JOHANNES KEPLER
UNIVERSITÄT LINZ
Netzwerk für Forschung, Lehre und Praxis

Symbolic computation in number theory

Dissertation

zur Erlangung des akademischen Grades

Doktor der Technischen Wissenschaften

Angefertigt am *Institut für Symbolisches Rechnen*

Betreuung:

Univ.-Prof. Dr. Franz Winkler
A. Univ.-Prof. Dr. Heinrich Rolletschek

Eingereicht von:

M.Sc. M.Sc.(Engg.) Rahul Ramesh Athale

Linz, Dezember 2004

Abstract

We used symbolic computation methods to analyse two number theory problems. We implemented some of these methods in the computer algebra systems Mathematica, Maple, and Macaulay. So the thesis consists of two parts. The first part deals with the work on prime gaps and the second one is about the generation of elliptic curves with high rank.

We carried out extensive computations to determine the validity of the conjecture regarding takeover point of 210 as the most frequent prime gap from 30. Also, we wrote a program in Mathematica to compute the approximate number of gaps up to a given positive integer. We apply statistical tests to the computed data and based on the results of those tests, we improve the takeover point in the jumping champion conjecture. We also consider the prime gaps modulo 6. We formulate a new conjecture based on the following observation: The number of gaps congruent to 0 modulo 6 equals approximately the number of gaps not congruent to 0 modulo 6.

In the second part, we discuss the method suggested by Yamagishi for the generation of the elliptic curves with high rank. We studied this approach extensively and implemented the method in Maple. We found some examples where this method does not produce the elliptic curves with desired rank. We suggest certain constraints on the parameters in Yamagishi's method to get the elliptic curves with desired rank in the case of rank 2. We also prove one of the required results using Macaulay.

Zusammenfassung

Wir haben Methoden des symbolischen Rechnens angewandt, um zwei Probleme in der Zahlentheorie zu analysieren. Einige dieser Methoden haben wir in den Computeralgebra Systemen Mathematica, Maple und Macaulay implementiert. Der erste Teil behandelt die Untersuchung von Primzahllücken (prime gaps) und im zweiten Teil geht es um die Erzeugung elliptischer Kurven hohen Rangs.

In umfangreichen Berechnungen haben wir die Gültigkeit der Vermutung über die Ablösung von 30 als häufigste Primzahllücke durch 210 untersucht. Wir haben auch ein Programm in Mathematica geschrieben zur approximativen Berechnung der Lücken unterhalb einer positiven ganzen Zahl. Wir wenden statistische Tests auf die erzeugten Daten an, und aufbauend auf diesen Tests geben wir eine Verbesserung des Punktes an, ab welchem der neue "Jumping Champion" überwiegt. Wir untersuchen auch Primzahllücken modulo 6. Wir formulieren eine neue Vermutung, welche sich auf die folgende Beobachtung stützt: die Zahl der Lücken, welche kongruent zu 0 sind modulo 6, gleicht in etwa der Zahl der Lücken, welche nicht kongruent zu 0 sind modulo 6.

Im zweiten Teil diskutieren wir die von Yamagishi vorgeschlagene Methode zur Erzeugung elliptischer Kurven hohen Rangs. Wir haben diesen Zugang eingehend untersucht und die Methode in Maple implementiert. Wir haben einige Beispiele gefunden, in denen diese Methode nicht die elliptische Kurve des gewünschten Rangs erzeugt. Wir schlagen gewisse Bedingungen an die Parameter in Yamagishis Methode vor, um im Fall von Rang 2 Kurven des gewünschten Rangs tatsächlich zu erzeugen. Wir verwenden Macaulay, um ein notwendiges Zwischenresultat zu beweisen.

Contents

Contents i

List of Tables iv

List of Figures vi

Acknowledgements vii

1 Introduction 1

I Prime GAPS 3

2 What are prime gaps? 5
- 2.1 Prime numbers 5
- 2.2 Prime gaps 8
  - 2.2.1 Finding first occurrence of prime gaps 10
  - 2.2.2 Finding prime pairs with the given prime gap 11
- 2.3 Definition of jumping champion 13

3 Theory of jumping champions 15
- 3.1 Brun's simple pure sieve 15
  - 3.1.1 General sieve problem 15
  - 3.1.2 Brun's simple pure sieve 16
  - 3.1.3 Application to the twin prime problem 18
- 3.2 Jumping champion tends to infinity 22
  - 3.2.1 An application of Brun's method 23
- 3.3 The candidates 23
  - 3.3.1 The k-tuple conjecture 24
  - 3.3.2 The heuristics 25
- 3.4 The takeover points 27
  - 3.4.1 Takeover point between 6 and 30 28
  - 3.4.2 Takeover point between 30 and 210 28

4 Computational results 29
4.1 Computations near the conjectured takeover points 29
4.1.1 Verifying the takeover point between 30 and 210 30
4.1.2 Comparing the behaviour of 30 and 210 near the takeover points 33
4.2 Statistical analysis 35
4.2.1 Non-parametric test 37
4.2.2 Parametric test 38
4.3 Prime gaps modulo six 38
4.4 Role of symbolic computation 41
4.5 Miscellaneous results 42

II RANKS of elliptic curves 43

5 Elliptic curves 45
5.1 Basic algebraic geometry notions 46
5.1.1 Affine variety 46
5.1.2 Dimension of an affine variety 47
5.1.3 Local properties of plane curves 49
5.1.4 Projective algebraic geometry 50
5.1.5 Dimension of a projective variety 51
5.2 What is an elliptic curve? 52
5.2.1 Nonsingularity of E 53
5.2.2 Cubic to Weierstrass 55
5.3 The group of rational points 57
5.3.1 Geometric version of the addition of rational points 58
5.3.2 Algebraic version of the addition of rational points 63
5.4 Structure of the group 64
5.5 Determination of the torsion group 65

6 Generation of elliptic curves with high rank 69
6.1 Determination of the rank 69
6.2 Brown-Myers approach 70
6.2.1 Rational torsion and curves over finite fields 71
6.2.2 Computing the rank of E_m 72
6.2.3 Rank 3 and beyond 74
6.3 Yamagishi approach 76
6.3.1 Generic case and its specialisation 76
6.3.2 Case of rank 2 78

7 Computational results 81
7.1 Dimension of V_n is 3 81
7.2 Implementation results of Yamagishi's algorithm 83
7.2.1 Maple code 83
7.2.2 Bad choices for the input arguments 85
7.2.3 Results with good input arguments 85
7.3 Results from other rank computations 86

Bibliography 89

List of Tables

9 First occurrence of small prime gaps

14 Jumping champions for small positive integers

28 A rough estimate of takeover point between jumping champions

30 Significant prime gaps in the interval of length 10^7 starting from $10^{410}, 10^{420}, \ldots, 10^{550}$

31 Significant prime gaps in the interval of length 10^7 starting from $10^{425}, 10^{426}, \ldots, 10^{435}$

32 Significant prime gaps in the interval of length 10^8 starting from $10^{430}, 10^{435}, 10^{455}, 10^{475}$

33 Comparison of number of prime gaps of size 30 and 210 in the interval of length 10^7 starting from random numbers in the range 10^{425} to 10^{429}

34 Comparison of number of prime gaps of size 6 and 30 in the intervals of length 10^7 and 10^8
- (i) Interval length 10^7
- (ii) Interval length 10^8

35 Comparison of the number of gaps in the intervals of different sizes
- (i) Comparison between 6 and 30
- (ii) Comparison between 30 and 210

36 Rank determination for Wilcoxon singed-rank test

39 The distribution of prime gaps modulo six in the interval 3 to 10^{10}

40 The distribution of prime gaps modulo six in the interval of size 10^8 and 10^7 starting from $10^{10}, 10^{20}, \ldots, 10^{100}, 10^{125}, \ldots, 10^{375}$
- (i) Interval length 10^8
- (ii) Interval length 10^7

41 Comparison of the distribution of prime gaps modulo six in the intervals of size 10^7 and 10^8 starting from $10^{100}, 10^{125}, 10^{150}, 10^{175}$

42 Big prime gaps with their starting prime

85 Examples of parameter values for Yamagishi's method where we do not get the elliptic curves with the desired rank
86 Ranks of curves generated randomly using implementation of Yamagishi's method for rank 2
87 Ranks of elliptic curves of type $y^2 = x^3 - x + m^2$ and $y^2 = x^3 - t^2x + 1$
(i) $y^2 = x^3 - x + m^2$
(ii) $y^2 = x^3 - t^2x + 1$

List of Figures

32 The number of prime gaps of size $d = 2, 4, , \ldots, 6000$ in the interval of length 10^8 starting from 10^{475}

59 Addition of two distinct points on an elliptic curve $E : y^2 = x^3 - 5x + 3$ defined over the field of real numbers $\mathbb{R}$

60 Computing $2P$ for a point P on an elliptic curve $E : y^2 = x^3 - 5x - 3$ defined over the field of real numbers $\mathbb{R}$

Acknowledgements

I thank all who have
loved me in their hearts,
With thanks and love from mine.
Deep thanks to all.

Sonnets From the Portuguese, 1850
Elizabeth Barrett Browning

First of all, I thank Prof. Franz Winkler, my adviser. His questions gave new directions to my work. He was always there to help me in academic as well as other problems, thank you so much. Prof. Bruno Buchberger taught us an important lesson "as simple as possible, as complicated as necessary". I thank him by trying to emulate his teaching in the thesis. I thank Prof. Josef Schicho and Prof. Heinrich Rolletschek for giving and pointing me to the important books that set the direction for the further work. I also appreciate Prof. Rolletschek's suggestions in prime gaps part of the thesis. I thank Prof. Günter Landsmann for the helpful discussions. I thank Greg Curtis for explaining subtleties in the English language. The system administration group helped me when I carried out the computations for my work and at other times, I thank Prof. Karoly Erdei, Werner Danielczyk-Landerl, and Peter Pregler. I thank Dr. Thomas Natschläger for explaining the intricacies of statistical tests.

I thank Prof. Franz Lichtenberger for his consideration and encouragement for my work on the thesis while working in SCCH. I also thank Dr. Klaus Pirklbauer and Mr. Mario Drobics for their help and consideration.

Special thanks are due to the secretaries at RISC and SCCH, Ramona, Betina, Isabel and Sandra, without you I would have needed at least two more months to complete the thesis, the time I would have spent in getting various documents during my stay in Austria.

I thank Harvey Dubner for providing me the computational data and for the joint work. I thank Hizuru Yamagishi for explaining details from her paper and translating her thesis in English for me. I also thank Andrew Odlyzko and Carl Pomerance for the discussions regarding my work on jumping champion and prime gaps modulo six, your comments gave a new insight.

I thank MiKTEX team for the Windows version of up-to-date TEX implementation. I thank Peter Wilson for writing wonderful `memoir` class for LATEX and also solving some of my typesetting problems. It was much easier to typeset the thesis with `memoir` class. Also I thank many people who spent their valuable time to give me solutions, sometimes in few minutes, for my LATEX problems on `comp.text.tex` newsgroup.

The suggestions and comments on my starting design of the thesis, on the forum on `http://www.typophile.com`, by professional designers and typesetters, helped a lot in understanding the basic concepts of typesetting. I thank them for their consideration and patience during my learning phase.

I thank Glauco Alfredo Lopez Diaz for our discussions. I thank Mohamed Shalaby and his family for Arabic food and their hospitality, Christian Vogt for coffee table discussions and of course coffee, Gabor Kusper and his mother for cookies, Cleo Pau for conversations on Indian movies, Cleo Pau, Petru Pau, Florina Piroi, Claudio Dupre, Fabrizio Caruso, Daniela Vasaru for great parties. They all made my life, in this foreign land, colourful, which directly or indirectly helped in the research.

To some people one cannot thank, one can only be grateful to. I am grateful to my parents for standing by me throughout my student years. Some are so part of your life and you that you don't even mention them.

I dedicate this thesis to my new beginning,

SIRA.

CHAPTER I

Introduction

> Man's ultimate concern must be expressed symbolically, because symbolic language alone is able to express the ultimate.
>
> *Dynamics of faith, 1957*
> Paul Tillich

The thesis consists of two parts. The first part deals with the work on prime gaps and the second one is about the generation of elliptic curves with high rank. We develop the definitions and theory needed in each part separately. The work in both parts is not related in the results obtained, but is related by the tool used, namely symbolic computation, to study them.

In 1980, Erdős and Strauss proved that the most frequent prime gap keeps on changing as we go to infinity. This poses a new question. What is the most frequent prime gap up to a given positive integer? What are the changing points? We carried out extensive computations to determine the validity of the conjecture regarding takeover point of 210 as the most frequent prime gap from 30. Also, we wrote a program to compute the approximate number of gaps up to given positive integer using Mathematica, please see Wolfram [1999] to know more about Mathematica. Using this program we could determine the approximate takeover point. Our work is described in the fourth chapter.

We apply statistical tests to the computed data and based on the results of those tests, we improve the takeover point in the jumping champion conjecture. We also consider the prime gaps modulo 6. We formulate a new conjecture based on this: The number of gaps congruent to 0 modulo 6 euals approximately the number of gaps not congruent to 0 modulo 6.

In 1999, Yamagishi gave a unified method to generate elliptic curves with high rank. We studied this approach extensively. We report examples that are not mentioned in the original work, which generate elliptic curves with lower

rank than the desired one. We implemented this method and used it to generate elliptic curves. We suggest certain constraints on the parameters in Yamagishi's method to get the elliptic curves with desired rank. We also prove some of the results in the original paper. The proof of one of the result is easier than the original proof given in the paper. The other proof was not given in the paper. We used Maple for implementation of the above method and Macaulay for a proof. Please see Char et al. [1991] for Maple system details and Eisenbud et al. [2001] for Macaulay. Our work, the parametrisation of variety in case of rank 2, is described in the last subsection of the sixth chapter, and the simpler proof of the fact that the dimension of the variety is 3, implementation details and other computations form the seventh chapter.

Part I

Prime GAPS

It will be another million years, at least,
before we understand the primes.

P. ERDŐS

CHAPTER 2

What are prime gaps?

> A lady is nothing very specific.
> One man's lady is another man's
> woman; sometimes, one man's
> lady is another man's wife.
> Definitions overlap but they
> almost never coincide.
>
> *Is There a Lady in the House, in Look*
> *(New York, 22 July 1958)*
> J. Russel Lynes

In the Mathematics world, prime numbers are well known and have been studied extensively since early Greek mathematicians of 500 B.C. Nowadays computer savvy people know them as they are the building blocks of secure cryptosystems. Also they are popular amongst the Internet users, as many users join in the search for the large primes (with thousands of digits) by utilising their idle computer time. But, there is still an argument going on over whether 1 should be called prime or composite or should have its own category. Therefore, we begin with the definitions. We will also state the necessary theorems just before they are first applied.

2.1 Prime numbers

The *positive integers* are the numbers $1, 2, 3, \ldots$. These numbers are also known as the *natural numbers*.

Definition 1. A *prime number* is a positive integer $p > 1$ that has no positive integer divisors other than 1 and p itself.

For example, the only divisors of 2 are 1 and 2 itself, making it a prime number. On the other hand, if a positive integer greater than one has more than two divisors, it is called a *composite number.* For example, 4 has three divisors, 1, 2 and 4. We say 2 is a *factor* or divisor of 4.

In a sense, the prime numbers form the building blocks of positive integers. The fundamental theorem of arithmetic states, every positive integer is either a prime or can be uniquely factored as a product of prime numbers in a unique way. For example, $4 = 2 \times 2$.

How one can find a prime number and how many prime numbers are there? Eratosthenes gave an answer to the first question in 200 B.C. He gave an algorithm, which is called *sieve of Eratosthenes.* It is elegant. The Sieve of Eratosthenes identifies all the prime numbers up to a given positive integer n as follows:

$m := 2$; lim $:= \lfloor \sqrt{n} \rfloor$;
mark 1 as special
WHILE $m \leqslant$ lim DO
  include m in list of primes
  cancel multiples of m
  increase m to the next unmarked number
END WHILE
append unmarked numbers to list of primes

Suppose we want to find the prime numbers up to 10. Let us use the sieve of Eratosthenes to find them.
Initial values:
$k := 1$; $l := \{\}$, l is the list of prime numbers

Ⓘ 2 3 4 5 6 7 8 9 10

Initially all numbers are unmarked.
Step one:
$m = 2$; $l = \{2\}$; $k = 2$

Ⓘ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ 9 ~~10~~

The special status of 1 is denoted by circling it, like Ⓘ . The composite numbers are struck through, like ~~4~~.
Step two:
$m = 3$; $l = \{2, 3\}$; $k = 3$

Ⓘ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~

Step three:
$m = 5$; $l = \{2, 3, 5\}$; $k = 5$

Ⓘ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~

Step four:
$k > \sqrt{10}$ therefore we exit the algorithm with $l = \{2, 3, 5, 7\}$.

The answer to the second question, how many primes are there, was given in 300 B.C. by Euclid.

THEOREM 1. *The number of primes are infinite.*

Proof. Suppose that there are only finitely many primes, say n. Let $p_1 = 2, p_2 = 3, \ldots, p_n$ be all of them. Let

$$N = 2 \times 3 \times 5 \times \cdots \times p_n + 1$$

Then $N \neq 1$ so by the fundamental theorem of arithmetic

$$N = q_1 \times q_2 \times \cdots \times q_m$$

where each q_i is prime and $m \geqslant 1$. If q_1 is one of the prime numbers from our finite list $\{2, 3, 5, \ldots, p_n\}$, then we can write $N = q_1 a + 1$ for some $a \in \mathbb{Z}$. As $q_1 \nmid 1$, we have $q_1 \nmid N$, a contradiction. Thus our assumption that $\{2, 3, 5, \ldots, p_n\}$ are all of the primes is false, which proves that there must be infinitely many primes. □

The proof of the above theorem can be found in any elementary number theory book, for example in this online in progress book by Stein. The number of primes up to a positive integer x is given by the *prime number theorem.*

THEOREM 2. *The number of primes not exceeding* x *is asymptotic to* $\frac{x}{\ln x}$, *where* $\ln x$ *denotes the natural logarithm of* x.

Please see subsection 3.1.2 for the definition of asymptotic. In other words, the number of primes less than or equal to x, denoted by $\pi(x)$, are approximately $\frac{n}{\ln x}$.

The interesting fact about primes is that there are still plenty of unanswered questions. Guy [1981] has a whole section devoted to unsolved problems concerning primes.

The question we discuss here is about the distribution of the prime numbers. What does this mean? It actually involves variety of problems. For instance, we wish to have an estimate for the number of primes up to a limit x, as it is given by Theorem 2. Another question is whether or not there exist infinitely many primes of a certain special form. A famous result in this respect is

THEOREM 3. *If* k *and* l *are relatively prime positive integers, then the arithmetic progression* $l, l + k, l + 2k, l + 3k, \ldots$ *contains infinitely many primes.*

Of course, the two kinds of questions may be combined by asking for the number of primes of the form $kd + l$ up to x. Along with the prime number theorem it was shown that it is asymptotic to $\frac{x}{\phi(k) \ln x}$, where $\phi(k)$ denotes the number of integers between 0 and k that are coprime with k, which means that there exist approximately the same number of primes in each relatively prime congruence class $\mod k$. For example, let us consider $l = 1$ and $k = 4$. We get that there are infinitely many primes of the form $4d + 1$, where d is a positive

integer. Also we get the number of primes of the form $4d + 1$ up to x is $\frac{x}{2 \ln x}$. Yet another question of interest concerns prime gaps, that is, intervals between two consecutive prime numbers. This is the question we discuss next.

We do not study the distribution in this sense, rather we are looking at the difference or gap between consecutive primes.

2.2 Prime gaps

DEFINITION 2. A *prime gap* G is the interval bounded by two consecutive prime numbers p_k and p_{k+1}.

