ is a prime,}$$

has a solution if and only if $p \equiv 1 \bmod 4$ or $p = 2$. Hence the factor $x^2 + 1$ can be divisible only by these primes. Since these primes are, roughly speaking, only half of all primes, there should be a contradiction for sufficiently large n, which implies that the equation $x(x^2 + 1) = n!$ has only finitely many solutions.

This example, however, represents only a special type of polynomial. i.e. there is one special factor $(x^2 + 1)$ that gives some important information of the density of prime divisors. That is, indeed, a good and new angle to consider for general polynomials $P(x)$. However, it is not easy to figure out in general the property of some other kinds of factors and estimate the density of primes.

Here I give a theorem which gives methods for when a density argument will work.

Theorem 6.2 *[2] Let $Q \in \mathbb{Z}[x]$ be any factor of P and take*

$$S(Q) := \{p \mid Q(x) \equiv 0 \bmod p \text{ has a solution}\} \subseteq \mathbb{P}.$$

If

$$d(S(Q)) < \frac{degQ}{degP},$$

then the equation $P(x) = n!$ has only finitely many solutions.

Note that d is the notion of *natural density* of a subset of primes A, and it is defined by

$$d(A) = \lim_{x \to \infty} \frac{\pi(x, A)}{\pi(x)}, \tag{6.3.1}$$

where $\pi(x)$ is the number of primes not exceeding x and $\pi(x, A)$ is the number of those belonging to A, defined whenever this limit exists.

Proof. Given a polynomial $P(x)$. Consider $P(x)$ itself as a factor, $S(P)$ represents the set of all the primes p that divide $P(x)$ for at least one x. We are given $d(S(P)) < \frac{degP}{degP} = 1$. Suppose that there exists a prime p such that $P(x) \equiv 0 \bmod p$ has no solutions. So if n satisfies $p < n$, then $P(x) = n!$ has no solutions at all. Otherwise, we obtain $n \leq p$. i.e. n has an upper bound. In conclusion, $P(x) = n!$ has only finitely many solutions (x, n).

Note that this case is based on n being sufficiently large. Now consider the case that there exists $Q(x)$ as a factor of $P(x)$, but $Q(x) \neq P(x)$. As $|x| \to \infty$, then we can get an asymptotic equivalence relation:

$$|Q(x)| \sim |P(x)|^{\frac{deg(Q)}{deg(P)}}, \tag{6.3.2}$$

equivalently we have

$$|Q(x)| - |P(x)|^{\frac{deg(Q)}{deg(P)}} = o\left(|P(x)|^{\frac{deg(Q)}{deg(P)}}\right) \tag{6.3.3}$$

when $x \to \infty$. Define a function

$$\psi_1(N, M) := \prod_{p \in M \cap \mathbb{P}} p^{\nu_p(N)} \tag{6.3.4}$$

for any $N \in \mathbb{N}$ and any set of natural numbers M. Now let $N = n!$ and $M = S(Q)$. Then we have

$$\psi_1(n!, S(Q)) = \prod_{p \in S(Q)} p^{\nu_p(n!)}.$$

And we are given that

$$Q(x) \mid \psi_1(n!, S(Q)), \tag{6.3.5}$$

which implies that $Q(x) \leq \psi_1(n!, S(Q))$. From the quite difficult to prove Proposition 4.1 [2], we have

$$\psi_1(n!, S(Q)) = (n!)^{d(S(Q))+o(1)}, \tag{6.3.6}$$

then they yield

$$Q(x) \leq (n!)^{d(S(Q))+o(1)}. \tag{6.3.7}$$

By (6.3.2), we can replace $|Q(x)|$ by $(1 + o(1))|P(x)|^{\frac{deg(Q)}{deg(P)}}$, which gives

$$(1 + o(1))|P(x)|^{\frac{deg(Q)}{deg(P)}} \leq (n!)^{d(S(Q))+o(1)}.$$

If $d(S(Q)) < \frac{degQ}{degP}$, and also suppose there exists a solution for $P(x) = n!$. Then

we obtain

$$\frac{1}{2}(n!)^{\frac{deg(Q)}{deg(P)}} \leq (1+o(1))(n!)^{\frac{deg(Q)}{deg(P)}} \leq (n!)^{d(S(Q))+o(1)}.$$

Denote $\frac{deg(Q)}{deg(P)} = \alpha$ and $d(S(Q)) + o(1) < \beta < \frac{deg(Q)}{deg(P)} = \alpha$. Then for some n_0 and $n_0 \leq n$, we have

$$\begin{aligned} \frac{1}{2}(n!)^{\alpha} &\leq (n!)^{\beta}, \\ (n!)^{\alpha-\beta} &\leq 2, \\ n! &\leq 2^{\frac{1}{\alpha-\beta}} = C, \end{aligned}$$

where C represents a constant. So it implies that there exists a constant C_1 such that $n \leq C_1$. Therefore $P(x) = n!$ has only a finite number of solutions. □