DEFINITION 3. The *measure* or *size* g of a prime gap G is the difference $g = p_{k+1} - p_k$ of its bounding primes.

A prime gap is often specified by its measure g and its initial prime p_k, denoted as p_1. A prime gap of measure g contains $g - 1$ consecutive composite integers. Since two is the only even prime, every prime gap is of even measure, with the sole exception of the prime gap of measure 1 following the prime 2.

It is an elementary fact that gaps of arbitrarily large measure exist. For $n > 0$ the integer $(n + 1)! + 1$ must be followed by at least n consecutive composites, divisible successively by $2, 3, \ldots, n + 1$. Note that, $n + 1$ represents only a lower bound on the measure of such gaps.

DEFINITION 4. The *merit* M of a prime gap of measure g following the prime p_1 is defined as $M = \frac{g}{\ln p_1}$.

It is the ratio of the measure of the gap to the *average* measure of gaps near that point; as a consequence of the prime number theorem, the average difference between consecutive primes near x is approximately $\ln x$.

DEFINITION 5. A prime gap of measure g is considered a *first occurrence* prime gap when no smaller consecutive primes differ by exactly g.

Thus, the gap of 4 following 7 is a first occurrence, while the gap of 4 following 13 is not. Note that this usage of the compound adjective *first occurrence* carries no implication whatsoever regarding historical precedence of discovery. Table 9 gives the first occurrence of prime gaps up to 50, the merit of the gap, and the prime from which it starts. The detailed list can be found at the web site by Nicely. The web site gives the first known occurrence of prime gaps and also whether it is the confirmed first occurrence or not. The site also reports many big gaps. I had also reported many gaps to the maintainer of the site, about that I will write in the fourth chapter.

DEFINITION 6. A prime gap of measure g is called *maximal* if it strictly exceeds all the preceding gaps, i.e., the difference between any two consecutive smaller primes is less than g.

Gap	Merit	Following the prime
1	1.44	2
2	1.82	3
4	2.06	7
6	1.91	23
8	1.78	89
10	2.03	139
12	2.27	199
14	2.96	113
16	2.13	1831
18	2.88	523
20	2.95	887
22	3.13	1129
24	3.23	1669
26	3.33	2477
28	3.50	2971
30	3.59	4297
32	3.71	5591
34	4.73	1327
36	3.93	9551
38	3.68	30593
40	4.05	19333
42	4.33	16141
44	4.55	15683
46	4.07	81463
48	4.68	28229
50	4.82	31907

TABLE 9: First occurrence of small prime gaps

Thus the gap of 6 following the prime 23 is a maximal prime gap, since each and every smaller prime is followed by a gap less than 6 in measure; but the gap of 10 following the prime 139, while a first occurrence, is not maximal, since a larger gap (the gap of 14 following the prime 113) precedes it in the sequence of integers. The maximal prime gaps are *ipso facto* first occurrence prime gaps.

How do we find the first occurrence of a prime gap? No general method more sophisticated than an exhaustive search is known for the determination of first occurrence and maximal prime gaps, please see Nicely, 1999. Nicely [1999]; Nyman and Nicely [2003] use some fast sieving techniques, which are improvements in the sieve of Eratosthenes algorithm stated earlier, to carry out the exhaustive search. These techniques have helped to check the first occurrence

of prime gaps faster, currently all the prime gaps up to 5×10^{16} are known.

To find consecutive primes with a given gap there are two possible options: The program written by Nicely and the algorithm given by Cutter.

2.2.1 Finding first occurrence of prime gaps

Nicely has written a program in UBASIC to search for given prime gaps in a given interval. The program is available from Nicely. It is inspired by the code developed by Harvey Dubner based on the concepts and strategies described in Dubner and Nelson [1997]. We sketch the main idea from the original paper.

We first state the theorem used in this method and also in the next subsection, known as *Chinese remainder theorem*. It can be found in any elementary number theory book. We state it from a web site called MATHWORLD, the web's most extensive mathematics resource, Weisstein.

THEOREM 4. *Given a set of simultaneous congruences*

$$x \equiv a_i \pmod{m_i}$$

for $i = 1, \ldots, r$ *and for which the* m_i *are pairwise relatively prime, the solution of the set of congruences is*

$$x = a_1 b_1 \frac{M}{m_1} + \cdots + a_r b_r \frac{M}{m_r} \pmod{M},$$

where

$$M = m_1 m_2 \cdots m_r$$

and the b_i *are determined from*

$$b_i \frac{M}{m_i} \equiv 1 \pmod{m_i}.$$

The method for finding a prime gap of given size uses a system of simultaneous modular equations to guarantee that a specific sequence of numbers will be composite.

Consider the system of modular equations,

$$x \equiv b_j \pmod{p_j}, \qquad p_j = j\text{th prime}. \tag{2.1}$$

The Chinese Remainder Theorem states that there is always a solution for x satisfying Equation (2.1), with

$$0 \leqslant x < m, \qquad m = \prod_j p_j. \tag{2.2}$$

For each j, starting at a number determined by x and b_j, every p_jth number is divisible by p_j and so is composite. For r equations, the set of b_j's determine a

particular pattern of composite numbers. By adding to the number of equations and selecting appropriate b's, more numbers join the composite pattern. In this manner any selection of numbers can be made composite. Using this approach it is faster to search for the bigger prime gaps.

The user has to download freely available UBASIC to run the program. The user can choose the range of positive integers in which the given prime gap is searched. Also all the gaps bigger than the user's choice are reported.

2.2.2 Finding prime pairs with the given prime gap

The first systematic method to find the consecutive primes with a given gap was given by Cutter, in Cutter [2001]. We reproduce the algorithm from the original paper along with the necessary theorem.

In 1928, D. H. Lehmer found out that if $p-1=qr$ where $q>p^{1/2}$ is factored, then there is a quick, practical way to show if p is a prime. In 1975, this result was extended by Lehmer, Brillhart and Selfridge, so that one only needs to have the factored part $q>p^{1/3}$ to get a quick test. The primality test is based on the following theorem.

THEOREM 5. *Let* $n-1=qr$, *where* q *is factored,* $q>n^{1/3}$ *and* $(q+1)^2\neq n$. *Assume that, for each prime* p_k *dividing* q, *there exists an* a_k *such that*

(i) $a_k^{n-1}\equiv 1 \pmod{n}$, *and*

(ii) $\gcd(a_k^{\frac{n-1}{p_k}}-1,n)=1$.

Write $r=2qs+t$ *where* $1\leqslant t<2q$. *Then* n *is prime if and only if* $s=0$ *or* t^2-8s *is not the square of an integer.*

To apply this to the prime gap problem, we need to have partial factorisations of $p-1$ and $p+g-1$, where g is the measure of the gap. To do this, we proceed as follows: For a given even integer g, we select a and b to be the largest integers with $2^a, 3^b < e^{g/4}$, where e is the base of the natural logarithm. Using Theorem 4, we select p_o to be the least positive integer modulo 2^a3^b satisfying

$$\text{if } g\equiv 2 \pmod 3, \text{ then } p_o\equiv 1 \pmod{2^a} \text{ and } p_o+g\equiv 1 \pmod{3^b},$$
$$\text{if } g\not\equiv 2 \pmod 3, \text{ then } p_o\equiv 1 \pmod{3^b} \text{ and } p_o+g\equiv 1 \pmod{2^a}.$$

The case distinction is needed, for if $g\equiv 2 \pmod 3$ and we select $p_o \pmod{2^a3^b}$ such that $p_o\equiv 1 \pmod{3^b}$ and $p_o+g\equiv 1 \pmod{2^a}$, then 3 would divide p_o+g. If we select $p_o \pmod{2^a3^b}$ such that $p_o\equiv 1 \pmod{2^a}$ and $p_o+g\equiv 1 \pmod{3^b}$, then we would have that 3 divides p_o when $g\equiv 1 \pmod 3$. Selecting $p\equiv p_o \pmod{2^a3^b}$ with $p<\min(2^{3a-1},3^{3b-1})$, we get $p-1$ and $p+g-1$ divisible by 2^a and 3^b (the order depending on $g \pmod 3$). Note that 2^a and 3^b are factors $>(p+g)^{1/3}>p^{1/3}$. Therefore we can use Theorem 5 to determine whether p and $p+g$ are prime.

The algorithm

The algorithm used for finding the consecutive primes with a given gap g is as follows.

STEP ONE: Find p_0, 2^a and 3^b as stated above.

STEP TWO: Test the numbers p of the form $p = p_0 + i2^a3^b$, as i runs from 1 to 10^6. Do not actually put all of these numbers through the primality test, as some of them may be divisible by small primes. Sieve these numbers out as follows: For each prime q up to 10^4, if i is in either of the residue classes

$$\frac{-p_0}{2^a3^b} \pmod q \quad \text{or} \quad \frac{-p_0-g}{2^a3^b} \pmod q,$$

then either p or $p+g$, respectively, will be divisible by q. So discard this value of i and store the remaining i's in a table, called $T_1(g)$.

STEP THREE: For each value of i in $T_1(g)$, use Theorem 5 to test if $p = p_0 + i2^a3^b$ is a prime. To do this, start with $a_k = 2$. If, along with the other hypotheses, conditions (i) and (ii) of Theorem 5 are met, we have a prime. If they are not satisfied, let a_k run through the primes, up to the limit 255. If we reach this limit with no success in finding an a_k, or proving p composite, then give up trying to determine the primality of this value of p and move on to the next i in $T_1(g)$. There are three ways to check that p is composite.

(i) $a_k{}^{p-1} \not\equiv 1 \pmod p$

(ii) $1 < \gcd(a_k{}^{(p-1)/b} - 1, p) < p$ where b is 2 or 3, depending on p

(iii) In Theorem 5 we have, $s > 0$ and $t^2 - 8s$ is the square of an integer

If we find an a_k which satisfies conditions (i) and (ii) of Theorem 5, then perform the same test with $p+g$ If we have primality of both p and $p+g$, we store the values p, $p+g$ and the respective a_k's in a table, call it $T_2(g)$.

STEP FOUR: For every prime pair p, $p+g$ in $T_2(g)$, determine whether the numbers $p+j$, as j runs from 1 to $g-1$, are composite. It is achieved in two steps.

(a) First check if the numbers $p+j$ are divisible by primes up to 10^4. For each prime $l < 10^4$, whenever $j \equiv -p \pmod l$, $p+j$ is divisible by l. Thus $p+j$ is composite. Store the remaining j's (those where $p+j$ is not divisible by a prime $< 10^4$) in a table $T_{3,p}(g)$.

(b) For each j in $T_{3,p}(g)$, run at least one pseudoprime test on $m = p+j$. If m is not a pseudoprime to either base 2 or 3, then it is composite and we go on to the next j in $T_{3,p}(g)$. If m should happen to pass pseudoprime tests to both the bases 2 and 3, we say m is probably prime and we disregard this prime pair p, $p+g$. Move to the next prime pair p, $p+g$ in $T_2(g)$. If all of the numbers $p+j$ where $j = 1, \ldots, g-1$, are not pseudoprimes to either base 2 or 3, then they are all composite, and we have found a consecutive pair of primes with gap g, as desired.

Please see Cutter [2001] for an example.

In the method explained in subsection 2.2.1, we can search for the prime pairs with a given gap in the interval of our choice, so we can choose smaller numbers. But we are not sure if we will get such a pair with the given gap. In the method given by Cutter, the prime pair we get is certainly not the first occurrence, and in most of the cases we will get large primes, but we are sure to get a prime pair with the given gap.

The researchers have also considered iterated differences between consecutive primes, for example Odlyzko [1993]. Let $d_0(n) = p_n$, the nth prime, for $n \geqslant 1$, and let $d_{k+1}(n) = |d_k(n) - d_k(n+1)|$ for $k \geqslant 0$, $n \geqslant 1$. A well known conjecture, usually ascribed to Gilbreath but actually due to Proth in the 19th century, says that $d_k(1) = 1$ for all $k \geqslant 1$.

2.3 Definition of jumping champion

DEFINITION 7. Given a positive integer x, a *jumping champion* is the most frequent prime gap up to x, we denote it by $D(x)$.

For example, at $x = 3$ there is only one prime gap, namely 1, so 1 is the jumping champion. At $x = 5$ both 1 and 2 appear once as a prime gap so both the numbers are jumping champions. The first question about the behaviour of jumping champions was raised by Harry Nelson in 1977–8, although he did not use the term jumping champion. The term was coined by John Horton Conway in 1993.

We reproduce Table 14 from Odlyzko et al. [1999]. The table gives the jumping champions for small positive integers, and at the end also gives a rough estimate of takeover point between jumping champions 6 and 30, and 30 and 210. The jumping champions are only mentioned for primes as they can only change when we encounter a new prime.

In Table 14 we can see that, up to 941, 2, 4 and 6 are jumping champions intermittently. After that 6 is the jumping champion till approximately 10^{35}. The entries ?30? and ?210? emphasize the fact that we still do not know when 30 or 210 become jumping champions. We also deduce from Table 14 that numbers 6, 30 and 210 are possible candidates for a jumping champion up to 10^{425}.

x	Champions for x	x	Champions for x
5	1 2	421	2 6
7	2	431	2 6
11	2	433	2
⋮	⋮	439	2 6
97	2	443	2 6
101	2 4	449	6
103	2	457	6
107	2 4	461	6
109	2	463	2 6
113	2 4	467	2 4 6
127	2 4	479	2 4 6
131	4	487	2 4 6
137	4	491	4
139	2 4	⋮	⋮
149	2 4	541	4
151	2	547	4 6
157	2	557	4 6
163	2	563	6
167	2 4	⋮	⋮
173	2 4	937	6
179	2 4 6	941	4 6
181	2	947	6
⋮	⋮	953	6
373	2	967	6
379	2 6	971	6
383	2 6	977	6
389	6	983	6
397	6	⋮	⋮
401	6	$1.7427 \cdot 10^{35}$	? 30 ?
409	6	⋮	⋮
419	6	10^{425}	? 210 ?

TABLE 14: Jumping champions for small positive integers

CHAPTER 3

Theory of jumping champions

> Change is the constant, the signal
> for rebirth, the egg of the phoenix.
>
> CHRISTINA BALDWIN

At around 1000, six is the most frequent prime gap. What happens if we consider jumping champions at 10,000 or 1,000,000? Researchers have enumerated all the gaps up to 5×10^{16}, see Nicely. The most frequent gap up to that point is still six. This might give an impression that *six* is *the* jumping champion from 1000 onwards. But, Erdős and Straus [1980] proved that the jumping champion changes. In fact, $D(x)$ tends to infinity as x tends to infinity.

3.1 Brun's simple pure sieve

The proof of Erdős and Straus uses extensively the idea of Brun's sieve method. Various sieve methods are well explained in Pollack [2004], Odlyzko [1971] Charles [2000]. We will follow the development in Pollack [2004].

We have seen the sieve of Eratosthenes in the earlier chapter. To explain Brun's idea we will first state the general sieve problem.

3.1.1 General sieve problem

The general sieve problem can be stated as follows: Given a finite sequence $\mathcal{A} = a_i$ of integers and a finite set of primes $\mathcal{P}$, estimate the quantity

$$S(\mathcal{A}, \mathcal{P}) := \big|\{a \in \mathcal{A} : \gcd(a, P) = 1\}\big|,$$

where $P := \prod_{p \in \mathcal{P}} p$.

In many situations, the sifting set of primes arises by truncating of an infinite set of primes. Therefore we allow the set of primes $\mathcal{P}$ to be infinite and introduce

a notation for sieving only by those primes $p \in \mathcal{P}$ with $p \leqslant z$, where z is a positive integer.

$$S(\mathcal{A}, \mathcal{P}, z) := \big|\{a \in \mathcal{A} : \gcd(a, P(z)) = 1\}\big|,$$

where

$$P(z) := \prod_{\substack{p \in \mathcal{P} \\ p \leqslant z}} p.$$

Thus $S(\mathcal{A}, \mathcal{P}, z) = S(\mathcal{A}, \mathcal{P} \cap [2, z])$.

Definition 8. An arithmetical function f is called *multiplicative* if f is not identically zero and if

$$f(mn) = f(m)f(n) \quad \text{whenever } \gcd(m, n) = 1.$$

For example, let $f_\alpha = n^\alpha$, where α is a fixed integer.

We use the notation A_d to denote the number of terms of $\mathcal{A}$ divisible by d, where d is an integer, that is,

$$A_d = \big|\{a \in \mathcal{A} : d \mid a\}\big|.$$

The letter X denotes an approximation to the size of $\mathcal{A}$. We assume the existence of a multiplicative function α taking values in $[0, 1]$ for which

$$A_d = X\alpha(d) + r(d) \tag{3.1}$$

for each $d \mid P$ (or each $d \mid P(z)$, as the case may be). In practice, we *choose* X and α, and we *define* $r(d)$, for $d \mid P$ such that Equation (3.1) holds.

3.1.2 Brun's simple pure sieve

We will state the Brun's simple pure sieve in general form and then will deduce the form with absolute constants. In the next section, we will apply this method to estimate the number of twin primes.

To state the theorem we need the definition of Möbius function.

Definition 9. The *Möbius function* is a number theoretic function defined by

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ has one or more repeated prime factors,} \\ 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes.} \end{cases} \tag{3.2}$$

For example, $\mu(1) = 1$ (by definition), $\mu(2) = -1$ (as 2 is prime), $\mu(3) = -1$ (as 3 is prime), $\mu(4) = 0$ (as 2 divides 4 two times), $\mu(6) = 1$ (as 6 has two primes factors, 2 and 3).

We will also use the Big-Oh and Little-oh notations. Suppose f and g are complex-valued functions of one or several variables. We write $f = O(g)$ if $|f| \leqslant C|g|$ for some constant C and all specified values of the variables; the constant C is referred to as the *implied constant.* For example, $x = O(x^2)$ for $x \geqslant 1$ (we may take $C = 1$), but *not* in the larger range $x \geqslant 0$ (consider values of x approaching 0). The notation $f \ll g$ is sometimes used in place of $f = O(g)$.

We say that $f = o(g)$ as $x \to a$ if

$$\lim_{x \to a} f(x)/g(x) = 0.$$

For example, $x = o(x^2)$ as $x \to \infty$. We say "f is asymptotic to g as x tends to a" and write $f \sim g$ as $x \to a$, if

$$\lim_{x \to a} f(x)/g(x) = 1.$$

If the value of a is not specified, we assume $a = \infty$.

THEOREM 6 (Brun's pure simple sieve, general form). *For every nonnegative even integer* m,

$$\sum_{d \mid P, \nu(d) \leqslant m-1} \mu(d) A_d \leqslant S(\mathcal{A}, \mathcal{P}) \leqslant \sum_{d \mid P, \nu(d) \leqslant m} \mu(d) A_d,$$

where $\nu(d)$ *denotes the number of prime factors of* d.

By substituting $A_d = X\alpha(d) + r(d)$ and estimating the resulting terms, we can get a more useful form of the theorem. Due to this substitution the usage of the theorem will be restricted, but it is sufficient for our purposes.

THEOREM 7 (Brun's pure simple sieve). *For every nonnegative even integer* m,

$$S(\mathcal{A}, \mathcal{P}) = X \prod_{p \in \mathcal{P}} (1 - \alpha(p)) + O\Big(\sum_{d \mid P, \nu(d) \leqslant m} |r(d)| \Big) + O\Big(X \sum_{d \mid P, \nu(d) \geqslant m} \alpha(d) \Big).$$

Here the implied constants are absolute, that is, independent of $\mathcal{A}$, $\mathcal{P}$ *and of the function* α.

Proof. From Theorem 6 we get,

$$\begin{aligned} S(\mathcal{A}, \mathcal{P}) &= \sum_{d \mid P, \nu(d) \leqslant m} \mu(d) A_d + O\Big(\sum_{d \mid P, \nu(d) = m} A_d \Big) \\ &= \sum_{d \mid P, \nu(d) \leqslant m} \mu(d)(X\alpha(d) + r(d)) + O\Big(\sum_{d \mid P, \nu(d) = m} A_d \Big) \\ &= X \sum_{d \mid P, \nu(d) \leqslant m} \mu(d)\alpha(d) + O\Big(\sum_{d \mid P, \nu(d) \leqslant m} |r(d)| \Big) + O\Big(\sum_{d \mid P, \nu(d) = m} A_d \Big). \end{aligned}$$

Writing $A_d = X\alpha(d) + r(d)$, we see the last of these error terms is

$$\ll X \sum_{d|P,\nu(d)=m} \alpha(d) + \sum_{d|P,\nu(d)=m} |r(d)|;$$

hence,

$$S(\mathcal{A},\mathcal{P}) = X \sum_{d|P,\nu(d)\leqslant m} \mu(d)\alpha(d) + O\Big(\sum_{d|P,\nu(d)\leqslant m} |r(d)|\Big) + O\Big(X \sum_{d|P,\nu(d)=m} \alpha(d)\Big). \tag{3.3}$$

To simplify the main term in the above equation we add back the terms of the sum corresponding to divisors d of P with $\nu(d) > m$. We can then estimate the main term as $X\prod_{p\in\mathcal{P}}(1-\alpha(p))$, but with the error which is

$$\ll X \sum_{d|P,\nu(d)>m} \alpha(d).$$

This error can be combined with the last error term appearing in Equation (3.3) to get

$$S(\mathcal{A},\mathcal{P}) = X\prod_{p\in\mathcal{P}}(1-\alpha(p)) + O\Big(\sum_{d|P,\nu(d)\leqslant m} |r(d)|\Big) + O\Big(X \sum_{d|P,\nu(d)\geqslant m} \alpha(d)\Big),$$

which is what we wanted to prove. □

3.1.3 Application to the twin prime problem

One of the most famous application of Brun's pure sieve is Brun's own contribution to the twin prime problem:

THEOREM 8. *As* $x \to \infty$,

$$\pi_2(x) \ll \frac{x}{\log^2 x}(\log\log x)^2,$$

where $\pi_2(x)$ *denotes the number of twin prime pairs less than or equal to* x *and* $\log x$ *denotes the natural logarithm of* x.

We prove the above theorem using the following theorem, which will be later proved using sieve method approach.

THEOREM 9. *Define*

$$\pi_2(x,z) := |\{n \leqslant x : p \mid n(n+2) \Longrightarrow p > z \text{ for all prime numbers } p\}|.$$

Suppose $z = z(x) \to \infty$ *as* $x \to \infty$ *while* $z(x) \leqslant x^{\frac{1}{20\log\log x}}$ *for all large* x. *Then*

$$\pi_2(x,z) \sim 2C_2 e^{-2\gamma} x/\log^2 z \quad (x \to \infty),$$

where γ *is the Euler-Mascheroni constant.*

Proof of Theorem 8. If p and $p+2$ are both prime, then either $p \leqslant z$ or both p and $p+2$ have no prime factors exceeding z. Hence for any choice of the parameter z we have

$$\pi_2(x) \leqslant z + \pi_2(x, z).$$

Now take $z = z(x) = x^{\frac{1}{20 \log\log x}}$. Then Theorem 9 implies that as $x \to \infty$,

$$\pi_2(x) \ll x^{\frac{1}{20 \log\log x}} + \frac{x}{\log^2 x}(\log\log x)^2 \ll \frac{x}{\log^2 x}(\log\log x)^2.$$

□

Now we will prove Theorem 9. The appropriate set of sieving parameters for the twin prime problem is:

$$\mathcal{A} := \{a_n = n(n+2), n \leqslant x\}, \quad \mathcal{P} := \{\text{all primes } p\}.$$

We aim to estimate $S(\mathcal{A}, \mathcal{P}, z)$, which is the $\pi_2(x, z)$ of Theorem 9. For the approximation X to the size of $\mathcal{A}$, we take $X = x$. For our approximation α to the probability an element of $\mathcal{A}$ is divisible by d, we take $\alpha(d) = \omega(d)/d$, where ω is defined by

$$\omega(N) := |\{a \in \mathbb{Z}/N\mathbb{Z} : a(a+2) = 0\}|.$$

The function ω and therefore α is multiplicative, which can be proved using Theorem 4. We need a lemma to estimate the value of the remainder term $r(d)$.

LEMMA 1. *Let* $a_1, a_2, \ldots, a_k$ *be* k *distinct residue classes* $\pmod d$, *where* d *is a positive integer. Then if* x *is any positive real number, the number of positive integers not exceeding* x *falling into any of the given residue classes is* $kx/d + \theta$, *where* $|\theta| \leqslant k$.

Proof. The set of integers $a \leqslant x$ falling into one of the given congruence classes consists of $k\lfloor x/d \rfloor$ elements belonging to one of the complete blocks below x, plus at most k additional elements. □

From Equation (3.1) we get,

$$\begin{aligned} r(d) &= A_d - X\alpha(d) \\ &= |\{n \leqslant x : n(n+2) \equiv 0 \pmod d\}| - x\omega(d)/d \quad (d \mid P) \end{aligned} \tag{3.4}$$

Applying Lemma 1 to Equation (3.4) we get,

$$|r(d)| \leqslant \omega(d) = \prod_{p \mid d} \omega(p) \leqslant 2^{\nu(d)} \quad (d \mid P).$$

We get the last inequality using the fact that, for each of the prime factors p the equation $a(a+2) = 0$ has at most two solutions in $\mathbb{Z}/p\mathbb{Z}$. Therefore $\omega(p) \leqslant 2$. Substituting the values of sieving parameters into Theorem 7 we get,

$$\pi_2(x, z) = x \prod_{p \leqslant z}(1 - \alpha(p)) + O\Big(\sum_{d \mid P, \nu(d) \leqslant m} 2^{\nu(d)}\Big) + O\Big(x \sum_{d \mid P, \nu(d) \geqslant m} \alpha(d)\Big), \tag{3.5}$$

where m is a nonnegative even integer. We now think of x as large, and we set,

$$m := 10\lfloor \log\log z \rfloor.$$

As x increases, z and therefore m also increases.

By Equation (3.5), to prove Theorem 9 we need to prove the following three statements to be true for our choice of m:

(i) As $x \to \infty$ (so that $z \to \infty$ as well),

$$x\prod_{p\leqslant z}(1-\alpha(p)) \sim 2C_2 e^{-2\gamma}\frac{x}{\log^2 z},$$

where $C_2 = \prod_{p>2}(1-(p-1)^{-2})$.

(ii) For all large x,

$$E_1 := \sum_{d|P,\nu(d)\leqslant m} 2^{\nu(d)}$$

satisfies $E_1 \leqslant 2x^{1/2} = o(x/\log^2 z)$.

(iii) As $x \to \infty$, we have

$$E_2 := x\sum_{d|P,\nu(d)\geqslant m} \alpha(d) \ll x/\log^5 z = o(x/\log^2 z).$$

We will need two results by Merten's, which we will state without proof. The proofs can be found in Hardy and Wright [1975, chap. 22]. Merten's results:

$$\sum_{p\leqslant x}\frac{1}{p} \leqslant \log\log x + O(1), \tag{3.6}$$

$$\prod_{p\leqslant x}\left(1-\frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\log x}. \tag{3.7}$$

Proof of (i). As $x \to \infty, z \to \infty$. We simplify the expression using the fact that $\omega(2) = 1$ and for any other prime p, $\omega(p) = 2$.

$$x\prod_{p\leqslant z}(1-\alpha(p)) = \frac{1}{2}x\prod_{2<p\leqslant z}(1-2/p)). \tag{3.8}$$

Further multiplying and dividing by the term $\prod_{p\leqslant z}(1-1/p)^2$, we get

$$= x\left(2\prod_{2<p\leqslant z}\frac{1-2/p}{(1-1/p)^2}\right)\prod_{p\leqslant z}(1-1/p)^2.$$

Using the value of C_2, and Merten's result (3.7), we get

$$\sim 2C_2 e^{-2\gamma}\frac{x}{\log^2 z}.$$

□

Proof of (ii). We provide an estimate for E_1 for large x.

$$\begin{aligned} E_1 &= \sum_{d|P, \nu(d) \leqslant m} 2^{\nu(d)}. \\ &= \sum_{k=0}^{m} 2^k \binom{\pi(z)}{k}. \end{aligned}$$

Using the properties of binomial coefficients, we get

$$\begin{aligned} &\leqslant \sum_{k=0}^{m} (2\pi(z))^k \\ &\leqslant \sum_{k=-\infty}^{m} (2\pi(z))^k = (2\pi(z))^m \frac{1}{1 - \frac{1}{2\pi(z)}}. \end{aligned}$$

As the second factor in the above expression is less than or equal to 2, we get

$$\leqslant 2(2\pi(z))^m.$$

For x large, $\pi(z) \leqslant z/2$, therefore we get

$$\leqslant 2z^m.$$

Substituting the value of m, we get

$$\leqslant 2z^{10 \log\log z} \leqslant 2z^{10 \log\log x}.$$

Substituting the value of z, we get

$$E_1 \leqslant 2x^{1/2}.$$

Now we want to prove that $x^{1/2}$ is $o(x/\log^2 z)$. We consider $\frac{x^{1/2}}{x/\log^2 z}$. Using the inequality $z \leqslant x$, we get

$$\frac{x^{1/2}}{x/\log^2 z} \leqslant \frac{x^{1/2}}{x/\log^2 x} = \frac{\log^2 x}{x^{1/2}} \to 0.$$

□

Proof of (iii). We begin by rewriting E_2

$$E_2 := x \sum_{d|P, \nu(d) \geqslant m} \alpha(d) = x \sum_{k \geqslant m} \sum_{\substack{d|P \\ \nu(d)=k}} \alpha(d).$$

The inner sum can be rewritten as

$$\sum_{\substack{d|P\\ \nu(d)=k}} \alpha(d) = \sum_{p_1<p_2<\cdots<p_k\leqslant z} \alpha(p_1)\alpha(p_2)\cdots\alpha(p_k) \leqslant \frac{1}{k!}\Big(\sum_{p\leqslant z}\alpha(p)\Big)^k,$$

because the *multinomial expansion* of the kth power on the right hand side, each term $\alpha(p_1)\alpha(p_2)\cdots\alpha(p_k)$ appears with coefficient $k!$. Since $\alpha(p) \leqslant 2/p$ for every p, using Merten's result (3.6), we get

$$\sum_{k\geqslant m} \frac{1}{k!}\Big(\sum_{p\leqslant z}\alpha(p)\Big)^k \leqslant \sum_{k\geqslant m}\frac{1}{k!}(2\log\log z + 2c)^k. \tag{3.9}$$

The ratio of the $(k+1)$th term in this series to the kth is given by

$$\frac{2\log\log z + 2c}{k+1} \leqslant \frac{2\log\log z + 2c}{10\lfloor\log\log z\rfloor + 1} \leqslant \frac{1}{2},$$

for large enough z, hence for large enough x. For such x, the right hand sum of (3.9) is bounded above by twice its first term. Because

$$e^m = 1 + m + m^2/2! + m^3/3! + \cdots \geqslant m^m/m!, \tag{3.10}$$

we have $m! \geqslant (m/e)^m$, so that

$$\sum_{k\geqslant m}\frac{1}{k!}\Big(\sum_{p\leqslant z}\alpha(p)\Big)^k \leqslant 2\left(\frac{2e\log\log z + 2ce}{m}\right)^m.$$

As $m = 10\lfloor\log\log z\rfloor$, the expression inside the parenthesis is smaller than any constant exceeding $2e/10$, so it is smaller than $3/5$. It follows that for large x,

$$\begin{aligned} E_2 \leqslant 2x(3/5)^m &= 2x(3/5)^{10\lfloor\log\log z\rfloor} \\ &\leqslant 2(5/3)^{10}x(3/5)^{10\log\log z} \ll x/\log^5 z, \end{aligned}$$

as $10\log(3/5) < -5$. Thus $E_2 = o(x/\log^2 z)$ as well. □

Thus we have proved Theorem 9.

3.2 Jumping champion tends to infinity

Now we are ready to see the proof by Erdős and Straus of the fact that jumping champion tends to infinity. The paper also discusses the rate with which jumping champion approaches the infinity, which is out of context here. We show that a well-known conjecture of Hardy and Littlewood implies that the most likely difference between consecutive primes tends to infinity with x, so that there is no most probable difference independent of x, where x is a positive integer.

3.2.1 An application of Brun's method

In Hardy and Littlewood [1922], they conjecture that the number of solutions of

$$p_i - p_j = 2k, \quad p_i \leqslant x, \tag{3.11}$$

equals

$$(c + o(1))\frac{x}{\log^2 x} \prod_{\substack{p|k \\ p \text{ odd}}} \frac{p-1}{p-2}, \tag{3.12}$$

where c is an absolute constant. Let p_i denote the ith prime; then (3.12) implies that the number of solutions of

$$p_{i+1} - p_i = 2k, \quad p_{i+1} \leqslant x, \tag{3.13}$$

also is of the form (3.12). Note that the left hand side of Equation (3.13) represents the difference between the consecutive prime numbers. As Equation (3.13) is a special case of Equation (3.11) with $i = j + 1$, the number of solutions of Equation (3.13) is not greater than the number of solutions of Equation (3.11). On the other hand, if we have a solution $p_i - p_j = 2k$ of Equation (3.11) which is not a solution of Equation (3.13), that is $i > j + 1$, then we get a triplet of primes

$$p_j, p_j + 2u, p_j + 2k, \quad \text{where } 1 \leqslant u < k. \tag{3.14}$$

From Brun's method discussed in Section 3.1 applied to prime triplet problem, it follows that the number of such triplets with $p_j < x$ is less than

$$c_k x \prod_{k<p<x^\epsilon} \left(1 - \frac{3}{p}\right) < c'_k \frac{x}{\log^3 x}, \quad \text{where } \epsilon > 0 \tag{3.15}$$

for each fixed u, and hence is less than or equal to $c''_k x/\log^3 x$ for all the triplets in (3.14), for some constants c_k, c'_k, c''_k. The primes satisfying (3.14) exclude three residue classes $\pmod p$ for $p > k$. In the last section we had excluded two residue classes when we were determining the number of twin primes. Since the bound given in (3.15) is small compared to the estimate (3.12) it follows that (3.12) is also an estimate for the number of solutions of Equation (3.13).

Now the estimate (3.12) implies that the most likely difference between consecutive primes goes to infinity with x. Denote the number of solutions of Equation (3.13) by $f(x, k)$ and let k_x be the minimum value of k for which $f(x, k)$ is maximal. By (3.12) we get that, for sufficiently large x we have $f(x, k) < f(x, k')$ where $k = p_1, \ldots, p_r$ and $k' = p_1, \ldots, p_{r+1}$.

3.3 The candidates

In the last section we proved that there is no most likely difference between consecutive primes independent of x. But what numbers will be likely candidates

for jumping champions given a value of x? As we saw in Table 14 the numbers 2, 4 and 6 appear as jumping champion. Using Hardy-Littlewood k-tuple conjecture we can even determine the likely candidates. We follow the discussion in Odlyzko et al. [1999].

3.3.1 The k-tuple conjecture

Let $0 < m_1 < m_2 < \cdots < m_k$ be the given k-tuple of integers. The k-tuple conjecture predicts that the number of primes $p \leqslant x$ such that $p + 2m_1, p + 2m_2, \ldots, p + 2m_k$ are all prime is

$$P(x; m_1, m_2, \ldots, m_k) \sim C(m_1, m_2, \ldots, m_k) \int_2^x \frac{dt}{\log^{k+1} t} \tag{3.16}$$

where

$$C(m_1, m_2, \ldots, m_k) = 2^k \prod_q \frac{(1 - w(q; m_1, m_2, \ldots, m_k)/q)}{(1 - 1/q)^{k+1}}. \tag{3.17}$$

In (3.17), q runs over all odd primes, and $w(q; m_1, m_2, \ldots, m_k)$ denotes the number of distinct residues of $0, m_1, m_2, \ldots, m_k \mod q$. $C(m_1, m_2, \ldots, m_k)$ are called Hardy-Littlewood constants. In the special case $k = 1$,

$$w(q; m) = 2 \text{ for } q \nmid m, \text{ namely 0 and } m \bmod q, \text{ and}$$
$$w(q; m) = 1 \text{ for } q \mid m, \text{ namely 0.}$$

Substituting these values in (3.17) and simplifying, we get

$$C(m) = 2 \prod_q \frac{q(q-2)}{(q-1)^2} \prod_{q \mid m} \frac{(q-1)}{(q-2)}, \tag{3.18}$$

which only depends on the odd primes dividing m. Therefore $C(m_1) = C(m_2)$ if and only if m_1 and m_2 have the same odd prime factors, possibly raised to different powers.

For example, let us check the estimates of the number of prime pairs with difference 2, and 4. To put these in the notation of (3.16), we substitute $k = 1, m = 1$, and $k = 1, m = 2$, respectively. The estimates are denoted by $P(x; 1)$ and $P(x; 2)$, respectively. We get the values of the Hardy-Littlewood constants by substituting $m = 1$ and 2 in $C(m)$,

$$C(1) = C(2) = 2 \prod_q \frac{q(q-2)}{(q-1)^2},$$

$C(1) = C(2)$ as there is no odd prime dividing 1 or 2. From this we can conclude that $P(x;1) \sim P(x;2)$.

Hardy and Littlewood did not make any predictions about the size of the error term in the k-tuple conjecture. The standard arguments that assume random cancellation of various terms suggest it should be about $\sqrt{x}$ for each k-tuple. This argument is supported for tuples $p, p+2$ by the Brent's computations. His results of this and some others computations involving the k-tuple conjecture are reported in Brent [1974, 1975].

3.3.2 The heuristics

In the preceding subsection we gave an estimate for the number $P(x;m)$ of prime $p \leqslant x$ such that $p + 2m$ is also prime. However, in our work we are primarily interested how often p and $p+2m$, for instance, p and $p+4$, occur as *consecutive* primes. What if $p + 2$ is also prime? We have to subtract that number, namely $P(x;1,2)$ from $P(x;2)$ to get the correct estimate of the number of primes p such that the next prime is $p + 4$. Now in this case there is only one prime triplet of the form $p, p + 2, p + 4$, namely (3, 5, 7), as for any other such triplet one of the number will be divisible by 3. Therefore the number of pairs of consecutive primes $(p, p + 4)$ is again asymptotic to $P(x;1)$ and $P(x;2)$.

Consider $P(x;3)$. This is the number of pairs of primes $(p, p + 6)$ with $p \leqslant x$. Included in this count are pairs of *nonconsecutive* primes, which we are not interested in, like $(11, 17)$ or $(13, 19)$. They give rise to triplets of the form $(p, p+2, p + 6)$ or $(p, p + 4, p + 6)$, which, in the notation of (3.16), are counted by $P(x;1,3)$ and $P(x;2,3)$, respectively. Therefore the number of primes $p \leqslant x$ such that the next prime is $p + 6$ is given by

$$P(x;3) - P(x;1,3) - P(x;2,3). \tag{3.19}$$

This number is indeed correct, but only since there exist no quadruples of primes of the form $(p, p+2, p+4, p+6)$. Otherwise such quadruples would be counted both by $P(x;1,3)$ and by $P(x;2,3)$, so they would be subtracted twice in (3.19). Hence the correct number would be obtained by adding the number of such quadruples once:

$$N(x,3) = P(x;3) - P(x;1,3) - P(x;2,3) + P(x;1,2,3). \tag{3.20}$$

Here and in the sequel we write $N(x,d)$ for the number of primes $p \leqslant x$ such that $p + 2d$ is the smallest prime greater than p.