Next we give an example. Consider the equation

$$x(x^2+1)(x^2+2) = n!. \tag{6.3.8}$$

According to the results we have shown, we cannot take the factors $Q(x)$ such that the set $S(Q)$ contains the whole of $\mathbb{P}$. So we can only choose the factors that are not including x. Let us take and consider the factors $Q(x) = x^2+1$ and $Q(x) = x^2+2$ respectively. Then we get $S(Q) = \{2\} \cup \{p \in \mathbb{P} : p \equiv 1 \bmod 4\}$ in case one and $S(Q) = \{2\} \cup \{p \in \mathbb{P} : p \equiv 1, 3 \bmod 8\}$ in case two. Therefore they imply $d(S(Q)) = \frac{1}{2}$ in both cases. However, $\frac{degQ}{degP} = \frac{2}{5}$, so Theorem 6.2 cannot be applied. Thus, let us consider the factor, $Q(x) = (x^2+1)(x^2+2)$. Then we get $S(Q) = \{2\} \cup \{p \in \mathbb{P} : p \equiv 1, 3, 5 \bmod 8\}$ which gives $d(S(Q)) = \frac{3}{4}$, while $\frac{degQ}{degP} = \frac{4}{5}$ in this case. Hence, it suffices to use Theorem 6.2, and then (6.3.8) has only finitely many solutions.

From this example, we find that Theorem 6.2 cannot always be employed for any given factor of a polynomial $P(x)$. Let us explore Theorem 6.2 by another example.

6.3.2 Cyclotomic polynomial being a factor

Firstly, I give a brief introduction of cyclotomic polynomials, which I get from [39]. In algebra, the mth cyclotomic polynomial, which is the unique irreducible polynomial with integer coefficients, is a divisor of $x^m - 1$ but it is not a divisor of $x^k - 1$ for any integer $k < m$. We denote Φ_m the mth cyclotomic polynomial Φ_m as a factor of $P(x)$. In addition, if m is a prime number, then

$$\Phi_m(x) = 1 + x + x^2 + \ldots + x^{m-1} = \sum_{i=0}^{m-1} x^i.$$

The prime divisors of the mth cyclotomic polynomial Φ_m are those primes such that $p \equiv 1 \bmod m$, so we have the density $d(S(\Phi_m)) = \frac{1}{\phi(m)}$. By Theorem 6.2, if $degP < \phi(m)^2$ then (6.1.1) has only a finite number of solutions.

From this simple observation, we can deal with (6.1.1), where $P(x)$ can be divided by the mth cyclotomic polynomial. In particular, for the case where $P(x) = x^m - 1$, if $m < \phi(m)^2$, then $x^m - 1 = n!$ has only finitely many solutions. Here we must exclude only the cases where $m = 1, 2, 4$ or 6, since they are the only values of m for which $m \geq \phi(m)^2$. Looking at these cases explicitly, when $m = 6$, $\Phi_6 = x^2 - x + 1$. $d(S(\Phi_6)) = \frac{1}{\phi(m)} = \frac{1}{2}$ and obviously $degP < \phi(6)^2$ would not suffice. But if we choose the factor $x^4 + x^2 + 1$ with $d(S(x^4 + x^2 + 1)) = \frac{1}{2}$, then we can apply Theorem 6.2 and obtain $x^6 - 1 = n!$ has only finitely many solutions. In terms of the case where $m = 1$ and the equation $x - 1 = n!$. It is easy to see that there is always a solution for this equation. And when $m = 2$ and $m = 4$, the equations $m^2 - 1 = n!$ and $m^4 - 1 = n!$ have already been discussed in previous chapters.

6.4 Two examples with no apparent solutions

6.4.1 The case $P(x) = x(x + 3)$

Example 6.3: The equation

$$n! = x(x + 3) \tag{6.4.1}$$

has no positive integer solutions for $n < 10^6$ by attempting to factor $x^2 + 3x - n!$ using Mathematica. The equations are all irreducible, leading to the conjecture that (6.4.1) has no solutions.

However, here we use quite a different approach for $n = 19$.

$$19! = 2^{16} \cdot 3^8 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19. \tag{6.4.2}$$

Proof. Case 1: We suppose x is a positive even integer. Then $x = 2^{16}y$, where y is a positive odd integer. Then (6.4.2) can be written as

$$19! = 2^{16}y(2^{16}y + 3). \tag{6.4.3}$$

Divide both sides of (6.4.3) by 2^{16}, then we have

$$3^8 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 = y(2^{16}y + 3). \tag{6.4.4}$$

It is easy to see that x must be divisible by 3, so we have $y = 3^7 z$, where z is a positive odd integer. Next, replace y of (6.4.4) by $3^7 z$ and divide (6.4.4) by 3^8. Then we have

$$5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 = z(2^{16}3^6 z + 1). \tag{6.4.5}$$

Take (6.4.5) modulo $2^{16}3^6$ to get

$$44,028,905 \equiv z \bmod 2^{16}3^6. \tag{6.4.6}$$

From the right hand side of (6.4.5), we obtain

$$2^{16}3^6 z^2 < 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19,$$

that is

$$z < \sqrt{\frac{5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19}{2^{16}3^6}} \leq 2.43343 \tag{6.4.7}$$