From (3.20), we get

$$N(x,3) \leqslant P(x;3), \quad \text{and}$$
$$N(x,3) \geqslant P(x;3) - P(x;1,3) - P(x;2,3).$$

To generalise this in case of $N(x,d)$ we will use the inclusion-exclusion principle.

THEOREM 10. *The inclusion-exclusion principle states that if* $A_1, A_2, \ldots, A_n$ *are finite sets, then*

$$|\bigcup_{i=1}^{x} A_i| = \sum_{i=1}^{x} |A_i| - \sum_{\substack{i,j \\ i\neq j}} |A_i \cap A_j| + \sum_{\substack{i,j,k \\ i\neq j\neq k\neq i}} |A_i \cap A_j \cap A_k| - \cdots \pm |(A_1 \cap A_2 \cdots \cap A_n)|. \tag{3.21}$$

By inclusion-exclusion principle and the fact that the partial sums of even and odd length are less than the total sum, we have

$$N(x,d) \leqslant \sum_{k=0}^{2j} (-1)^k \sum_{0<m_1<\ldots<m_k<d} P(x; m_1, \ldots, m_k, d), \tag{3.22}$$

$$N(x,d) \geqslant \sum_{k=0}^{2j+1} (-1)^k \sum_{0<m_1<\ldots<m_k<d} P(x; m_1, \ldots, m_k, d), \tag{3.23}$$

where $j = 0, 1, \ldots$. Note that the $k = 0$ term is $P(x;d)$. Odlyzko, Rubinstein, and Wolf compare $N(x,d)$ with

$$\int_2^x \sum_{k=1}^{l} \frac{A_{d,k}}{\log^{k+1} t} dt, \tag{3.24}$$

where l is a positive integer, and

$$A_{d,k} = (-1)^{k+1} \sum_{0<m_1<\ldots<m_{k-1}<d} C(m_1, \ldots, m_{k-1}, d), \tag{3.25}$$

so that $A_{d,1} = C(d)$. We can see the reason for the comparison if we substitute $d = 3$ in (3.24) to get $N(x,3)$. The sum in (3.25) runs over $\binom{d-1}{k-1}$ terms and $A_{d,k}$ grows nicely with this binomial coefficient. Odlyzko et al. [1999] in fact show that for fixed k,

$$A_{d,k+1} \sim (-1)^k A_{d,1} \frac{(2d)^k}{k!}, \quad \text{as } d \to \infty.$$

Using (3.24) and the expansion of exponential function given as the first equality in (3.10) and simplifying, we get a good approximation to the number of gaps of size $2d$ up to x.

$$N(x,d) \sim A_{d,1} \int_2^x \frac{\exp(-2d/\log t)}{\log^2 t} dt. \tag{3.26}$$

To get a good approximation, d has to be large and x has to be large compared to d. This restricts the range in which we may use the approximation (3.26).

The presence of the $A_{d,1}$ factor in (3.26) indicates that, in order to make $N(x,d)$ huge, it is preferable for d to have many small prime factors. Let us check the expression for $C(d)$, (3.18), again.

$$C(m) = 2\prod_{q}\frac{q(q-2)}{(q-1)^2}\prod_{q|m}\frac{(q-1)}{(q-2)},$$

If we have many small factors, the part $\prod_{q|m}\frac{(q-1)}{(q-2)}$ will contribute more.

On the other hand, the $\exp(-2d/\log t)$ term in the integrand tells us that amongst all values of d that produce the same value for $A_{d,1}$, the smallest one wins. More precisely, let

$$\begin{aligned} 2d_1 &= 2^{a_0}p_1^{a_1}\cdots p_j^{a_j},\\ 2d_2 &= 2p_1\cdots p_j,\\ 2d_3 &= 2\cdot 3\cdots q_j, \end{aligned} \tag{3.27}$$

where $a_i \geqslant 1$, the p_i's are odd primes, and q_j is the jth odd prime, namely $q_1 = 3, q_2 = 5, \ldots$. Note that $d_3 \leqslant d_2 \leqslant d_1$.

Applying Formula (3.26) to d_3 sufficiently large, we get $N(x,d_2) \geqslant N(x,d_1)$ as $A_{d_2,1} = A_{d_1,1}$ but $d_2 \leqslant d_1$, and $N(x,d_3) \geqslant N(x,d_2)$ as $A_{d_3,1} \geqslant A_{d_2,1}$ and $d_3 < d_2$. The product of all the primes up to a given prime, as in (3.27) is called *primorial*. This proves that the primorials are the likely candidates for a jumping champion. The first three primorials are 2, 6, 30. We have already seen that 2 and 6 appeared as a jumping champion.

3.4 The takeover points

Integrating (3.26), we get that $N(x, 3\cdots q_{j+1})$ begins to overtake $N(x, 3\cdots q_j)$ *roughly* when

$$\frac{q_{j+1}-1}{q_{j+1}-2}\exp\left(\frac{-2\cdot 3\cdots q_{j+1}}{\log x}\right) > \exp\left(\frac{-2\cdot 3\cdots q_j}{\log x}\right). \tag{3.28}$$

Simplifying the above expression the rough takeover point comes out to be

$$x > \exp(2\cdot 3\cdots q_j\cdot(q_{j+1}-1)(q_{j+1}-2)). \tag{3.29}$$

Wolf on his web site gives a rough estimate of the takeover point between jumping champions. In Table 28, n denotes the number of consecutive primes we consider to form the primorial and the last column gives the rough estimate from which point the primorial in the middle column will be the dominant gap. For example, 6 is jumping champion roughly from 3.21×10^2. We have seen in Table 14 that it actually becomes jumping champion at about 1000.

n	Primorial	Takeover point
2	6	3.21×10^{2}
3	30	1.70×10^{36}
4	210	5.81×10^{428}
5	2310	1.48×10^{8656}
6	30030	1.30×10^{138357}
7	510510	8.02×10^{3233259}
8	9699690	$8.50 \times 10^{69820169}$
9	223092870	$5.14 \times 10^{1992163572}$
10	6469693230	$3.56 \times 10^{74595540317}$

TABLE 28: A rough estimate of takeover point between jumping champions

3.4.1 Takeover point between 6 and 30

To get the rough estimate we substitute $q_1 = 3$ and $q_2 = 5$ in (3.28). Simplifying after substituting, we get $x > \exp(24/\log(4/3))$, or roughly $x > 1.70295 \times 10^{36}$. Using the approximation in (3.29), we get $x > e^{72}$, or $x > 1.85867 \times 10^{31}$.

Odlyzko, Rubinstein, and Wolf, use the coefficients from Brent [1974] to compute (3.24) with all the terms, $l = 2$ when $2d = 6$ and $l = 8$ when $2d = 30$. Based on the computation they claim that 30 should take over as jumping champion roughly at $x = 1.7427 \times 10^{35}$.

Harley conjectures the takeover point to be $x = 1.74274 \times 10^{35}$. He uses his own implementation to compute Hardy-Littlewood constants using `pari/gp` calculator. Please check Batut et al. [2000] for details about `pari/gp`, and Harley [1994] for the computation details.

I checked the takeover point using an implementation in `Mathematica` to compute Hardy-Littlewood constants by Renze, Wagon, and Wick. I got the takeover point around $x = 1.74275 \times 10^{35}$. It is in the same range as other computations. Also it shows that the estimates (3.28) and (3.29) are pretty close.

3.4.2 Takeover point between 30 and 210

To get the rough estimate we substitute $q_1 = 3, q_2 = 5$ and $q_3 = 7$ in (3.28). Simplifying after substituting, we get $x > \exp(180/\log(6/5))$, or approximately $x > 5.81401 \times 10^{428}$. Using the approximation in (3.29), we get $x > e^{900}$, or $x > 7.32881 \times 10^{390}$.

Odlyzko, Rubinstein, and Wolf predict that taking $l = 4$ terms in (3.24), 210 will first begin to beat 30 sometime in the interval $10^{425} < x < 10^{426}$. I get the same results taking $l = 6$ terms in (3.24).

CHAPTER 4

Computational results

> The practice of computation is in rather low repute today, and the idea that computation can be *fun* is rarely spoken aloud.
>
> *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*
> HAROLD M. EDWARDS

The jumping champion conjecture states that 210 becomes jumping champion at around 10^{425}. In this chapter, we consider several intervals near that point to check the most dominant gap in them for the computational evidence of the above conjecture. Also we report some additional facts, like big prime gaps, found during these computations. These are reported in Athale [2002]. Based on our computations, we improve the jumping champion conjecture made in Odlyzko et al. [1999]. The computations communicated by Dubner further substantiates our claim.

In the latter part, we consider the prime gaps modulo *six*. Based on the observations we conjecture that the number of gaps congruent to zero modulo six is approximately equal to the number of gaps not congruent to zero modulo six. The work was reported in Athale [2003].

4.1 Computations near the conjectured takeover points

In Odlyzko et al. [1999], they take an interval of size 10^7 near the conjectured takeover point to check the most dominant prime gap. The interesting thing is that in this interval 210 is not the most dominant prime gap. This motivated us

x	$G(d, x, 10^7)$ where $d =$					
	30	42	60	90	180	210
10^{410}	44	32	46	*47*	18	41
10^{420}	*44*	29	33	32	31	34
10^{430}	*43*	30	41	28	30	36
10^{440}	*49*	28	29	28	20	29
10^{450}	26	24	30	29	26	*34*
10^{460}	25	*44*	29	29	28	30
10^{470}	24	30	*34*	*34*	17	29
10^{480}	*41*	36	22	25	21	22
10^{490}	*32*	22	22	29	24	28
10^{500}	*38*	26	31	31	27	24
10^{510}	*31*	29	28	21	20	29
10^{520}	20	14	23	*28*	14	20
10^{530}	22	23	23	19	23	*30*
10^{540}	21	11	16	*28*	23	21
10^{550}	17	18	23	*32*	24	09
Sum	Sum of $G(d, x, 10^7)$ from $x = 10^{430}$					
	389	*335*	*351*	*361*	*297*	*341*
Total sum	*477*	*396*	*430*	*440*	*346*	*416*

TABLE 30: Significant prime gaps in the interval of length 10^7 starting from $10^{410}, 10^{420}, \ldots, 10^{550}$

to check the most dominant prime gap in the intervals of size 10^7 around the conjectured takeover point. We consider intervals of different lengths at various points to analyse the claim of the jumping champion conjecture.

4.1.1 Verifying the takeover point between 30 and 210

We checked the intervals of size 10^7 starting from $10^{410}, 10^{420}, \ldots, 10^{550}$. We give the results in Table 30.

Let us denote by $G(d, x, l)$ the number of times d appears as a gap between consecutive primes in the interval $[x, x + l]$. Table 30 lists the values of $G(d, x, l)$ where $l = 10^7, x = 10^i$, for $i = 410, 420, \ldots, 550$. The most dominant gap in a row is *emphasised*. The values of d in Table 30 are the ones that give the dominant gaps, that is, the other gaps occur less frequently. The last but one row gives the sum of the values in each column starting from row 10^{430}, as the conjectured takeover point is 10^{425}. The last row gives the number of times d has appeared as

the gap between consecutive primes in the chosen intervals starting from 10^{410}. If 210 should take over as jumping champion at around 10^{425} then it should be the dominant gap in the most of the chosen intervals. The rows giving the sums are added just to facilitate the comparison. As one can see from Table 30, 30 dominates 210 till 10^{440}. So, we did further computations.

x	$G(d, x, 10^7)$ where d =							
	6	18	30	60	90	180	210	420
10^{425}	21	24	*56*	37	26	38	41	32
10^{426}	31	23	37	*42*	34	34	35	23
10^{427}	25	23	30	37	30	26	30	29
10^{428}	28	34	*39*	35	34	35	34	30
10^{429}	16	27	33	*50*	32	28	31	33
10^{430}	28	28	*43*	41	28	30	36	25
10^{431}	23	28	35	30	34	*40*	*40*	23
10^{432}	*33*	32	27	25	22	24	*33*	26
10^{433}	38	30	39	36	*40*	36	35	24
10^{434}	26	*33*	35	40	29	*43*	27	27
10^{435}	29	*39*	36	35	*39*	32	37	24

TABLE 31: Significant prime gaps in the interval of length 10^7 starting from $10^{425}, 10^{426}, \ldots, 10^{435}$

The intervals of size 10^7 near 10^{425} also do not have 210 as the most dominant gap. Table 31 lists the values of $G(d, x, l)$ where $l = 10^7, x = 10^i$, for $i = 425, 426, \ldots, 435$. By the conjecture, if $d = 210$ takes over as jumping champion at 10^{425}, then it should be the dominating gap from this point onwards. But, in the intervals starting from 10^{425} and 10^{426}, $d = 30$ clearly dominates $d = 210$. Moreover, in all these computations shown in Table 31, $d = 30$ dominates $d = 210$ *eight* times. Also 60 is a dominant gap near 10^{425}. Note that 60 is the product of 2 and 30, which is a primorial.

We did not get any clear takeover behaviour with the intervals of size 10^7, so we continued the experiments with the intervals of size 10^8. The aim was to find out whether bigger intervals give some dominant gap, a candidate for the jumping champion. We considered five intervals of size 10^8 starting from 10^{430}, 10^{435}, 10^{455}, 10^{475} and 10^{495}, respectively. This choice of intervals was based on the observations gathered from the intervals of size 10^7. Intervals starting from 10^{430} and 10^{435} were chosen to check the dominant gap near the conjectured takeover point 10^{425}. Table 32 lists the values of $G(d, x, l)$ where $l = 10^8, x = 10^{430}, 10^{435}, 10^{455}, 10^{475}$ and 10^{495}. We list all the significant gaps, that is, for which $G(d, x, l)$ is greater than most of the other values of d.

x	$G(d, x, 10^8)$ where d =							
	30	42	60	90	120	150	210	420
10^{430}	*366*	282	339	325	312	313	336	298
10^{435}	*360*	285	352	343	296	310	323	260
10^{455}	272	273	297	303	306	287	*325*	270
10^{475}	267	263	257	269	262	259	280	*284*
10^{495}	*271*	209	238	231	217	241	252	202

TABLE 32: Significant prime gaps in the interval of length 10^8 starting from 10^{430}, 10^{435}, 10^{455}, 10^{475}

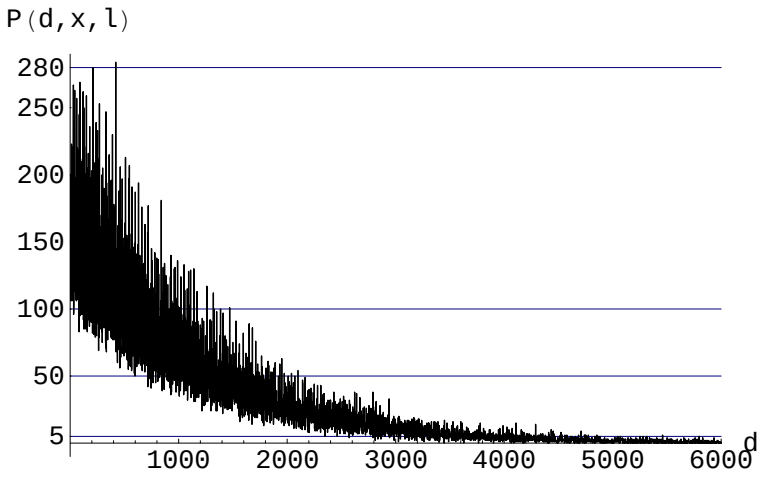


FIGURE 32: The number of prime gaps of size $d = 2, 4, , \ldots, 6000$ in the interval of length 10^8 starting from 10^{475}

These computations generated lot of data. We point out the main observations.

- 30 dominates 210 in the intervals starting from 10^{430} and 10^{435}. This suggests, maybe, the takeover point is not near 10^{425}.

- Figure 32 shows the number of times d appears as the gap between consecutive primes in the interval of size 10^8, starting from 10^{475}. All the even numbers from 2 to 3446 appear as gaps between consecutive primes at least once in this interval. From Figure 32 it is clear that, almost all the numbers below 1000 appear as gap for more than 50 times, and most of the numbers below 6000 appear as gap for more than 4 times. All the five intervals of size 10^8, which we checked, depict the same behaviour.

Some experts suggested that, may be, this behaviour is due to the fact that we have started the intervals from a power of 10, like 10^{425}, 10^{430} and so on. Two of the authors of Odlyzko et al. [1999] did not agree with this claim when I spoke with them personally, as prime numbers are random. But, we checked the intervals of size 10^7 around the conjectured takeover point anyway. Table 33 lists the values of $G(d, x, l)$ for these intervals.

x	$G(d, x, 10^7)$, d =	
	30	210
$6.343 \cdot 10^{425}$	*47*	31
$2.357 \cdot 10^{425}$	*43*	38
$9.072 \cdot 10^{425}$	*40*	26
$7.991 \cdot 10^{426}$	*40*	23
$3.950 \cdot 10^{426}$	*41*	38
$5.190 \cdot 10^{426}$	*37*	31
$9.556 \cdot 10^{427}$	35	*36*
$4.553 \cdot 10^{427}$	*38*	31
$3.959 \cdot 10^{427}$	*39*	33
$3.572 \cdot 10^{428}$	26	*47*
$5.631 \cdot 10^{428}$	30	*32*
$2.438 \cdot 10^{428}$	36	*47*
$9.273 \cdot 10^{429}$	*36*	28
$3.015 \cdot 10^{429}$	*40*	39
$5.660 \cdot 10^{429}$	35	*40*

TABLE 33: Comparison of number of prime gaps of size 30 and 210 in the interval of length 10^7 starting from random numbers in the range 10^{425} to 10^{429}

4.1.2 Comparing the behaviour of 30 and 210 near the takeover points

We also know about the other conjectured takeover point, namely between 6 and 30. When does 30 takes over as the dominant gap from 6 if we consider intervals near the conjectured takeover point? We considered intervals of size 10^7 starting from random numbers and also intervals of size 10^8 starting from $10^{33}, 10^{34}, \ldots, 10^{39}$.

In the intervals of size 10^7 starting from 10 random numbers near the conjectured takeover point $1.7 \cdot 10^{35}$, 30 appears as the most dominant gap in 8 intervals and in the remaining intervals, 6 is the most dominant gap. It is evident from

x	$G(d, x, 10^7)$, d =	
	6	30
$1.942 \cdot 10^{35}$	3874	*3960*
$2.009 \cdot 10^{35}$	3856	*3947*
$2.144 \cdot 10^{35}$	3915	*3941*
$2.350 \cdot 10^{35}$	3879	*3887*
$2.503 \cdot 10^{35}$	3864	*4043*
$3.016 \cdot 10^{35}$	3772	*3981*
$4.048 \cdot 10^{35}$	*3893*	3873
$7.020 \cdot 10^{35}$	*3871*	3869
$9.030 \cdot 10^{35}$	3616	*3856*
$9.028 \cdot 10^{35}$	3772	*3812*

(i) Interval length 10^7

x	$G(d, x, 10^8)$, d =	
	6	30
10^{33}	*44747*	43554
10^{34}	41638	*41723*
10^{35}	*39515*	39496
10^{36}	37182	*37774*
10^{37}	35560	*36113*
10^{38}	33924	*34519*
10^{39}	31879	*33110*

(ii) Interval length 10^8

TABLE 34: Comparison of number of prime gaps of size 6 and 30 in the intervals of length 10^7 and 10^8

Table 34(i) that the difference between the number of gaps of size 6 and 30 is not significant in those two intervals.

Intervals of size 10^8 show the same behaviour. From Table 34(ii) we see that 30 is the dominant gap even in the interval starting from 10^{34}. In the interval starting from 10^{35}, 6 is the dominant gap but the difference between the number of gaps of size 6 and 30 is insignificant. In the next 4 intervals, 30 is the dominant gap.

Therefore it is more likely that the conjectured takeover point $1.7 \cdot 10^{35}$ between 6 and 30 as the jumping champion is correct. But we cannot say anything about the validity of the jumping champion conjecture, regarding the correctness of the conjectured takeover point. In the next section, we will apply statistical tests to the data to get more insight.

Finally, we give the results of computations communicated by Dubner. He computes certain number of prime gaps, say a million and then compares the number of gaps of size 30 and 210. The interval covered by these gaps is bigger than our intervals. These data strengthened our guess that the takeover point will be somewhere around 10^{450}. Table 35 shows the results of the computations done by Dubner. In Table 35(i) we can see that 30 is the dominant gap in the gaps computed starting from 10^{35}. This is in accordance with the results in Table 34. Also, even if we consider bigger size intervals, namely intervals containing million or more gaps, as in Table 35(ii), near 10^{450}, the difference between the number of gaps of 210 and 30 is not significant.

Starting from	Number of gaps					
	10^6		10^7		10^9	
	d = 6	d = 30	d = 6	d = 30	d = 6	d = 30
10^{30}	*37024*	35035	*369824*	353492	*37032427*	35301521
10^{34}			*328309*	326098	*32796095*	32578055
10^{35}	31935	*37024*	318524	*319441*	31880704	*31936440*
10^{36}			310434	*314247*		
10^{40}	27912	*31769*	279423	*291058*	27999629	*29096022*

(i) Comparison between 6 and 30

Starting from	Number of gaps					
	10^6		$2 \cdot 10^6$		$5 \cdot 10^6$	
	d = 30	d = 210	d = 30	d = 210	d = 30	d = 210
10^{400}	*3719*	3602				
10^{450}	3331	*3334*	6677	*6717*		
10^{460}	*3264*	3254				
10^{500}	2971	*3037*			14888	*15415*

(ii) Comparison between 30 and 210

TABLE 35: Comparison of the number of gaps in the intervals of different sizes

4.2 Statistical analysis

We conjectured, after analysing the data obtained from the experiments, that the takeover point will be around 10^{450}. The data generated by computations (Dubner [2003]) strengthened this feeling. Now we apply the statistical tests to our data.

We are considering here the number of gaps of size 6 and 30, these are two samples. Two samples are said to be dependent on each other when the elements of one are related to those of the other in some significant or meaningful manner. In fact the two samples consist of observations made of the same objects, individuals or more generally, on the same selected population elements. Our two samples actually consist of observations on the same objects, which, generally, implies that they are dependent. We wish to check if the difference between the means of the samples around the conjectured takeover is zero or not.

We apply two tests, one parametric and other non-parametric for testing dif-

ferences between means of two samples, dependent samples or matched paired observations. The details of the tests can be found in books like Mendenhall and Sincich [1995]; Sheskin [2004] and the web sites by Lowry; NIST [2000].

A	B	A – B	Rank	Signed-rank
43	36	7	17	17
49	29	20	27	27
26	34	-8	20	-20
56	41	15	24	24
37	35	2	5	5
30	30	0		
39	34	5	10.5	10.5
33	31	2	5	5
43	36	7	17	17
35	40	-5	10.5	-10.5
27	33	-6	14	-14
39	35	4	8	8
35	27	8	20	20
36	37	-1	2	-2
47	31	16	25	25
43	38	5	10.5	10.5
40	26	14	23	23
40	23	17	26	26
41	38	3	7	7
37	31	6	14	14
35	36	-1	2	-2
38	31	7	17	17
39	33	6	14	14
26	47	-21	28	-28
30	32	-2	5	-5
36	47	-11	22	-22
36	28	8	20	20
40	39	1	2	2
35	40	-5	10.5	-10.5
366	336	30	29	29
360	323	37	30	30

TABLE 36: Rank determination for Wilcoxon singed-rank test

4.2.1 Non-parametric test

First we apply the non-parametric test called Wilcoxon signed-rank test. The main reason to choose a non-parametric test is that we have the samples coming from intervals of different lengths, 10^7 and 10^8. We consider all the intervals of size 10^7 starting from between 10^{425} and 10^{450} from Tables (30, 31, 33) and intervals of size 10^8 starting from 10^{430} and 10^{435} from Table 32. We wish to check the if the distributions of gaps of size 30 and size 210 are identical in this interval as the conjectured takeover point is around 10^{425} and our guess is it is around 10^{450}.

Let us call the distribution of gaps of size 30, A and that of 210, B. We begin the test by computing the difference between all the observations in the matched pairs. These differences are ranked by magnitude, irrespective of sign. A mean rank is used in case of equal performance differences and zero differences are ignored. A sign is then attached to each rank corresponding to the sign of the difference. Table 36 shows the signed rank determination of the data.

First we formulate the null hypothesis for one-tailed test:

$$H_o : \text{Distributions A and B are identical.}$$

The alternative hypothesis is:

$$H_a : \text{Distribution A is shifted to the right of B.}$$

The null hypothesis states that the difference between means of A and B is zero, and the alternate hypothesis states that the mean of A is greater than mean of B.

There are 30 records, denoted by N, so the sum of all the ranks in the fourth column will be $N(N+1)/2 = 465$. Sum of positive signed-rank is denoted by T_+ and negative signed-rank is denoted by T_-. We get $T_+ = 351$ and $T_- = 114$.

A *statistic* is a numerical descriptive measure computed from sample data. The decision whether to reject the null hypothesis is based on a statistic, called a *test statistic*. Here, the test statistic is T_-, the rank sum of the negative differences. If $T_- \leqslant T_o$, we reject the null hypothesis, where T_o is given in Mendenhall and Sincich [1995, Table 16 of Appendix II]. For one-tailed test, $N = 30$ at $\alpha = 0.01$ we get $T_o = 120$. So we can reject the null hypothesis with 99% confidence and get that the distribution of gaps of size 30 is shifted to the right of 210. Or in other words, statistically there are more gaps of size 30 than of size 210 in the interval we are considering.

Suppose now we only consider the intervals of size 10^7, that is, we do not consider last two rows in Table 36, then $T_- = 114$. But T_o for $N = 28$ at $\alpha = 0.01$ is 102. For $\alpha = 0.025$ $T_o = 117$. So we can reject H_o in this case with less confidence, but still we get the same result as before.

4.2.2 Parametric test

The parametric test for testing whether two distributions differ or not is called t-test. We consider all the rows except the last two ones in Table 36.

First we formulate the null hypothesis for a directional test:

$$H_o : \mu_A - \mu_B = 0,$$

that is, the mean of the difference in the results is zero. The alternative hypothesis is:

$$H_a : \mu_A > \mu_B.$$

The mean of the differences, denoted by m, is $m = 3.35$ and standard deviation of the differences, denoted by S, is $S = 9.09$. Now t is obtained using the following formula:
$t = \frac{m-\delta}{S}\sqrt{n}$ where $\delta = 0$, for testing equal means. We get $t = 1.95$. We reject the null hypothesis if for some α, $t_\alpha \leqslant t$, for $df = 26$, where df denotes degrees of freedom. We assume that the prime numbers follow Poisson distribution. In this case, $df = N - 2$. We have $N = 28$ so $df = 26$. For $df = 26$ and $\alpha = 0.05$ for a directional test, $t_\alpha = 1.71$. For $df = 26$ and $\alpha = 0.025$ for a directional test, $t_\alpha = 2.06$. So we can reject the null hypothesis at $\alpha = 0.05$ and accept the alternative hypothesis.

Using both the tests we get that the gaps of size 30 occur more than the gaps of size 210 up to 10^{450} using our computational results. Based on all the above observations we update the jumping champion conjecture:
Updated jumping champion conjecture: 210 takes over as a jumping champion at around 10^{450}.

4.3 Prime gaps modulo six

During the experiments, we observed that the number of gaps not congruent to zero modulo six equals approximately the number of gaps congruent to zero modulo six. This motivated us to carry out further experiments to determine the nature of the distribution of the prime gaps modulo six. In this section we present the results of these experiments.

Let us start with an easy observation:

$$|\#(g \equiv 2 \mod 6) - \#(g \equiv 4 \mod 6)| \leqslant 2, \tag{4.1}$$

where # denotes number of and g denotes gaps. If we start counting the gaps from any number greater than or equal to five instead of three, the right hand side of the above inequality can be changed to *one.* This is because there is only one triplet of primes of the form, $p, p+2, p+4$ where p is a prime. Now let us see

Interval from	$\#(g = 6m+2)$ x	$\#(g = 6m+4)$ y	$\#(g = 6m)$ z	Ratio $\frac{(x+y)}{z}$	Ratio Total
3	14107249	14107249	22633034	1.247	1.247
10^9	13068799	13068798	21237156	1.231	1.239
2×10^9	12726823	12726823	20773604	1.225	1.235
3×10^9	12512554	12512555	20487166	1.222	1.231
4×10^9	12359174	12359173	20274064	1.219	1.229
5×10^9	12242540	12242540	20106065	1.218	1.227
6×10^9	12144403	12144404	19970177	1.216	1.226
7×10^9	12063731	12063730	19851841	1.215	1.225
8×10^9	11992984	11992984	19753573	1.214	1.223
9×10^9	11928110	11928111	19673095	1.213	1.222

TABLE 39: The distribution of prime gaps modulo six in the interval 3 to 10^{10}

why the inequality holds if we start counting the gaps from any number greater than or equal to five. Consider primes 5 and 7. All the numbers of the form $7 + (6m + 2)$ are divisible by 3, where m is a natural number, and precisely these are the numbers that give the gap $6m+2$, a number congruent to two modulo six. Therefore no next prime number will add to the number of prime gaps congruent to two modulo six before adding one to the number of prime gaps congruent to four modulo six. In general, if p and $p + 6m + 2$ are prime numbers, then all the numbers of the form $(p + 6m + 2) + 6k + 2$ will be divisible by 3, where m and k are natural numbers. Note that the numbers p and $p + 6m + 2$ are both prime if p is congruent to two modulo three. We can similarly show that if we start with two consecutive primes with the gap congruent to two modulo four, no next prime number will give the gap congruent to four modulo six before there is one prime number that gives the gap congruent to two modulo six. This proves the inequality 4.1.

Let us denote the ratio of the number of gaps not congruent to zero modulo six to the number of gaps congruent to zero modulo six by $\mathscr{R}$.

$$\mathscr{R} = \frac{\#(g \equiv 2 \mod 6) + \#(g \equiv 4 \mod 6)}{\#(g \equiv 0 \mod 6)}. \tag{4.2}$$

First, let us see how $\mathscr{R}$ changes from 3 up to 10^{10}. Later we give the values of number of gaps and $\mathscr{R}$, in the intervals of size 10^8 starting from $10^{10}, 10^{20}, \ldots, 10^{100}$, and intervals of size 10^7 starting from $10^{100}, 10^{125}, \ldots, 10^{400}$. The size of the intervals might change the value of $\mathscr{R}$; we check the ratio in the intervals of size 10^8 and 10^7 starting from 10^{100}, 10^{125}, 10^{150}, and 10^{175}.

To enumerate the number of gaps from 3 to 10^{10}, we divide the interval in ten parts, namely $[3, 10^9], [10^9, 2 \times 10^9], \ldots, [9 \times 10^9, 10^{10}]$. The last gap in an interval

is the difference between the first prime in the next interval and the last prime in the interval. Table 39 gives the number of gaps distributed modulo six; and the ratio is the ratio in the interval, and the total ratio is the cumulative ratio. The value of the ratio, and therefore, of the total ratio decreases as the number of gaps increase.

Interval from	$\#(g = 6m+2)$ x	$\#(g = 6m+4)$ y	$\#(g = 6m)$ z	Ratio $\frac{(x+y)}{z}$
10^{10}	1190120	1190119	1961691	1.213
10^{20}	572273	572273	1026526	1.115
10^{30}	375027	375028	696118	1.077
10^{40}	279785	279784	527627	1.061
10^{50}	222471	222470	425014	1.047
10^{60}	184763	184763	354163	1.043
10^{70}	157768	157769	305032	1.034
10^{80}	137634	137634	267034	1.031
10^{90}	122575	122575	237355	1.033
10^{100}	109617	109617	214607	1.022

(i) Interval length 10^8

Interval from	$\#(g = 6m+2)$ x	$\#(g = 6m+4)$ y	$\#(g = 6m)$ z	Ratio $\frac{(x+y)}{z}$
10^{100}	10868	10868	21535	1.009
10^{125}	8738	8738	17014	1.027
10^{150}	7341	7340	14521	1.011
10^{175}	6307	6307	12270	1.028
10^{200}	5450	5450	10648	1.024
10^{225}	4912	4913	9635	1.020
10^{250}	4339	4340	8597	1.010
10^{275}	3968	3969	7814	1.016
10^{300}	3690	3690	7046	1.047
10^{325}	3318	3318	6512	1.019
10^{350}	3082	3082	6156	1.001
10^{375}	2946	2946	5852	1.007

(ii) Interval length 10^7

TABLE 40: The distribution of prime gaps modulo six in the interval of size 10^8 and 10^7 starting from $10^{10}, 10^{20}, \ldots, 10^{100}, 10^{125}, \ldots, 10^{375}$

To check the behaviour of $\mathscr{R}$ as the size of the primes increases, we check

the ratio in the intervals of size 10^8 starting from $10^{10}, 10^{20}, \ldots, 10^{100}$. Table 40(i) gives the number of gaps distributed modulo six; and the value of $\mathscr{R}$ in the interval. The ratio decreases as the size of the primes increases. If we continue to check the value of $\mathscr{R}$ in the intervals starting from greater numbers the ratio does not decrease continuously. But, it is clear from Table 40(ii), that the ratio $\mathscr{R}$ is approximately 1.

Interval from	Size	$\#(g = 6m+2)$ x	$\#(g = 6m+4)$ y	$\#(g = 6m)$ z	Ratio $\frac{(x+y)}{z}$
10^{100}	10^7	10868	10868	21535	1.009
	10^8	109617	109617	214607	1.022
10^{125}	10^7	8738	8738	17014	1.027
	10^8	87885	87885	171698	1.024
10^{150}	10^7	7341	7340	14521	1.011
	10^8	73297	73297	143468	1.022
10^{175}	10^7	6307	6307	12270	1.028
	10^8	56241	56241	110584	1.017

TABLE 41: Comparison of the distribution of prime gaps modulo six in the intervals of size 10^7 and 10^8 starting from $10^{100}, 10^{125}, 10^{150}, 10^{175}$

Table 41 shows that $\mathscr{R}$ changes with the change in the size of the interval, but we cannot say anything more about the change in the behaviour. The only thing that remains constant is, that it hovers around 1.

Dubner had communicated all the gaps in the computation of 3,000,000 starting from 10^{550}. We got $\mathscr{R} = 1.00675$. Similarly for 2,000,000 gaps starting from 10^{450} we got $\mathscr{R} = 1.00635$. These observations might give the impression that the value of $\mathscr{R}$ always remains greater than 1. But, the value of $\mathscr{R} = 0.991561$ for the gaps in the interval of size 10^6 starting from 10^{900}.

From all the above observations we conjecture:
Conjecture: $\mathscr{R} \sim 1$.

4.4 Role of symbolic computation

We used Mathematica to compute these big prime numbers. Mathematica generates the probable primes but that does not significantly change the results of our computation. The computation of $l = 6$ terms in (3.24) took many days to complete and required huge memory. We computed them in steps such that the memory usage was below 100 megabytes. The benefit of the symbolic computation was, we could compute the formulae and later could substitute the different values say 10^{425} or 10^{430} to get the numerical value of the approximate number of

gaps. Once we have the formula, the numeric computation does not take much time. Also one can save all these formulae for later use.

We also computed the value of $\mathscr{R}$ for gaps up to 10^{10} using the implementation of Hardy-Littlewood constants by Renze, Wagon, and Wick in Mathematica. We computed $N(x, d)$ for $x = 10^{10}$ and $d = 2, 4, \ldots, 40, 42$. These cover majority of the gaps so it is meaningful to compute $\mathscr{R}$. We get,
$\mathscr{R} = 1.224$ (k-tuple conjecture)
$\mathscr{R} = 1.222$ (explicit counting) please see Table 39.

4.5 Miscellaneous results

We came across some big prime gaps during these experiments. Table 42 lists some of them of size greater than 11000 in the increasing order and the prime after which the gap occurs. The complete list of known prime gaps can be found on the web site by Nicely.

Gap (d)	Following prime	Gap (d)	Following prime
11058	$10^{475} + 90282073$	11072	$10^{490} + 9646279$
11098	$10^{510} + 610491$	11212	$10^{475} + 30588861$
11246	$10^{475} + 71201311$	11274	$10^{540} + 8462997$
11300	$10^{510} + 9697429$	11430	$10^{475} + 99806517$
11618	$10^{420} + 6009073$	12026	$10^{480} + 4698193$
12030	$10^{475} + 61533597$	12762	$10^{520} + 82921$
15504	$10^{540} + 8726037$	15582	$10^{550} + 1800169$

TABLE 42: Big prime gaps with their starting prime

Part II

Ranks of elliptic curves

It is possible to write endlessly on
elliptic curves (This is not a threat).

Elliptic Curves: Diophatine Analysis
Serge Lang

CHAPTER 5

Elliptic curves

> Not everything that can be counted counts, and not everything that counts can be counted.
>
> *Sign hanging in Einstein's office at Princeton*

> This is a fascinating area of algebraic geometry dealing with nonsingular curves of genus 1 — in English, solutions to equations $y^2 = x^3 + Ax + B$. It turns out to have important connections to number theory and in particular to factorisation of ordinary integers (and thus to cryptography). Also, what appear to be simple Diophantine equations often lead to elliptic curves. Through Riemann surfaces it has connections to topology; through modular forms and zeta functions to analysis. Elliptic curves also played a role in the recent resolution of the conjecture known as Fermat's Last Theorem.

This is the introduction for the topic of elliptic curves in *The Mathematical Atlas* maintained by Rusin, which is available online. This gives us some of the reasons of the popularity of the elliptic curves in the mathematical world in recent years. In short, their use in solving theoretical problems as well as in practical applications have made them an interesting area of research.

There are several books on the topic, approaching it from the different point of views and covering some part of it. The most comprehensive are the two volumes by Silverman, namely Silverman [1992, 1994]. I have relied upon some other books during my work, which are easier to read, such as, Silverman and Tate [1992], Cassels [1991], Blake, Seroussi, and Smart [1999]. The web site maintained by Fermigier gives a list of links to the research articles on this topic

and related material on the web. I also referred two lecture notes on elliptic curves available on the Internet, Milne [1996] and Connell [1999]. Here we will follow the development of the topic roughly as in Connell [1999]. But first we will define some basic concepts and will state the necessary theorems from algebraic geometry that will be necessary in the later development. Throughout this chapter let K be a field and n be a positive integer unless otherwise stated.

5.1 Basic algebraic geometry notions

For algebraic geometric concepts, we follow here the development given in Winkler [1999–2000] and Cox, Little, and O'Shea [1998] because of their computational flavour. The concepts can also be found in the classical books like Fulton [1989] and Hartshorne [1977]. My personal favourite is Shafarevich [1994]. The online notes Milne [2003], contain most basic concepts.

5.1.1 Affine variety

We will first define what do we mean by a curve. For this, we need to state some basic algebraic geometric definitions.

DEFINITION 10. The n-*dimensional affine space* over K is defined as

$$\mathbb{A}^n(K) := \{(a_1, a_2, \ldots, a_n) \mid a_i \in K\}.$$

If K is clear from the context, we simply write $\mathbb{A}^n$. The elements of $\mathbb{A}^n$ are called *points*. $\mathbb{A}^1$ is called the *affine line*, and $\mathbb{A}^2$ is called the *affine plane*.