From (6.4.6) and (6.4.7), we have

$$0 < z = 2^{16}3^6q + 44,028,905 \leq 2.43343, \tag{6.4.8}$$

which has no solutions for any integer q when $z = 1$ or $z = 2$. This contradiction completes the proof that $19! = x(x+3)$ has no solutions. □

Case 2: Now suppose x is a positive even integer and consider the equation

$$19! = x(x-3). \tag{6.4.9}$$

Let $x = 2^{16}y$ and $y = 3^7z$, where y and z are both positive odd integers and $3 \nmid z$. Do division by $2^{16} \cdot 3^8$ as the previous case, then we have

$$5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 = (2^{16}3^6z - 1)z, \tag{6.4.10}$$

which implies

$$\frac{5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19}{2^{16}3^6} < z^2 < \frac{5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19}{2^{15}3^6}$$

$$2.43343 < z < 3.44139.$$

It gives $z = 3$, however, since the prime factorization of $19!$ and $y = 3^7z$, we can conclude that the smallest prime factor of z should be larger than or equal to 5, which contradicts $z = 3$. Therefore, we complete the proof of this case.

Note that for (6.4.1), the case where x is a negative even integer is, in fact, the same as case 2 above. i.e. It yields (6.4.9). Also, the case that x is a negative odd integer can be considered the same as case 1 above. Therefore, we complete (6.4.1) for all cases.

6.4.2 The case $P(x) = x(x+1)(x+2)$

Example 6.4: Numerical exploration leads to the conjecture that the equation

$$n! = x(x+1)(x+2) \tag{6.4.11}$$

has only the solutions (n, x) when it equals $(3, 1)$, $(4, 2)$, $(5, 4)$ or $(6, 8)$. Firstly I will solve this problem in some special cases, then prove it by an approach that I believe can be applied for any case.

Case 1: Suppose $x = 2^\alpha$, where α is any integer. Consider the equation

$$n! = 2^\alpha(2^\alpha + 1)(2^\alpha + 2) = 2^{\alpha+1}(2^\alpha + 1)(2^{\alpha-1} + 1). \tag{6.4.12}$$

According to the Factorial Divisible by Prime Power Theorem, let $p^{\alpha_p(n)}$ be the largest power of prime p which divides $n!$, that is, $p^{\alpha_p(n)} \mid n!$ but $p^{\alpha_p(n)+1} \nmid n!$. Then $\alpha_p(n) = \frac{n-\delta_p(n)}{p-1} \leq n - 1$ for any prime factor p, where $\delta_p(n)$ is the digit sum of n when written in base p.

Definition: Let $n \in \mathbb{Z}$ and $n \geq 0$. The **digit sum** of n to base p is the sum of all the digits of n when expressed in base p. That is, if:

$$n = \sum_{k\geq 0} c_k p^k,$$

where $0 \leq c_k < p$, then

$$\delta_p(n) = \sum_{k\geq 0} c_k.$$

For each term on the right hand side of (6.4.12), we have

$$2^{\alpha+1} = 2^{\alpha_2(n)} \leq 2^{n-1} < 2^n,$$

$$2^\alpha + 1 < 2^{\alpha+1} < 2^n,$$

$$2^{\alpha-1} + 1 < 2^n.$$

Thus by (6.4.12), we have

$$n! < 2^{3n}.$$

By Stirling's approximation for $n!$, we have

$$\left(\frac{n}{e}\right)^n < 2^{3n},$$

which implies

$$n \log n - n < 3n \log 2.$$

Thus we obtain $n < 22$ and we can check that there is no such solution for $4 \leq n \leq 21$ numerically by hand.

Case 2: Suppose $x = p_1 p_2 \dots p_l$, a square-free number. Consider the equation

$$n! = p_1 p_2 \dots p_l (p_1 p_2 \dots p_l + 1)(p_1 p_2 \dots p_l + 2).$$

Since $p_l \leq n$, then we have

$$x = p_1 p_2 \dots p_l \leq n^l \leq n^{\frac{2n}{\log n}}. \tag{6.4.13}$$

But

$$x = n^{\frac{n}{3}(1+o(1))}, \tag{6.4.14}$$

since

$$n^{n(1+o(1))} \sim n! = (x+1)(x+2)(x+3) \sim x^3,$$

when x is sufficiently large. So by (6.4.13) and (6.4.14), we have for n sufficiently large

$$n^{\frac{n}{3}(\frac{1}{2})} \leq n^{\frac{n}{3}(1+o(1))} \leq n^{\frac{2n}{\log n}}.$$

which gives

$$\frac{n}{6} \leq \frac{2n}{\log n}.$$

Therefore we obtain $n \leq 162755$, then we can solve this problem numerically up to this upper bound. Note we can make all of the ranges explicit and believe this last range will cover all possibilities.

Case 3: Suppose $x = p^\alpha$, where p is an odd prime and α is any integer. For the equation

$$n! = p^\alpha (p^\alpha + 1)(p^\alpha + 2), \tag{6.4.15}$$

where p^α and $(p^\alpha + 2)$ are both odd integers, while $(p^\alpha + 1)$ is even. Suppose

$$n! = 2^{\beta_1} p_2^{\beta_2} \dots p_i^{\beta_i} \dots p_l^1 \dots p_m^1. \tag{6.4.16}$$

Then $\beta_1 = \alpha_2(n)$ is the largest power for the prime 2 dividing $n!$, so we have

$$2^{\beta_1} \mid p^\alpha + 1. \tag{6.4.17}$$

From the property of decomposition of $n!$ into prime factors [12], we also have

$$2^{\beta_1} > p_i^{\beta_i} = p^\alpha, \quad \text{as } \beta_i < \beta_1 \text{ for some } i,$$

or

$$2^{\beta_1} \geq p_i^{\beta_i} + 1 = p^\alpha + 1. \tag{6.4.18}$$

So from (6.4.17) and (6.4.18), we have

$$2^{\beta_1} = p^\alpha + 1,$$

which implies

$$n! = p^\alpha (p^\alpha + 1)(p^\alpha + 2) \leq 2^{\beta_1} \cdot 2^{\beta_1} \cdot (2 \cdot 2^{\beta_1}) = 2^{3\beta_1 + 1}. \tag{6.4.19}$$

Since $\beta_1 = \alpha_2(n) = \frac{n - \delta_2(n)}{2-1} \leq n - 1$, by Stirling's approximation of $n!$, then we have

$$\left(\frac{n}{e}\right)^n < 2^{3(n-1)+1}.$$

Therefore, we obtain

$$n \leq 20.$$

As we have shown, there are only four pairs of solutions when $n \leq 20$.

Next I give the proof that should be valid for all cases. Before doing that, I introduce a theorem, which I discovered when I studied the pattern of the power of prime factors in $x(x+1)(x+2)$ using Mathematica.

Theorem 6.3 *For any integer $x > 0$ in the polynomial $x(x+1)(x+2)$, we have for each odd prime p,*

$$\nu_p(x(x+1)(x+2) = c \quad \textit{where } c > 0$$

if and only if

$$x \equiv p^c - 2 + p^c q \bmod p^{c+1} \quad \textit{where } 0 \leq q \leq p-2 \tag{6.4.20}$$

or

$$x \equiv p^c - 1 + p^c q \bmod p^{c+1} \quad \textit{where } 0 \leq q \leq p-2 \tag{6.4.21}$$

or

$$x \equiv p^c + p^c q \bmod p^{c+1} \quad \textit{where } 0 \leq q \leq p-2. \tag{6.4.22}$$

Proof. Suppose x can be divided by p and $p^c \mid x$, where c is the highest power. Then neither $x+1$ nor $x+2$ can be divided by p. Let $x = p^c r$, where r cannot be divided by p. Therefore we have

$$x = p^c r = p^c(\alpha p + \beta) \equiv p^c \beta \bmod p^{c+1} \quad \text{where } 0 \leq \alpha,\ 1 \leq \beta < p.$$

Equivalently, let $\beta = 1 + q$. We get

$$x \equiv p^c + p^c q \bmod p^{c+1} \quad \text{where } 0 \leq q \leq p-2.$$

Similarly, if $p^c \mid x+1$, we have

$$x \equiv p^c - 1 + p^c q \bmod p^{c+1} \quad \text{where } 0 \leq q \leq p-2;$$

if $p^c \mid x+2$, we have

$$x \equiv p^c - 2 + p^c q \bmod p^{c+1} \quad \text{where } 0 \leq q \leq p-2.$$

Next consider if we have

$$x \equiv p^c + p^c q \bmod p^{c+1} \quad \text{where } 0 \le q \le p-2,$$

then we can write

$$x = p^{c+1}\gamma + p^c + p^c q = p^c(p\gamma + 1 + q).$$

Since $0 \le q \le p-2$, then $1 \le q+1 < p-1$, so $(p\gamma + 1 + q)$ can never be the multiples of p. Thus, we complete the proof. □

Next I show, by way of an example, the method of proof that (6.4.11) has no solutions when $n \ge 7$.

Proof. Suppose that there exist some solutions for (6.4.11), then

$$\alpha_p(n) = \nu_p(x(x+1)(x+2)) = \nu_p((x+3)!) - \nu_p(x!).$$

Therefore, it implies

$$\frac{n - \delta_p(n)}{p-1} = \sum_{j \ge 1} \left(\left\lfloor \frac{x+3}{p^j} \right\rfloor - \left\lfloor \frac{x}{p^j} \right\rfloor \right), \tag{6.4.23}$$

where left and right hand side represent the largest power of each prime p which divides $n!$ and $x(x+1)(x+2)$ respectively.