DEFINITION 11. Let $f \in K[x_1, x_2, \ldots, x_n]$. A point $P = (a_1, a_2, \ldots, a_n) \in \mathbb{A}^n(K)$ is a *root* or *zero* of f if and only if $f(P) = f(a_1, a_2, \ldots, a_n) = 0$.

DEFINITION 12. A subset $V \subseteq \mathbb{A}^n(K)$ is an *affine algebraic set* if and only if there is a set of polynomials $S \subseteq K[x_1, x_2, \ldots, x_n]$ such that

$$V = V(S) = \{P \in \mathbb{A}^n(K) \mid f(P) = 0 \text{ for all } f \in S\}.$$

DEFINITION 13. Let X be a subset of $\mathbb{A}^n(K)$. The set of all polynomials in $K[x_1, x_2, \ldots, x_n]$ vanishing on all the points in X form an ideal. This ideal is the *ideal of* X, $I(X)$.

$$I(X) := \{f \in K[x_1, x_2, \ldots, x_n] \mid f(P) = 0 \text{ for all } P \in X\}.$$

DEFINITION 14. An algebraic set $V \subseteq \mathbb{A}^n$ is *reducible* if and only if there are algebraic sets V_1, V_2 different from V such that $V = V_1 \cup V_2$. Otherwise V is *irreducible*. An irreducible algebraic set is also called a *variety*.

For example, the line $\mathbb{R}^1$ is a 1-dimensional affine space. Consider the polynomial $f \in \mathbb{R}[x]$, $f = x - 1$. For $P = 1$ we get, $f(P) = 1 - 1 = 0$. Therefore P is a root or zero of f, in fact, it is the only root. Consider $V(f)$. It is the point P and so it is an algebraic set. Now if we consider $X = P$ then $I(X)$ will consists of the polynomials that vanish at 1. We can write this as $I(X) = \langle x - 1 \rangle$. It can be shown that $V(f)$ is irreducible using the argument in Cox et al. [1998, chapter 4, section 5]. Therefore $V(f)$, that is, point P is a variety.

5.1.2 Dimension of an affine variety

To define the dimension of an affine variety we will need the definition of the dimension of an ideal.

DEFINITION 15. Let $I \subset K[x_1, x_2, \ldots, x_n]$ be a proper ideal and $\{i_1, i_2, \ldots, i_d\}$ a subset of $\{1, 2, \ldots, n\}$. The set $\{x_{i_1}, x_{i_2}, \ldots, x_{i_d}\}$ is said to be *independent modulo* I if

$$I \cap K[x_{i_1}, x_{i_2}, \ldots, x_{i_d}] = \{0\}.$$

We denote the set $\{X \subseteq \{x_1, x_2, \ldots, x_n\} \mid X \text{ is independent modulo } I\}$ by $\Delta(I)$. The *dimension* of I, denoted by $\dim(I)$, is the maximal number of elements in any set of variables independent modulo I, that is

$$\dim(I) = \max(\{|X| \mid X \in \Delta(I)\}).$$

For the ideals $\{0\}$ and $K[x_1, x_2, \ldots, x_n]$ we let their dimensions be -1 and n, respectively.

DEFINITION 16. Let $V \subseteq \mathbb{A}^n$ be a variety. The integral domain

$$\Gamma(V) = K[x_1, x_2, \ldots, x_n]/I(V)$$

is called the *coordinate ring* of V.

For $V(f)$ in the earlier example, $I(V) = \langle x - 1 \rangle$, and $\Gamma(V) = K[x]/\langle x - 1 \rangle = K$.

DEFINITION 17. The *field of rational functions* $\mathcal{K}(V)$ of a variety $V \subseteq \mathbb{A}^n$ is the quotient field of $\Gamma(V)$.

This is possible as $\Gamma(V)$ is an integral domain. In our example, $\mathcal{K}(V) = K$, as K is a field. The field of rational functions $\mathcal{K}(V)$ can be constructed as

$$\mathcal{K}(V) = \{\frac{f}{g} \mid f, g \in K[x_1, x_2, \ldots, x_n], g \notin I(V)\}/\sim,$$

where $\frac{f}{g} \sim \frac{f'}{g'} \iff fg' - f'g \in I(V)$.

DEFINITION 18. The *dimension* of a variety V, $\dim(V)$, is the transcendence degree of $\mathcal{K}(V)$ over K. The *dimension* of an algebraic set V is the maximal dimension of an irreducible component of V.

In our example the dimension of V is 0, as the transcendence degree of K over K is 0. There is a very close relationship between the dimension of ideals and the dimension of the corresponding varieties.

THEOREM 11. *Let* $V \subseteq \mathbb{A}^n$ *be a variety. Then* $\dim(I(V)) = \dim(V)$.

Proof. Please see Winkler [1999–2000]. □

We can also define the dimension of variety V using the affine Hilbert function of $I(V)$. We follow the development in Cox et al. [1998, chapter 9].

DEFINITION 19. Let I be an ideal in $K[x_1, x_2, \ldots, x_n]$, and let $K[x_1, x_2, \ldots, x_n]_{\leqslant s}$ denote the set of polynomials of total degree $\leqslant s$ in $K[x_1, x_2, \ldots, x_n]$. Also let $I_{\leqslant s} = I \cap K[x_1, x_2, \ldots, x_n]_{\leqslant s}$ denote the set of polynomials in I of total degree $\leqslant s$. The *affine Hilbert function* of I is the function on the nonnegative integers s defined by

$$\begin{aligned} {}^{a}HF_I(s) &= \dim K[x_1, x_2, \ldots, x_n]_{\leqslant s}/I_{\leqslant s} \\ &= \dim K[x_1, x_2, \ldots, x_n]_{\leqslant s} - \dim I_{\leqslant s}. \end{aligned}$$

DEFINITION 20. The polynomial which equals ${}^{a}HF_I(s)$ for sufficiently large s is called the *affine Hilbert polynomial* of I and is denoted ${}^{a}HP_I(s)$.

DEFINITION 21. The *dimension* of an affine variety $V \subset K^n$, denoted by $\dim V$, is the degree of the affine Hilbert polynomial of the corresponding ideal $I = I(V) \subset K[x_1, x_2, \ldots, x_n]$.

One drawback of this definition is that to find the dimension of a variety V, we need to know $I(V)$, which, in general, is difficult to compute. The following theorem gives a method to determine the dimension when the field K is algebraically closed.

THEOREM 12 (The dimension theorem). *Let* $V = V(I)$ *be an affine variety, where* $I \subset K[x_1, x_2, \ldots, x_n]$ *is an ideal. If* K *is algebraically closed, then*

$$\dim V = \deg {}^{a}HP_I.$$

Proof. Please see Cox et al. [1998, chapter 9, section 3]. □

5.1.3 Local properties of plane curves

Now we have all the necessary notions to define an affine plane curve.

DEFINITION 22. Two polynomials $f, g \in K[x, y]$ are *equivalent* if and only if $f = \lambda g$ for some $\lambda \in K^*$, where K^* denotes the set of nonzero elements in K. We define an (*affine plane*) *curve* as an congruence class of non-constant polynomials under this congruence relation.

The *degree* of a curve is the degree of a defining polynomial of the curve. A curve of degree 1 is called a *line*.

If $f = \prod f_i^{e_i}$, where the f_i are the irreducible factors of f, then the f_i are called the *components* of f and e_i the *multiplicity* of the component f_i. If $e_i = 1$ then f_i is a *simple* component, otherwise a *multiple* component.

DEFINITION 23. Let $\mathcal{C}$ be a curve, f a defining polynomial for $\mathcal{C}$, $P = (a, b) \in \mathbb{A}^2$. Point P is a *point on* $\mathcal{C}$ if and only if $f(a, b) = 0$. Point P is a *simple* point on $\mathcal{C}$ if and only P is a point on $\mathcal{C}$ and $\frac{\partial f}{\partial x}(P) \neq 0$ or $\frac{\partial f}{\partial y}(P) \neq 0$. A point on $\mathcal{C}$ which is not a simple point is called a *multiple* or *singular* point on $\mathcal{C}$.

DEFINITION 24. A curve having only simple points is called a *nonsingular* curve.

The curve given by $y^2 = x^3 + x^2$ is an example of a singular curve. It can be easily seen that the origin is a singular point. Elliptic curves are nonsingular.

DEFINITION 25. Let the plane curve $\mathcal{C}$ be defined by the polynomial $f(x, y)$, $P = (a, b)$ a point on $\mathcal{C}$. If all the partial derivatives $\frac{\partial^{i+j} f}{\partial x^i \partial y^j}$ of order $i + j < m$ vanish at P but at least one of the partial derivatives of order m does not vanish at P, then m is the *multiplicity* of P on $\mathcal{C}$, written as $m_P(\mathcal{C})$.

If $m_P(\mathcal{C}) = 2$, then P is a *double point*. The origin in the above example is a double point.

Intersection multiplicity

Let f, g be plane curves, $P \in \mathbb{A}^2$. We denote the intersection multiplicity by $m_P(f \cap g)$. The following seven properties define the *intersection multiplicity*.

(i) $m_P(f \cap g)$ is a nonnegative integer if P is not a point on a common component of f and g. Otherwise we let $m_P(f \cap g) = \infty$.

(ii) $m_P(f \cap g) = 0$ if and only if $P \notin f \cap g$. Furthermore, $m_P(f \cap g)$ depends only on those components of f and g containing P.

(iii) If T is an affine change of coordinates in $\mathbb{A}^2$ and $T(Q) = P$, then $m_P(f^T \cap g^T) = m_P(f \cap g)$.

(iv) $m_P(f \cap g) = m_P(g \cap f)$.

(v) $m_P(f \cap g) \geqslant m_P(f) \cdot m_P(g)$. Equality holds if and only if f and g do not have a common tangent at P.

(vi) The intersection multiplicity should be additive on unions of curves: if $f = \prod f_i^{r_i}$ and $g = \prod g_j^{s_j}$, then

$$m_P(f \cap g) = \sum_{i,j} r_i s_j \cdot m_P(f_i \cap g_j).$$

(vii) For an irreducible curve f the intersection multiplicity with g should depend only on the residue of g in $\Gamma(f)$. So, for arbitrary f,

$$m_P(f \cap g) = m_P(f \cap (g + af)) \quad \text{for arbitrary } a \in K[x, y].$$

THEOREM 13. *For all plane curves* f, g *and all points* $P \in \mathbb{A}^2$ *there is a uniquely defined intersection multiplicity* $m_P(f \cap g)$ *satisfying the properties (i)–(vii).*

Proof. For the proof please see Winkler [1999–2000]. It in fact gives an algorithm to compute the intersection multiplicity. □

5.1.4 Projective algebraic geometry

DEFINITION 26. A *form* or *homogeneous polynomial* in the polynomial ring $R[x_1, x_2, \ldots, x_n]$ over the ring R is a polynomial, in which every term has the same degree.

Now let us define the projective space. Later we will define the concept of projective algebraic set and other concepts as we did in the affine case.

DEFINITION 27. Let n be a nonnegative integer. For $(c_1, c_2, \ldots, c_{n+1}) \in \mathbb{A}^{n+1}(K) \setminus \{(0, 0, \ldots, 0)\}$, by $(c_1 : c_2 : \ldots : c_{n+1})$ we denote the line in $\mathbb{A}^{n+1}(K)$ through $(c_1, c_2, \ldots, c_{n+1})$ and $\mathcal{O} = (0, 0, \ldots, 0)$. So

$$(c_1 : c_2 : \ldots : c_{n+1}) := \{(\lambda c_1, \lambda c_2, \ldots, \lambda c_{n+1}) \mid \lambda \in K\}.$$

The n-*dimensional projective space* $\mathbb{P}^n(K)$ over K is the set of all such lines through the origin in $\mathbb{A}^{n+1}$, that is,

$$\mathbb{P}^n(K) := \{(c_1 : c_2 : \ldots : c_{n+1}) \mid (c_1 : c_2 : \ldots : c_{n+1}) \in \mathbb{A}^{n+1}(K) \setminus \{\mathcal{O}\}\}.$$

The line $(c_1 : c_2 : \ldots : c_{n+1}) \in \mathbb{A}^{n+1}(K)$ is a *point* in $\mathbb{P}^n(K)$. The $(n+1)$-tuple $(c_1, c_2, \ldots, c_{n+1})$ is called (a *set of*) *homogeneous coordinates* of the point $(c_1 : c_2 : \ldots : c_{n+1})$.

DEFINITION 28. A point $P \in \mathbb{P}^n$ is a *root* of the polynomial $f(x_1, x_2, \ldots, x_{n+1}) \in K[x_1, x_2, \ldots, x_{n+1}]$ if and only if $f(c_1, c_2, \ldots, c_{n+1}) = 0$ for every choice of homogeneous coordinates $(c_1 : c_2 : \ldots : c_{n+1})$ of P. In this case we write $f(P) = 0$.

For $S \subseteq K[x_1, x_2, \ldots, x_{n+1}]$ we define

$$V_p(S) := \{P \in \mathbb{P}^n \mid f(P) = 0 \text{ for all } f \in S\}.$$

$V_p(S)$ is a *projective algebraic set*.

DEFINITION 29. For a set $X \subseteq \mathbb{P}^n$ let

$$I(X) := \{f \in K[x_1, x_2, \ldots, x_{n+1}] \mid f(P) = 0 \text{ for every } P \in X\}.$$

$I(X)$ is the *ideal of* X.

DEFINITION 30. The ideal $I \subseteq K[x_1, x_2, \ldots, x_{n+1}]$ is *homogeneous* if an only if, for every

$$f = \sum_{i=0}^{d} f_i \in I, \quad f_i \text{ form of degree } i,$$

also $f_i \in I$ for $0 \leqslant i \leqslant d$.

DEFINITION 31. As for the affine algebraic sets, we call a projective algebraic set $V \subseteq \mathbb{P}^n$ *irreducible* if and only if it cannot be written as the union of two proper algebraic subsets. An irreducible projective algebraic set is a *projective variety*.

A projective curve $\mathcal{C}$ of degree n is defined by a polynomial equation of the form

$$\sum_{i+j+k=n} a_{ijk} x^i y^j z^k = 0.$$

We now state the theorem for which we defined most of the above notions.

THEOREM 14 (Bezout's theorem). *Let* F *and* G *be curves of degrees* m *and* n*, respectively, having no common components. Then*

$$\sum_P m_P(F \cap G) = mn.$$

Proof. Please see Cox et al. [1998, chapter 8, section 7] or Fulton [1989] or Hartshorne [1977]. □

5.1.5 Dimension of a projective variety

DEFINITION 32. The *dimension* of a projective variety $V \subset \mathbb{P}^n(K)$, denoted by $\dim V$, is the degree of the Hilbert polynomial of the corresponding homogeneous ideal $I = I(V) \subset K[x_1, x_2, \ldots, x_{n+1}]$.

THEOREM 15 (The dimension theorem). *Let* $V = V(I) \subset \mathbb{P}^n(K)$ *be a projective variety, where* $I \subset K[x_1, x_2, \ldots, x_{n+1}]$ *is a homogeneous ideal. If* V *is nonempty and* K *is algebraically closed, then*

$$\dim V = \deg^a HP_I.$$

Proof. Please see Cox et al. [1998, chapter 9, section 3]. □

5.2 What is an elliptic curve?

First we will define what we mean by an elliptic curve as there are many definitions coming from different approaches.

DEFINITION 33. An *elliptic curve*, denoted by E, is an affine nonsingular curve defined over K by an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{5.1}$$

where $a_1, a_2, a_3, a_4, a_6 \in K$, together with the point at infinity, $\mathcal{O}$.

In the subsections we will see for what values of a_i is nonsingular and also how to convert any cubic in the Weierstrass form given by Equation (5.1).

To remember the Weierstrass equation think of the terms as being in a graded ring with

$$\begin{aligned} \text{weight of } x &= 2, \\ \text{weight of } y &= 3, \\ \text{weight of } a_i &= i, \end{aligned}$$

so that each term in the equation has weight 6. This also explains the absence of a_5, for further details please see Connell [1999, section 1.3].

Let us see how we can simplify Equation (5.1). Also we will define the elementary constants associated with Equation (5.1). If the character of the field $K \neq 2$, we can complete the square on the left hand side by defining $\eta = y + (a_1x + a_3)/2$. We get,

$$\eta^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}, \tag{5.2}$$

where

$$b_2 = a_1^2 + 4a_2, \quad b_4 = a_1a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6. \tag{5.3}$$

If the character of the field $K \neq 3$ we can complete the cube by setting $\xi = x + b_2/12$. We get,

$$\eta^2 = \xi^3 - \frac{c_4}{48}\xi - \frac{c_6}{864}, \tag{5.4}$$

where

$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6. \tag{5.5}$$

We also define

$$b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2, \tag{5.6}$$

and the discriminant

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6. \tag{5.7}$$

The constants in (5.3) and (5.5)–(5.7) are defined for all the elliptic curves, regardless of the characteristic of the field K. The condition that the curve defined by Equation (5.1) is nonsingular, and so it defines an elliptic curve, is stated as

$$\Delta \neq 0.$$

Then we can define j-invariant of an elliptic curve in terms of the above constants

$$j = c_4^3/\Delta. \tag{5.8}$$

Using the transformations given above, we can transform Equation (5.1) of an elliptic curve defined over the field of real numbers into the following format:

$$y^2 = x^3 + ax + b. \tag{5.9}$$

In this case $\Delta = -16(4a^3 + 27b^2) \neq 0$.

Now let us define a rational point on an elliptic curve. For details please see Silverman and Tate [1992].

DEFINITION 34. A point $P = (x, y)$ satisfying Equation (5.1) is called a *rational point* on the elliptic curve if $x, y \in K$. $\mathcal{O}$ is rational.

For example, consider an elliptic curve $E : y^2 = x^3 - 5x + 3$ defined over the field of real numbers $\mathbb{R}$, then $P = (2, -1)$ and $Q = (2, 1)$ are two rational points on the given elliptic curve. The values of constants for this curve are as follows:

$$\begin{gathered} b_2 = 0, b_4 = -10, b_6 = 12, b_8 = -25, \\ c_4 = 240, c_6 = -2592, \\ \Delta = 4112, j = \frac{864000}{257}. \end{gathered}$$

We calculated these values using a Maple program called *apecs*, arithmetic of plane elliptic curves. It is available from the author's, Connell [1999], web site.

5.2.1 Nonsingularity of E

We check for what values of a_i Equation (5.1) defines an elliptic curve, that is, Equation (5.1) is nonsingular. We first prove that any nonsingular curve is irreducible.

Consider a homogeneous polynomial $F = F(X_0, \ldots, X_n) \in K[X_0, \ldots, X_n]$ of degree d. The Taylor expansion can be written as

$$F(X_0 + \lambda_0, \ldots, X_n + \lambda_n) = F_0 + F_1 + \cdots,$$

where $F_i = F_i(\lambda_0, \ldots, \lambda_n)$ is homogeneous of degree i in the λ's, each coefficient of which is homogeneous of degree $d - i$ in the X's. Thus $F_0 = F(X_0, \ldots, X_n)$ and

$$F_1 = \sum_{i=0}^{n} a_i \lambda_i, \quad \text{where} \quad a_i = \frac{\partial F_0}{\partial X_i}.$$

LEMMA 2. *Let* $F = F(X, Y, Z)$ *be a nonzero homogeneous polynomial. If* F *is nonsingular then it is absolutely irreducible, that is, irreducible over* $\overline{K}$*, where* $\overline{K}$ *denotes algebraic closure of* K.