By applying Mathematica 8.0, we work out that the patterns of each side of (6.4.23). Here gives the matrix that includes the values of n, and for each value $n \le 20$, the largest power for $p = 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19$ dividing $n!$.

```
MatrixForm[
Table[{n,
(n - Total[IntegerDigits[n, 3]])/2, (n - Total[IntegerDigits[n, 5]])/4,
(n - Total[IntegerDigits[n, 7]])/6, (n - Total[IntegerDigits[n, 11]])/10,
(n - Total[IntegerDigits[n, 13]])/12, (n - Total[IntegerDigits[n, 17]])/16,
(n - Total[IntegerDigits[n, 19]])/18}, {n, 1, 20}], TableHeadings →
{None, {n, "α3(n)", "α5(n)", "α7(n)", "α11(n)", "α13(n)", "α17(n)", "α19(n)"}}]
```

n	α_3(n)	α_5(n)	α_7(n)	α_{11}(n)	α_{13}(n)	α_{17}(n)	α_{19}(n)
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	1	0	0	0	0	0	0
4	1	0	0	0	0	0	0
5	1	1	0	0	0	0	0
6	2	1	0	0	0	0	0
7	2	1	1	0	0	0	0
8	2	1	1	0	0	0	0
9	4	1	1	0	0	0	0
10	4	2	1	0	0	0	0
11	4	2	1	1	0	0	0
12	5	2	1	1	0	0	0
13	5	2	1	1	1	0	0
14	5	2	2	1	1	0	0
15	6	3	2	1	1	0	0
16	6	3	2	1	1	0	0
17	6	3	2	1	1	1	0
18	8	3	2	1	1	1	0
19	8	3	2	1	1	1	1
20	8	4	2	1	1	1	1

Take $n = 10$ as an example. We obtain from the matrix that $\alpha_3(10) = 4,\ \alpha_5(10) = 2$ and $\alpha_7(10) = 1$. To solve (6.4.23), we need to find out the value of x such that

$$\nu_3(x(x+1)(x+2)) = 4, \tag{6.4.24}$$

$$\nu_5(x(x+1)(x+2)) = 2, \tag{6.4.25}$$

$$\nu_7(x(x+1)(x+2)) = 1, \tag{6.4.26}$$

which can be dealt with from the pattern of the right side of (6.4.23). By Theorem 6.3, I work out that for those x that satisfy (6.4.20)-(6.4.22), they can be

$$x \equiv 79,\ 80,\ 81,\ 160,\ 161,\ \text{or } 162 \bmod 3^5 = 243, \tag{6.4.27}$$

$$x \equiv 23,\ 24,\ 25,\ 48,\ 49,\ 50,\ 73,\ 74,\ 75,\ 98,\ 99,\ \text{or } 100 \bmod 5^3 = 125, \tag{6.4.28}$$

$$x \equiv 5,\ 6,\ 7,\ 12,\ 13,\ 14,\ 19,\ 20,\ 21,\ 26,\ 27,\ 28,\ 33,\ 34,\ 35,\ 40,\ 41,\ \text{or } 42 \bmod 7^2 = 49. \tag{6.4.29}$$

By Chinese Remainder Theorem, there are $6 \cdot 12 \cdot 18$ possibilities for x. By applying Mathematica, I find out that the smallest value is $x = 2023$, which satisfies (6.3.27)-(6.3.29).

Here I give the matrix that shows for $2017 \leq x \leq 2034$, the largest power for $p = 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19$ dividing $x(x+1)(x+2)$.

```
MatrixForm[
Table[{m + 1, Sum[IntegerPart[(m + 3)/3^j] - IntegerPart[m/3^j],
{j, 1, Log[m + 3.]/Log[3.]}],
Sum[IntegerPart[(m + 3)/5^j] - IntegerPart[m/5^j], {j, 1, Log[m + 3.]/Log[5.]}],
Sum[IntegerPart[(m + 3)/7^j] - IntegerPart[m/7^j], {j, 1, Log[m + 3.]/Log[7.]}],
Sum[IntegerPart[(m + 3)/11^j] - IntegerPart[m/11^j], {j, 1, Log[m + 3.]/Log[11.]}],
Sum[IntegerPart[(m + 3)/13^j] - IntegerPart[m/13^j], {j, 1, Log[m + 3.]/Log[13.]}],
Sum[IntegerPart[(m + 3)/17^j] - IntegerPart[m/17^j], {j, 1, Log[m + 3.]/Log[17.]}],
Sum[IntegerPart[(m + 3)/19^j] - IntegerPart[m/19^j],
{j, 1, Log[m + 3.]/Log[19.]}]}, {m, 2016, 2060}], TableHeadings →
{None, {x, "α3(P)", "α5(P)", "α7(P)",  "α11(P)", "α13(P)", "α17((P)", "α19(P)"}}]
```

x	α_3(P)	α_5(P)	α_7(P)	α_{11}(P)	α_{13}(P)	α_{17}(P)	α_{19}(P)
2017	1	0	0	0	0	0	0
2018	1	1	0	0	0	0	0
2019	1	1	0	0	0	0	0
2020	1	1	0	0	0	0	0
2021	1	0	1	0	0	2	0
2022	1	0	1	1	0	2	0
2023	4	2	1	1	0	2	0
2024	4	2	0	1	0	0	0
2025	4	2	0	0	0	0	0
2026	1	0	0	0	2	0	0
2027	1	0	0	0	2	0	0
2028	1	1	1	0	2	0	0
2029	1	1	1	0	0	0	0
2030	1	1	1	0	0	0	0
2031	1	0	0	0	0	0	1
2032	2	0	0	0	0	0	1
2033	2	1	0	1	0	0	1
2034	2	1	0	1	0	0	0

* Note that P represents the polynomial $x(x+1)(x+2)$.

Since $10! < x(x+1)(x+2) = 2023 \cdot 2024 \cdot 2025$, then there does not exist such x satisfying (6.4.23), which implies that (6.4.11) has no solutions. Except that, it is easy to find that 2023 can be divided by 11 and 13 from the matrix above, while $p = 11,\ 13$ are not the factors of 10! as $n = 10 < 11,\ 13$.

In this way, for any $n > 10$, there will be at least four prime factors dividing $n!$ to be considered. Then by (6.4.20)-(6.4.22), there will give more congruences that x need to be followed and much more possibilities for x. Thus I assume that it can lead to huge x such that $n! < x(x+1)(x+2)$ occurs all the time. □

In order to verify my assumption, I would like to show another case when $n = 15$ and prove it in this way.

From the first matrix, we have

$$\alpha_3(15) = 6, \tag{6.4.30}$$

$$\alpha_5(15) = 3, \tag{6.4.31}$$

$$\alpha_7(15) = 2, \tag{6.4.32}$$

$$\alpha_{11}(15) = 1, \tag{6.4.33}$$

$$\alpha_{13}(15) = 1. \tag{6.4.34}$$

If (6.4.11) has a solution, then the equations

$$\nu_3(x(x+1)(x+2)) = 6, \tag{6.4.35}$$

$$\nu_5(x(x+1)(x+2)) = 3, \tag{6.4.36}$$

$$\nu_7(x(x+1)(x+2)) = 2, \tag{6.4.37}$$

$$\nu_{11}(x(x+1)(x+2)) = 1, \tag{6.4.38}$$

$$\nu_{13}(x(x+1)(x+2)) = 1, \tag{6.4.39}$$

must be satisfied at least. By (6.4.20)-(6.4.22), I obtain that x must be

$$\begin{aligned}
x &\equiv 727,\ 728,\ 729,\ 1456,\ 1457 \text{ or } 1458 \bmod 3^7 = 2187,\\
x &\equiv 123,\ 124,\ 125,\ 248,\ 249,\ 250,\ 373,\ 374,\ 375,\ 498,\ 499\\
&\quad \text{or } 500 \bmod 5^4 = 625,\\
x &\equiv 47,\ 48,\ 49,\ 96,\ 97,\ 98,\ 145,\ 146,\ 147,\ 194,\ 195,\ 196,\\
&\quad 243,\ 244,\ 245,\ 292, 293 \text{ or } 294 \bmod 7^3 = 343,\\
x &\equiv 9,\ 10,\ 11,\ 20,\ 21,\ 22,\ 31,\ 32,\ 33,\ 42,\ 43,\ 44,\ 53,\\
&\quad 54,\ 55,\ 64,\ 65,\ 66,\ 75,\ 76,\ 77,\ 86,\ 87,\ 88,\ 97,\ 98,\ 99,\ 108,\\
&\quad 109 \text{ or } 110 \bmod 11^2 = 121,\\
x &\equiv 11,\ 12,\ 13,\ 24,\ 25,\ 26,\ 37,\ 38,\ 39,\ 50,\ 51,\ 52,\ 63,\ 64,\\
&\quad 65,\ 76,\ 77,\ 78,\ 89,\ 90,\ 91,\ 102,\ 103,\ 104,\ 115,\ 116,\ 117,\ 128,\\
&\quad 129,\ 130,\ 141,\ 142,\ 143,\ 154,\ 155 \text{ or } 156 \bmod 13^2 = 169.
\end{aligned}$$

By a numerical calculation, I find out that the smallest value of x is 1184623. It is obviously to see that $15! < 1184623 \cdot 1184624 \cdot 1184625$, and this case confirms my assumption again.

6.5 Conclusion

When I was studying the results or proofs set out in this thesis, I found that there are lots of steps that the authors did not explain clearly. However, for me, or those people who start to do research in mathematics, we need better explanations for many of steps. Therefore, one of the purposes in writing this thesis is to create an accessible tool for readers. Foremost, I hope to contribute to this subject after I made improvements for some original researches and gave some my own ideas.

Here I will give a brief conclusion and show you all improvements I made.