Proof. Let $F = GH$ where G and H are homogeneous of positive degree defined over $\overline{K}$, and let P be a point of intersection on the curves corresponding to G and H. Then $\frac{\partial F}{\partial X} = G\frac{\partial H}{\partial X} + \frac{\partial G}{\partial X}H$ vanishes at P, and similarly for the other variables. Thus P is a singular point of F. □

THEOREM 16. *The Weierstrass equation is singular if and only if* $\Delta = 0$ *and then there is a unique singularity of order* 2 *as follows:*

(a) If $c_4 \neq 0$ *there is a* K*-rational node at the point with coordinates*

$$x_0 = (18b_6 - b_2 b_4)/c_4$$
$$y_0 = (b_2 b_5 + 3b_7)/c_4 = \begin{cases} -(a_1 x_0 + a_3)/2 & \text{if } \operatorname{char}(K) \neq 2 \\ (a_3^2 + a_1^2 a_4)/a_1^3 & \text{if } \operatorname{char}(K) = 2 \end{cases}$$

where

$$b_5 = a_1 a_4 - 2a_2 a_3,$$
$$b_7 = a_1(a_3^2 - 12a_6) + 8a_3 a_4.$$

The two tangents are given in terms of the parameter t *by* $x = x_0 + t$, $y = y_0 + \mu t$ *for the two distinct roots of the separable polynomial* $\mu^2 + a_1\mu - 3x_0 - a_2 = 0$. *When* $\operatorname{char}(K) \neq 2$, *these are*

$$\mu = \frac{-a_1 c_4 \pm \sqrt{-c_4 c_6}}{2c_4}.$$

(b) If $c_4 = 0$ *there is a cusp at the point with coordinates*

$$\operatorname{char}(K) = 2: \qquad x_0 = \sqrt{a_4}, \qquad y_0 = \sqrt{a_2 a_4 + a_6},$$
$$\operatorname{char}(K) = 3: \qquad x_0 = -\sqrt[3]{a_3^2 + a_6}, \qquad y_0 = a_1 x_0 + a_3,$$
$$\operatorname{char}(K) \neq 2, 3: \qquad x_0 = -b_2/12, \qquad y_0 = -\frac{1}{2}(a_1 x_0 + a_3).$$

The unique tangent line is $x = x_0 + t$, $y = y_0 + \mu t$ *where* $\mu = \sqrt[4]{a_4} + \sqrt{a_2}$ *when* $\operatorname{char}(K) = 2$, *and* $\mu = -a_1/2$ *otherwise.*

In either case

$$f_x = a_1 y_0 - 3x_0^2 - 2a_2 x_0 - a_4 = 0,$$
$$f_y = 2y_0 + a_1 x_0 + a_3 = 0.$$

Note that f_x *denotes the partial derivative of* f *with respect to* x. *A singular Weierstrass equation remains singular over every field extension* K'/K*; moreover, the nature of the singularity is constant.*

Sketch of the proof: First let $\mathrm{char}(K) \neq 2, 3$. Then as detailed above, a linear change of the affine coordinates, which clearly does not affect the occurrence of singularities, allows us to take the simple form

$$f = \eta^2 - \xi^3 + \frac{c_4}{48}\xi + \frac{c_6}{864},$$
$$f_\eta = 2\eta,$$
$$f_\xi = -3\xi^2 + \frac{c_4}{48}.$$

If these three quantities are 0 then $\xi = \pm\sqrt{c_4}/12$, $\eta = 0$, $c_6 = \mp(\sqrt{c_4})^3$, hence $\Delta = 0$ and the Taylor expansion reduces to

$$f(\pm\sqrt{c_4}/12 + \lambda, \mu) = (\mu^2 \mp \sqrt{c_4}\lambda^2/4) - \lambda^3.$$

Thus the singularity is of order 2 and the number of tangents is 2 or 1 according as $c_4 \neq 0$ or $c_4 = 0$.

Please see Connell [1999] for the case of fields of characteristic 2 and 3. □

5.2.2 Cubic to Weierstrass

One can define an elliptic curve in a more general way: A plane nonsingular cubic with a rational point, *rational* means the coordinates are in the designated field K and does not refer to the rational field $\mathbb{Q}$, unless of course $K = \mathbb{Q}$. An example of such a curve that is not a Weierstrass equation is the Fermat curve

$$x^3 + y^3 = 1, \quad \text{with points} \quad (x, y) = (1, 0),\ (0, 1),$$

assuming the characteristic of K, denoted by $\mathrm{char}(K)$ is not equal to 3. We will see how to transform such an equation into Weierstrass form.

Let K be a field such that $\mathrm{char}(K) \neq 2, 3$ and consider the curve defined by a cubic equation in u and v over K with a rational point (p, q). Now we can translate both variables to shift the rational point (p, q) to the origin. Replacing u by $u + p$ and v by $v + q$ we can assume that the rational point is $(0, 0)$:

$$s_1 u^3 + s_2 u^2 v + s_3 u v^2 + s_4 v^3 + s_5 u^2 + s_6 uv + s_7 v^2 + s_8 u + s_9 v = 0. \qquad (5.10)$$

Let f denote the polynomial on the left side of Equation (5.10).

We now describe the algorithm, due to Nagell, please see Connell [1999] for further details, to transform f into Weierstrass form, or to discover that the curve is not elliptic.

STEP ONE: Interchange u and v if necessary to ensure $s_9 \neq 0$. Note that, if both s_8 and s_9 are 0 then $(0,0)$ is a singular point, please see Theorem 16 for the proof, and the curve is not elliptic.

STEP TWO: Substitute $u = U/W$, $v = V/W$ and clear the denominators to obtain the homogenised form

$$F = F_3 + F_2 W + F_1 W^2 = 0,$$

where

$$\begin{aligned} F_3 &= s_1 U^3 + s_2 U^2 V + s_3 U V^2 + s_4 V^3, \\ F_2 &= s_5 U^2 + s_6 U V + s_7 V^2, \\ F_1 &= s_8 U + s_9 V. \end{aligned}$$

The rational point P with (u,v) coordinates $(0,0)$ has projective coordinates $(U,V,W) = (0,0,1)$. The tangent line at P, given by $F_1 = 0$, meets the curve in the point $Q = (-e_2 s_9, e_2 s_8, e_3)$ where $e_i = F_i(s_9, -s_8)$, $i = 2,3$. The e_i cannot both be 0 because that would make the tangent a component and the curve would be reducible, and by Lemma 2 will not be elliptic. Now $e_2 = 0$ means that $P = Q$ is a flex, the tangent has triple contact with the curve at P, while $e_3 = 0$ means that Q is at infinity. If $e_3 \neq 0$ we can make the coordinate change $U = U' - (s_9 e_2/e_3)W'$, $V = V' + (s_8 e_2/e_3)W'$, $W = W'$, while if $e_3 = 0$ we can make the change $U = U' - s_9 W'$, $V = V' + s_8 W'$, $W = U'$. In either case Q is now at the origin, $(U',V',W') = (0,0,1)$, and the tangent at P is given by $s_8 U' + s_9 V' = 0$. We can now return to affine coordinates by the transformations $u' = U'/W', v' = V'/W'$; projective coordinates were only needed to deal with the case when Q was at infinity.

STEP THREE: If the equation in terms of u', v' is $f' = f'_3 + f'_2 + f'_1 = 0$ where $f'_i = f'_i(u',v')$ denotes the homogeneous part of f' of degree i, then

$$u'^2 f'_3(1,t) + u' f'_2(1,t) + f'_1(1,t) = 0,$$

where $t = v'/u'$. Thus

$$u' = \frac{-\phi_2 \pm \sqrt{\delta}}{2\phi_3}, \quad v' = tu', \tag{5.11}$$

where $\phi_i = f'_i(1,t)$ and $\delta = \phi_2^2 - 4\phi_1\phi_3$. The values of t such that $\delta = 0$ are the slopes of the tangents to the curve that pass through Q, and one of these values is $t_0 = -s_8/s_9$. We write $t = t_0 + 1/\tau$ so that $\rho = \tau^4\delta$ is a cubic polynomial in τ.

STEP FOUR: Finally, if

$$\rho = c\tau^3 + d\tau^2 + e\tau + k,$$

then $c \neq 0$, since $c = 0$ implies that the original curve is not elliptic, and the substitutions $\tau = x/c$, $\rho = y^2/c^2$ give the Weierstrass equation

$$y^2 = x^3 + dx^2 + cex + c^2k.$$

The relations between the original variables u, v and x, y can be traced back starting with Equation (5.11) where

$$t = t_0 + c/x, \quad \delta = c^2y^2/x^4.$$

5.3 The group of rational points

The set of rational points forms an abelian group, denoted by $E(K)$, with $\mathcal{O}$ as the identity, under the addition operation. That is, there is a map

$$\begin{aligned} E(K) \times E(K) &\to E(K) \\ (A, B) &\mapsto A + B \end{aligned}$$

that gives $E(K)$ the structure of an abelian group. Let us define this map which we called as the addition of rational points on an elliptic curve. For that we will use the fact that an elliptic curve meets a line in three points.

By the application of Theorem 14, we get that a cubic curve meets a line in three points. We will follow the details as in Verrill.

Suppose the cubic curve is given by

$$F(x, y, z) = 0,$$

where F has degree 3. Note that equation of the elliptic curve in the projective coordinates will be

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3,$$

where a_is are same as in Equation (5.1). Suppose the line is given by

$$ax + by + cz = 0.$$

One of a, b or c is nonzero. Suppose $c \neq 0$, so points on the line are given by $z = -(ax + by)/c$. Then where the line and cubic intersect, we have

$$F(x, y, -(ax + by)/c) = 0.$$

This is a homogeneous polynomial in two variables, so it looks like

$$\alpha_1 x^3 + \alpha_2 x^2 y + \alpha_3 x y^2 + \alpha_4 y^3 = 0.$$

If $y = 0$ is not a solution, then dividing by y^3 we have

$$\alpha_1 \left(\frac{x}{y}\right)^3 + \alpha_2 \left(\frac{x}{y}\right)^2 + \alpha_3 \left(\frac{x}{y}\right) + \alpha_4 = 0.$$

By the fundamental theorem of algebra, over an algebraically closed field, we can factor this polynomial as:

$$\left(p_1 \left(\frac{x}{y}\right) + q_1\right) \left(p_2 \left(\frac{x}{y}\right) + q_2\right) \left(p_3 \left(\frac{x}{y}\right) + q_3\right) = 0.$$

Multiplying back through by y^3, we have

$$(p_1 x + q_1 y)(p_2 x + q_2 y)(p_3 x + q_3 y) = 0.$$

If $y = 0$ is a solution, we will still be able to factor the original polynomial as above. So, there are three solutions, giving three points on the intersection of the line with the conic. The multiplicity of a root is the number of times the factor occurs in this factorisation.

For example, consider the cubic curve which we considered in the previous section:

$$\mathcal{C} : y^2 z = x^3 + x^2 z.$$

We consider here the equation of the curve in the projective coordinates. Take the line $L : x = 0$. Substituting the equation for L into the equation for $\mathcal{C}$, we get

$$y^2 z = 0.$$

There are three factors of this cubic, y, y and z. If $y = 0$, we get the point $(0 : 0 : 1)$. Since this factor has multiplicity two, the line L intersects $\mathcal{C}$ with multiplicity 2 at $(0 : 0 : 1)$. The third point of intersection is $\mathcal{O} = (0 : 1 : 0)$.

5.3.1 Geometric version of the addition of rational points

DEFINITION 35. Now the group law is defined as follows. Let P, Q be two rational points on an elliptic curve E. Let R be the third point of intersection with the curve. Then we denote by $P + Q$ the third point of intersection with the curve of the line passing through R and $\mathcal{O}$. We get the idea of this operation in Figure 59.

The construction has to be interpreted appropriately if two or more of the points involved coincide. For example, if $P = Q$, we consider the tangent to the curve at P, as in Figure 60.

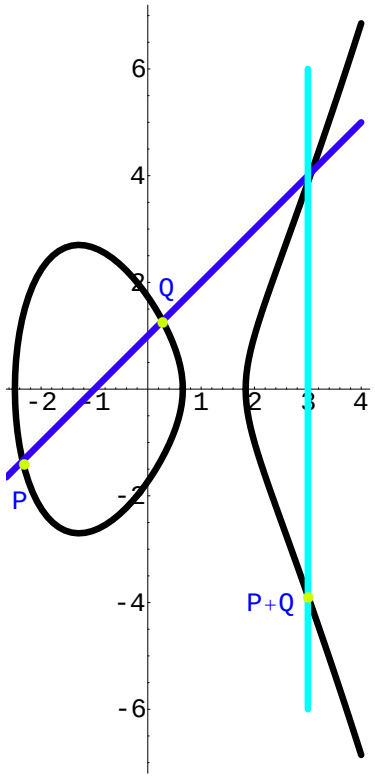


FIGURE 59: Addition of two distinct points on an elliptic curve $E : y^2 = x^3 - 5x + 3$ defined over the field of real numbers $\mathbb{R}$

To prove that $E(K)$ forms an abelian group under the addition operation defined above, we have to prove the following four statements:

(i) For all $P \in E(K), \mathcal{O} + P = P$, that is, $\mathcal{O}$ is the identity of $E(K)$.

(ii) For every $P \in E(K)$, there exists a unique point Q such that $P + Q = \mathcal{O}$. The point Q is called the inverse of point P, and is usually denoted by $-P$.

(iii) For all $P, Q \in E(K), P + Q = Q + P$, that is, the addition operation is commutative.

(iv) For all $P, Q, R \in E(K), (P + Q) + R = P + (Q + R)$, that is, the addition operation is associative.

Proof of (i). It is the direct application of Definition 35. By a change of coordinates any rational point on E can be moved to the line at infinity, that is, every point of E could act as the identity of the group $E(K)$. □

Proof of (ii). Let the third intersection point of the tangent at $\mathcal{O}$ be denoted by R. Let Q be the third intersection point of the line through P and R. Then by Definition 35, $P + Q = \mathcal{O}$. □

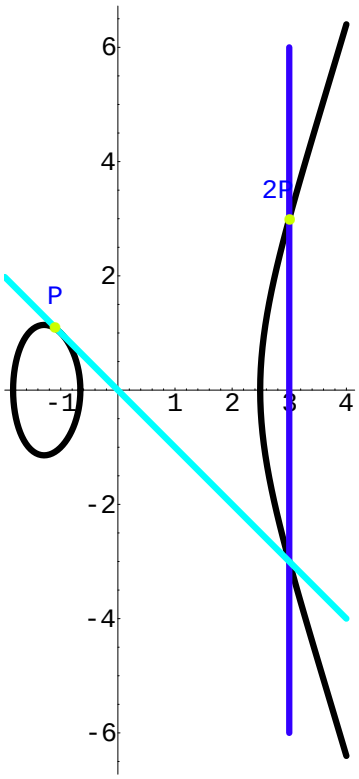


FIGURE 60: Computing $2P$ for a point P on an elliptic curve $E : y^2 = x^3 - 5x - 3$ defined over the field of real numbers $\mathbb{R}$

Proof of (iii). The addition of the points P and Q does not depend on the order of the points, as the line passing through them does not change with the order of them. This proves that the addition operation is commutative. □

Proof of (iv). We need the following lemma for the proof of associativity of the addition operation.

LEMMA 3. *If $P_1, \dots P_8$ are points in $\mathbb{P}^2$, no 4 on a line, and no 7 on a conic, then there is a 9th point Q such that an cubic through $P_1, P_2, \dots, P_8$ also passes through Q.*

Sketch of proof of lemma. Any cubic curve is given by an equation of the form

$$\begin{aligned} f(x,y,z) = i_1x^3 + i_2x^2y + i_3x^2z + i_4xy^2 + i_5xz^2 \\ +i_6xyz + i_7y^3 + i_8y^2z + i_9yz^2 + i_{10}z^3 = 0. \end{aligned}$$

Given any cubics we can add them together to get another, just by adding the coefficients; and we can also multiply by any element of K. So the cubic equations form a vector space of dimension 10, and any cubic corresponds to a point:

$$(i_1, i_2, i_3, i_4, i_5, i_6, i_7, i_8, i_9, i_{10}) \in K^{10}.$$

To say a point lies on a cubic curve given by an equation $f(X, Y, Z)$ as above puts a linear condition on the coefficients $i_1, i_2, \ldots, i_{10}$. For example, if we say that $(1, 1, 1)$ must lie on $f(x, y, z) = 0$, then we must have $f(1, 1, 1) = 0$, so we must have

$$f(1, 1, 1) = i_1 + i_2 + i_3 + i_4 + i_5 + i_6 + i_7 + i_8 + i_9 + i_{10} = 0.$$

Or, if $(1, 0, 0)$ is on $f(x, y, z) = 0$, we must have

$$f(1, 0, 0) = i_1 = 0.$$

Generally, saying that a point is on the cubic puts a linear condition on the space of cubic. So, the space of all cubics is 10 dimensional. The space of cubics through a given point, for example, the space of cubics passing through $(1, 0, 0)$ is 9 dimensional. Each extra point we require to be on a set of cubics will reduce the dimension by 1, *provided* that the conditions are linearly independent. The points $P_1, P_2, \ldots, P_8$ are linearly independent.

So the space of cubics through $P_1, \ldots P_8$ is $10 - 8 = 2$ dimensional. This two dimensional vector space will be spanned by 2 elements, call them F_1 and F_2. They span this space means that all the points $P_1, \ldots P_8$ lie on both $F_1 = 0$ and $F_2 = 0$. Therefore, for any other curve $G = 0$ through these points, that curve is in this subspace, and so can be expressed in terms of the basis, so for some μ, ν we have

$$G = \mu F_1 + \nu F_2.$$

By Bezout's theorem, Theorem 14, the number of points on $F_1 \cap F_2 = 9$. So, there is another point Q on $F_1 = 0$ and $F_2 = 0$. We have $F_1(Q) = F_2(Q) = 0$. This means that

$$G(Q) = \mu F_1(Q) + \nu F_2(Q) = 0 + 0 = 0.$$

This proves Q also lies on $G = 0$. This proves there is a ninth point, Q lying on all cubics through $P_1, \ldots P_8$. □

We need to show that for $P, Q, R \in E(K)$ we have

$$(P + Q) + R = P + (Q + R).$$

It is enough to show the equality of inverses:

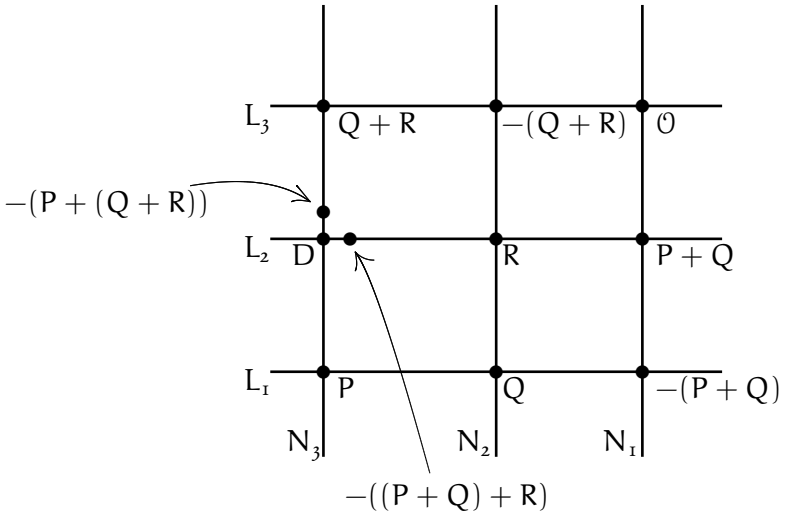
$$-((P + Q) + R) = -(P + (Q + R)).$$

Let us consider the following lines through the given points.