In Chapter 2 for example, I improved on the work of Dabrowski. In Chapter 3, I have worked hard on proving Theorem 3.1, I gave Lemma 3.3 and Lemma 3.4, which were not explained in the original article [19] but were applied as known results. I had a lot of fun when I was working on Section 3.4, where I discussed some other related equations, like $n! = x^2 \pm y^2$ and $n! = x^2 + y^2 + z^2$. I figured out some conditions in which these equations have a solution or have not. Especially for the case $n! = x^2 + y^2 + z^2$, there are a few new developments. Moreover I found for one subsequence $(60, 120, 240, 480, \ldots)$, the theorem I stated falls short of giving a characterization of every n on the list, which is not less interesting than Brocard's problem for me.

In Section 3.5, I translated the German article [13] and improved the presentation of the results in Section 3.5.1. The most important improvement is that, I established Lemma 3.14, which is about the relation between the prime factor of $(1+a)(1+2a)...(1+(m-1)a)$ and $m!$. I took two more pages to state and prove this result. Also, I used the characterization of the factors $T(n, a, b)$ of $n!$ and showed two explicit examples for different values of p to solve $n! = x^p - y^p$, which has no solutions. For the case that $p = 3$ and $y = 1$, I proved it in a different way from the original article.

In terms of the result of Richard Pollack and Harold Shapiro, the ideas are totally new for me, so my presentation follows the same basic approach as Pollack and Shapiro's work, but with many improvements and enhancements. For each proof of lemmas they employed, I gave more details from step to step than the original article. So I hope it is helpful for people to understand their approach.

As for the last chapter, some different and new thoughts were given from the result of Daniel Betrend and Jorgen E.Harmse. By studying and applying their ideas, I discussed the equation $n! = x^2 - A$ where A is square-free in a different way from Dabrowski's work. I gave a few examples in Section 6.2 and concluded that there are only a finite number of solutions for this type of equation. In Chapter 6, Theorem 6.2 is important and useful for solving some type of polynomials. However, it is not proved in the original article. Under the assistance of my professor, I figured out and gave a clear proof.

One of main purposes in Chapter 6 is to give some polynomials such that $P(x) = n!$ has no solutions. We tried various methods to solve the cases $n! = x(x+2)$ and $n! = x(x+1)(x+2)$ respectively. Especially for the latter case, I discovered the pattern of the power of prime factors in $x(x+1)(x+2)$, which I think is quite useful information for me or people who work on this polynomial. Next I showed how to use my method and prove that the equation $n! = x(x+1)(x+2)$ has no solutions for all $n > 6$. Even though the method is not strong enough to give a complete proof, I believe that the pattern of the power of prime factors in $x(x+1)(x+2)$ and my method will be applied successfully one day.

For proving Theorem 6.3 and Lemma 3.8, I applied Mathematica and gave the concluding remarks by some matrices, which I developed in my thesis as well.

Each of the methods and results given in this thesis is deficient, in that it does not provide a solution for Brocard's original conjecture, namely that

$$\begin{aligned} 4! + 1 &= 5^2, \\ 5! + 1 &= 11^2, \\ 7! + 1 &= 71^2. \end{aligned}$$

are the only solutions to $n!+1 = x^2$ in positive integers. It is trivial to check these are solutions. I checked values of $n!+1$ for $8 \leq n \leq 130,000$ and found no perfect square, indeed no powerful value. Other references have probably checked a much larger range. Since the problem has been in existence for over 127 years, it is very likely that these are the only solutions.

Except for the ABC conjecture based proof, the methods described here solve closely related problems. It seems that none of them provide methods for solving the original problem. Even the ABC conjecture based proof is deficient, in that it gives a finite number of solutions, and that finite number is unknown. Even if it was known, it could be large.

So I did not manage to solve the original problem. Of the ideas I stumbled over, perhaps the sieving idea used in Section 3.4.3, or the Chinese Remainder Theorem based idea of Section 6.4 are the most promising. Time did not permit further development of these ideas. For the closely related problems I found $n! = x(x+1)(x+2)$ to be the most promising. It has the form $a!b! = c!$, compared with the original Brocard's problem $a!b! = 4c!$.

References

[1] T.M.Apostol, *Introduction to Analytic Number Theory*, Springer, (1976), ISBN 978-0-387-90163-3.

[2] D.Berend and J.E.Harmse, *On polynomial-factorial diophantine equations*, Transactions of the American Mathematical Society, **358** (2005), 1741--1779.

[3] D.Berend and Osgood, C.F., *On the equation $P(x) = n!$ and a question of Erdös*, Journal of Number Theory **42** (1992), 189--193.

[4] H.Brocard, *"Question 166"*, Nouv. Corres. Math. **2:** 287.

[5] H.Brocard, *"Question 1532"*, Nouv. Corres. Math. **4:** 391.

[6] R.Breusch, *Zur Verallgemeinerung des Bertrandschen Postulates, daß zwischen x und $2x$ stets Primzahlen liegen*, Math. Journal **34** (1932), 505--526; P.Erdös, *Über die Primzahlen gewisser arithmetischer Reihen*, Math.Journal **39** (1935), 473--491.

[7] Eugéne Charles Catalan, *Note extraite dune lettre adressée à léditeur* J. Reine Angew. Math. **27** (1844), 192.

[8] A.Dabrowski, *On the Diophantine Equation $x! + A = y^2$*, Nieuw Archief Voor Wiskunde **14** (1996), 321--324.

[9] P.G.L.Dirichlet, *Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält*, Abhand. Ak. Wiss. Berlin **48** (1837).

[10] U. Dudley, *A Guide To Elementary Number Theory*, Mathematical Association of America, (2009), ISBN:978-0883853474.

[11] L.Euler, 1747. S. z. B. *Commentationes Arithmeticae Collectae* (Petropoli, 1849), I, p. 50. und II, p. 523. Auch in Lehrbüchern, s. z. B. G. WERTHEIM, *Anfangsgründe der Zahlenlehre* (Braunschweig, 1902), 298.

[12] P.Erdös,*Advanced Problem 4226*, Amer. Math. Monthly **53** (1946), 594. Solution by W.J.Harrington. Amer. Math. Monthly **55** (1948), 433--435.

[13] P.Erdös, and R.Obláth, *Über diophantishe Gleichungen der Form* $n! = x^p \pm y^p$ *und* $n! \pm m! = x^p$, Acta Litt. Sci. Szeged **8** (1937), 241--255.

[14] A.A.Gioia, *The Theory of Numbers: An Introduction*, Dover Publications **3** (2001), ISBN 0-486-41449-3.

[15] A.Granville, R.A.Mollin and H.C.Williams, *An upper bound for the least inert prime in a quadratic field*, Canad. J. Math. **52** (2000).

[16] D. R. Heath-Brown, *Zero-free regions for Dirichlet L-functions and the least prime in an arithmetic progression*, Proc. London Math. Soc (3) **64** (1992), 265--338.

[17] G.H.Hardy and E.M.Wright. *An Introduction to the Theory of Numbers*, Oxford University Press **5** (1979), 310--311.

[18] K.H.Rosen, *Elementary Number Theory and Its Applications*, Monmouth University, **3** (2011), ISBN-13: 978-0201578898.

[19] J.M.De Koninck and F.Luca, *Analytic number theory; exploring the anatomy of integers*, American Mathematical Society (2012), ISBN-13: 978-0821875773.

[20] E.Landau, *Handbuch Der Lehre Von Der Verteilung Der Primzahlen*, Vol. I, Teubner, Leipzig, (1909).

[21] F. Luca, *The diophantine equation* $P(x) = n!$ *and a result of M. OVERHOLT,Glas.* Mat. Ser. *III* **37**(**57**)(2002), 269--273.

[22] Yu. V. Linnik, *On the least prime in an arithmetic progression I.* The basic theorem Rec. Math. (Mat. Sbornik) N.S. **15** (**57**) (1944), 139--178.

[23] Yu. V. Linnik, *On the least prime in an arithmetic progression II.* The Deuring-Heilbronn phenomenon Rec. Math. (Mat. Sbornik) N.S. **15** (**57**) (1944), 347--368.

[24] K.Molsen, *Zur Verallgemeinerung der Bertrandschen Postulates*, Deutsche Math. **6** (1941), 248--256.

[25] D. W. Masser, *Open problems*, in Chen, W. W. L., Proceedings of the Symposium on Analytic Number Theory, London: Imperial College (1985).

[26] Preda Mihailescu, *Primary Cyclotomic Units and a Proof of Catalan's Conjecture*, J. Reine angew. Math. **572** (2004), 167--195.

[27] M.B. Nathanson, *Elementary methods in Number Theory*, Springer, (2000), ISBN 0-38798912-9.

[28] Joseph Oesterlé, *Nouvelles approches du thorme de Fermat*, Astérisque, Séminaire Bourbaki exp 694 (161) (1988), 165--186.

[29] M. Overholt, *The Diophantine Equation* $n! + 1 = m^2$, Bull.London Math.Soc. **42** (1993), 104.

[30] R.M.Pollack and H.N.Shapiro, *The Next to Last Case of a Factorial Diophantine Equation*, Communications on pure and applied mathematics, **26** (1973), 313--325.

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

[32] E.Trevino, *Numerically explicit estimates for character sums*, PhD Thesis, Dartmouth College (2011).

[33] L. Szpiro, *Seminaire sur les pinceaux des courbes de genre au moins deux*, Astérisque **86** (1981), 44--78.

[34] L. Szpiro, *Présentation de la théorie d'Arakelov*, Contemp. Math. **67** (1987), 279--293.

[35] I. M. Vinogradov, *On the distribution of residues and non-residues of powers*, J. Physico-Mathematical Soc. of Perm **1** (1918), 94--96.

[36] E.T.Whittaker and G.N.Watson, *Modern Analysis*, Camb. Univ. Press, (1944), ISBN 0-521-09189-6.

[37] Stothers, W. W., *Polynomial identities and hauptmoduln*, Quarterly J. Math. Oxford, 2 **32** (1981), 349--370.

[38] *http://www.math.unicaen.fr/ nitaj/abc.html*

[39] *http://en.wikipedia.org/wiki/Cyclotomic polynomial*