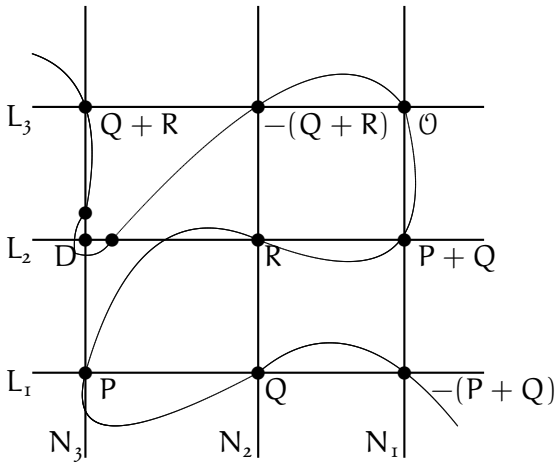
(i) L_1 through $P, Q, -(P + Q)$,
(ii) L_2 through $P + Q, R, -((P + Q) + R)$,
(iii) L_3 through $Q + R, \mathcal{O}, -(Q + R)$

(iv) N_1 through $P+Q, \mathcal{O}, -(P+Q)$,
(v) N_2 through $Q, R, -(Q+R)$,
(vi) N_3 through $P, Q+R, -(P+(Q+R))$.

We can draw a picture to represent all the above information, and we also label a point D where L_2 intersects N_3:



This picture should be taken as a reminder of which lines pass through which points, not as a remotely accurate drawing. Please note that, our elliptic curve is in the background, also passing through these points:



Again, this is not an accurate picture. Also note, we don't know whether E passes through D. This is what we want to show.

We know that $-((P+Q)+R)$ lies on L_2, by the definition of L_2. Similarly $-(P+(Q+R))$ lies on N_3, by the definition of N_3. But we would like these points to be equal, that is, they must both be equal to the point D which is on $L_2 \cup N_3$.

Now we have two cubic curves, $L_1L_2L_3 = 0$ and $N_1N_2N_3 = 0$. We know by construction that these both pass through the eight points

$$\mathcal{O}, P, Q, R, P + Q, Q + R, -(P + Q), -(Q + R).$$

By Theorem 14, we know that any two cubics intersect in 9 points. Let us call the 9th point D. Let us show that the prerequisites of Lemma 3 are met so that we can apply it. No four of the points $\mathcal{O}, P, Q, R, P + Q, Q + R, -(P + Q), -(Q + R)$ can lie on a line. If any four points are on a line, then since they are also on E, we have that $\#(L \cap E) \geqslant 4$, which contradicts Bezout's theorem. By Bezout's theorem, there are exactly $1 \cdot 3 = 3$ points on the intersection, as the line is a degree 1 curve. Also, no 7 points can lie on a conic. Suppose 7 are on a conic, as they are also on E, we get, $\#(C \cap E) \geqslant 7$, which again contradicts Bezout's theorem. Note that conic has degree 2 and so by Bezout's theorem there are $3 \cdot 2 = 6$ points on the intersection.

Now as the conditions of Lemma 3 are met, by applying it, we get that any other cubic through these 8 points also passes through D.

So, since E passes through these 8 points, it also passes through D. So on $N_1N_2N_3 \cap E$ we have the points $\mathcal{O}, P, Q, R, P+Q, Q+R, -(P+Q), -(Q+R), -(P+(Q + R)), D$. But since there are only 9 points on the intersection of two cubics, two of these must be equal, but, by definition, D is not equal to any of the first 8, so we have $D = -(P + (Q + R))$.

Similarly, by considering the 10 labeled points on $L_1L_2L_2 \cap E$, we will have $D = -((P + Q) + R))$. So we have

$$-(P + (Q + R)) = D = -((P + Q) + R)).$$

Please see web site Verrill [2004] to have a look at the nice picture showing the associativity of the addition operation. □

The group of rational points on the elliptic curves defined over the finite fields is used in cryptography. A basic example can be found in Athale and Winkler [2002] and the details can be found in many books including Blake, Seroussi, and Smart [1999].

5.3.2 Algebraic version of the addition of rational points

We now describe algebraically the group operations for Weierstrass equation. Since $\mathcal{O}$ is going to be the group identity and since it is the only point at infinity, we can confine our description of $-P_1$ and $P_1 + P_2$ to the affine coordinates: let $P_i = (x_i, y_i)$. The line $x = x_1$ contains the point P_1 and, considering its projective version $X = x_1z$, it also contains $\mathcal{O}$. Thus $-P_1$ is the third point of intersection of the line with the curve, which therefore has x-coordinate x_1 and it

remains to calculate the y-coordinate. By substituting x_1 for x in Equation (5.1) we obtain a quadratic equation for y:

$$y^2 + (a_1x_1 + a_3)y - (x_1^3 + a_2x_1^2 + a_4x_1 + a_6) = 0.$$

The sum of the roots is $-(a_1x_1 + a_3)$, and one root is y_1, hence the other root, which is the y-coordinate of $-P_1$, is $-a_1x_1 - a_3 - y_1$.

Next let us calculate $P_1 + P_2 = P_3 = (x_3, y_3)$. If $x_1 \neq x_2$, that is, $P_1 \neq \pm P_2$, then the line joining P_1 and P_2 is $y = y_1 + \lambda(x - x_1)$, where $\lambda = (y_2 - y_1)/(x_2 - x_1)$. Substituting this expression for y into the Weierstrass equation gives a cubic equation for x whose three roots are x_1, x_2, x_3. Identifying the sum of the roots with the negative of the coefficient of x^2 yields $x_3 = -x_1 - x_2 - a_2 + a_1\lambda + \lambda^2$ and putting this into the equation of the line gives the y-coordinate of $-P_3$ from which we find $y_3 = -[y_1 + (x_3 - x_1)\lambda + a_1x_3 + a_3]$.

There remains the case $P_1 = P_2$, which is treated similarly where now $y = y_1 + \lambda(x - x_1)$ is the tangent line. We get the following formulae, for $(x_2, y_2) \neq -(x_1, y_1)$ we have the addition law

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3), \tag{5.12}$$

where

$$\begin{aligned} x_3 &= -x_1 - x_2 - a_2 + a_1\lambda + \lambda^2, \\ y_3 &= -y_1 - (x_3 - x_1)\lambda - a_1x_3 - a_3, \end{aligned} \tag{5.13}$$

and

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2, \\ \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{if } x_1 = x_2. \end{cases} \tag{5.14}$$

5.4 Structure of the group

In the last section, we proved that $E(K)$ forms an abelian group. The next question is what is the structure of this group, namely is it finite or infinite? We are interested especially in the structure of the group when the elliptic curve is defined over rational numbers. We denote the set of rational numbers by $\mathbb{Q}$. The following theorem gives the answer, please see Cohen [1993]; Milne [1996].

THEOREM 17 (Mordell). *Let E be an elliptic curve over $\mathbb{Q}$. The group of points of E with coordinates in $\mathbb{Q}$ (denoted naturally by $E(\mathbb{Q})$) is a finitely generated abelian group. In other words,*

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r,$$

where r is a nonnegative integer called the rank of the curve, and $E(\mathbb{Q})_{\text{tors}}$ is the torsion subgroup of $E(\mathbb{Q})$, which is a finite abelian group.

Mazur further gave all the possible torsion groups.

THEOREM 18 (Mazur). *Let* E *be an elliptic curve over* $\mathbb{Q}$. *Then the torsion subgroup* $E(\mathbb{Q})_{\text{tors}}$ *is exactly one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z} \quad 1 \leqslant n \leqslant 10 \text{ or } n = 12,$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z} \quad 1 \leqslant n \leqslant 4.$$

We give a list of elliptic curves with their torsion subgroups. The torsion subgroup follows the equation of the curve. The examples are taken from Milne [1996, exercise 8.11] and Cremona [1997, table 1].

$y^2 = x^3 + 2$	$\mathcal{O}$
$y^2 = x^3 + x$	$\mathbb{Z}/2\mathbb{Z}$
$y^2 = x^3 + 4$	$\mathbb{Z}/3\mathbb{Z}$
$y^2 = x^3 + 4x$	$\mathbb{Z}/4\mathbb{Z}$
$y^2 + y = x^3 - x^2$	$\mathbb{Z}/5\mathbb{Z}$
$y^2 = x^3 + 1$	$\mathbb{Z}/6\mathbb{Z}$
$y^2 - xy + 2y = x^3 + 2x^2$	$\mathbb{Z}/7\mathbb{Z}$
$y^2 + 7xy - 6y = x^3 - 6x^2$	$\mathbb{Z}/8\mathbb{Z}$
$y^2 + xy + y = x^3 - x^2 - 14x + 29$	$\mathbb{Z}/9\mathbb{Z}$
$y^2 - 7xy - 36y = x^3 - 18x^2$	$\mathbb{Z}/10\mathbb{Z}$
$y^2 + 43xy - 210y = x^3 - 210x^2$	$\mathbb{Z}/12\mathbb{Z}$
$y^2 = x^3 - x$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
$y^2 = x^3 + 5x^2 + 4x$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$
$y^2 + 5xy - 6y = x^3 - 3x^2$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$
$y^2 = x^3 + 337x^2 + 20736x$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$

The above list shows that in fact one can find curves with any of the possible torsion subgroups given by Mazur. In the next section we will see given an elliptic curve how to determine its torsion subgroup.

5.5 Determination of the torsion group

The following theorem, proved independently by E. Lutz and T. Nagell, gives a very efficient method to compute the torsion subgroup of an elliptic curve defined over $\mathbb{Q}$.

THEOREM 19 (Nagell-Lutz). *Let* E *be an elliptic curve over* $\mathbb{Q}$ *with equation*

$$y^2 = x^3 + ax + b, \quad \textit{where } a, b \in \mathbb{Z}.$$

Then for all nonzero torsion points P *we have:*

(i) The coordinates of P *are in* $\mathbb{Z}$*, that is,*

$$x_P, y_P \in \mathbb{Z}.$$

(ii) If P *is of order greater than 2, then*

$$y_P^2 \mid 4a^3 + 27b^2.$$

(iii) If P *is of order 2 then,*

$$y_P = 0 \text{ and } x_P^3 + ax_P + b = 0.$$

Let us see the algorithm based on Theorem 19, as described in Cremona [1997, chapter 3]. Theorem 19 is applicable to the elliptic curves of the form $y^2 = x^3 + ax + b$, with no x^2 term. While such an equation may be obtained from $y^2 = x^3 + ax^2 + bx + c$ by completing the cube, this would involve a further scaling of coordinates, and so would lead to larger numbers. So we give the algorithm for the computation of torsion points for the elliptic curves given by $y^2 = x^3 + ax^2 + bx + c$. If $a_1 = a_3 = 0$ we can apply the following result directly; otherwise, put $a = b_2$, $b = 8b_4$ and $c = 16b_6$.

INPUT: a, b, c (integer coefficients of a nonsingular cubic).
OUTPUT: A list of all torsion points on $y^2 = x^3 + ax^2 + bx + c$, with orders.
$\Delta = 27c^2 + 4a^3c + 4b^3 - a^2b^2 - 18abc$
`y_list = positive_divisors(square_part(`Δ`))`
FOR $y \in$ `y_list` DO
  `x_list = integer_roots(`$x^3 + ax^2 + bx + c - y^2$`);`
  FOR $x \in$ `x_list` DO
    `P = point(`x, y`);`
    `n = order(P);`
    IF $n > 0$ THEN
      Output P, n
    END IF
  END FOR
END FOR
{Subroutine to compute order of a point}
$n = 1$; $Q = P$;
WHILE `integral(`x_Q`)` AND $Q \neq \mathcal{O}$ DO
  $n = n + 1$; $Q = Q + P$
END WHILE
IF $Q \neq \mathcal{O}$ THEN
  $n = 0$
END IF
Return n

For simplicity we only give the algorithm for curves with no xy or y terms; in the general case, one works internally with points on a scaled model (including the calculation of the order), as described above, converting back to the original model on output. Since we know in advance, due to Theorem 18, that no point will have order greater than 12, when computing the order of a point we simply use repeated addition until we reach a non-integral point or the identity $\mathcal{O}$. The subroutine `order(P)` returns 0 for a point of infinite order. Also: `square_part(`Δ`)` returns the largest integer whose square divides Δ; `integer_roots` returns a list of the integer roots of a cubic with integral coefficients; and `integral(x)` tests whether its (rational) argument is integral.

The remaining part of $E(\mathbb{Q})$ is an infinite group. The number of generators of this subgroup is the rank. The important fact to note is, it is very difficult to generate the curves with high rank. We will see two approaches for that, in the next chapter. Also the determination of the rank of an elliptic curve can be time consuming and at the end we might get the rank determined on the basis of some other conjectures.

CHAPTER 6

Generation of elliptic curves with high rank

> Don't tell people how to do things. Tell them what to do and let them surprise you with their results.
>
> GEORGE S. PATTON

In this chapter, we will see two approaches to generate elliptic curves with high rank. But, we also mention some methods that are used to determine the rank. These methods are used only to confirm the rank of the generated curves with the approaches discussed in this chapter, or in the software used to find rank. So, here we will not go into the details of the methods.

6.1 Determination of the rank

Cremona [1997, chapter 3] divides the procedure of the determination of rank into two parts. First, we have a searching routine which looks for points up to some bound on the numerator and denominator of the x-coordinate of points on the curve. As this routine finds points, it gives them to the second routine, which has at each stage a $\mathbb{Z}$-basis for a subgroup A of $E(\mathbb{Q})/T$, that is, $E(\mathbb{Q})$ modulo the torsion group,: initially $A = 0$. This second routine uses the height pairing to determine one of three possibilities: the new point P may be independent of those already found and can then be added to our cumulative list of independent points; the rank of A is thus increased by 1. Secondly, P may be an integral combination of the current basis (modulo torsion) and can then be ignored. Finally, if a multiple kP of P is an integral combination of the current basis for some $k > 1$, we can find a basis for a new subgroup A which contains the old A with index k.

Zimmer gives a list of the algorithms for the computation of ranks and a brief information about each of them. We list the algorithms here, please see the article for more information. It also gives reference to the original articles.

1. Manin's *conditional* algorithm
2. Special 2-descent via 2-isogeny
3. General 2-descent (following Birch and Swinnerton-Dyer)
4. General 3-descent (following J. quer)

It can take many hours to determine the rank of a given curve and in some cases it might only determined based on some conjectures.

6.2 Brown-Myers approach

In this section, we will see an elementary method to prove that every curve in a certain family of elliptic curves has rank greater than or equal 2. Please see Brown and Myers [2002] for further details. We also give some of our computations done by hand based on this idea.

Let us denote the family of elliptic curves by E_m, and is given by the following equation

$$E_m : y^2 = x^3 - x + m^2, \tag{6.1}$$

where m is a nonnegative integer. We want to show that rank of every curve defined by Equation (6.1) has rank greater than 2.

Brown and Myers observed that points P and Q, as defined below, lie on all the curves in E_m. Using the formula (5.12) for the point addition we find that following list of integer points lie on E_m.

$$\begin{aligned} P &= (0, m), \\ Q &= (-1, m), \\ P + Q &= (1, -m), \\ P + 2Q &= (m^2, m^3), \\ 2P + Q &= (4m^2 - 1, 8m^3 - 3m), \\ P - Q &= (4m^2 + 1, -8m^3 - 3m), \\ 3P &= (64m^6 - 8m^5, 512m^9 - 96m^5 + 3m) \end{aligned} \tag{6.2}$$

Based on this observation, Brown and Myers [2002] formulate the following theorem:

THEOREM 20. *Let m be a nonnegative integer, and let E_m be the elliptic curve with equation $y^2 = x^3 - x + m^2$.*

(a) If $m \geqslant 1$, *then* $E_m(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}\}$.
(b) If $m \geqslant 2$, *then* $\operatorname{rank}(E_m(\mathbb{Q})) \geqslant 2$, *and* P *and* Q *are independent points.*
(c) There are infinitely many values of m *for which* $\operatorname{rank}(E_m(\mathbb{Q})) \geqslant 3$.

In the remainder of this section, we prove the above theorem using some elementary results about elliptic curves.

6.2.1 Rational torsion and curves over finite fields

The following lemma greatly simplifies our work. If p is a prime, we write $p^e \parallel a$ if $p^e \mid a$ and $p^{e+1} \nmid a$.

LEMMA 4. *(a) If* (x, y) *is a rational point on the elliptic curve* $E : y^2 = x^3 + ax + b$, *then* $x = u/r^2$ *and* $y = v/r^3$ *for some integers* u, v, r *with* $\gcd(u, r) = \gcd(v, r) = 1$.
(b) The only rational points on $E_0 : y2 = x^3 - x$ *are* $(0, 0)$, $(1, 0)$, $(-1, 0)$, *and* $\mathcal{O}$.

Proof. (a) Put $x = u/s$ and $y = v/t$ with $\gcd(u, s) = \gcd(v, t) = 1$. A little algebra yields

$$s^3 * v^2 = t^2(u^3 + aus^2 + bs^3).$$

If $p^e \parallel s$ then $p^{3e} \mid s^3v^2$. Since $p \nmid u$ and $p \mid (aus^2 + bs^3)$, it follows that $p^{3e} \mid t^2$. No higher power of p can divide t^2; otherwise $p \mid v$, contrary to the assumption that $\gcd(v, t) = 1$. Hence, $p^{3e} \parallel t^2$. If $p^f \parallel t$, then it follows that $3e = 2f$, that is, $f = 3c$ and $e = 2c$ for some integer c. Thus, $p^{3c} \parallel t$ and $p^{2c} \parallel s$. Since this holds for each prime p, we conclude that $s = r^2$ and $t = r^3$ for some integer r.

(b) Now $\mathcal{O}$ is a rational point, by definition. Suppose (x, y) is a finite rational point of E_0; by (a), $x = u/r^2$ and $y = v/r^3$ for integers u, v, and r, with r relatively prime to u and v. Substituting and expanding, we find that

$$v^2 = u(u^2 - r^4).$$

If $u = 0, 1$, or -1, then $v = 0$, accounting for the points $(0, 0)$, $(1, 0)$, and $(-1, 0)$. Let $g = \gcd(u, v)$, so that $u = gu_1, v = gv_1$, and $\gcd(u_1, v_1) = 1$. We find that

$$gv_1^2 = u_1(g^2u_1^2 - r^4).$$

Since u_1 and v_1 have no common factors, it follows that $u_1 \mid g$; writing $g = u_1u_2$ leads to the equation

$$u_2v_1^2 = u_1^4u_2^2 - r^4.$$

Hence $u_2 \mid r^4$. But $\gcd(u, r) = 1$, so $u_2 = 1$ and we are led to the equation

$$v_1^2 = u_1^4 - r^4. \tag{6.3}$$

From Fermat's theorem that the area of a right triangle is never a square, we get that Equation (6.3) has no solutions in nonzero integers. Hence, the only rational points on E_0 are $(0, 0)$, $(1, 0)$, $(-1, 0)$, and $\mathcal{O}$.

□

Now, if $E : y^2 = x^3 + ax + b$ is an elliptic curve with a and b in $\mathbb{Z}$, and if p is a prime, then we may regard E as a *curve* over the p-element finite field $\mathbb{F}_p$, with a, b, x, and y elements of the field $\mathbb{F}_p$. If the discriminant $\Delta(E) = -16(4a^3 + 27b^2)$ is prime to p, then the cubic $x^3 + ax + b$ has distinct roots and E is an elliptic curve over $\mathbb{F}_p$. If this happens, E is said to have good reduction at p, and $E(\mathbb{F}_1)$ is called the group of $\mathbb{F}_p$-points of E.

This property is important to check because if E has good reduction at p, then the reduction modulo p theorem ensures that there is an injection, that is, a one-to-one mapping, of the group $E(\mathbb{Q})_{\text{tors}}$ of rational torsion points into the group $E(\mathbb{F}_p)$, please see Silverman and Tate [1992] for further details. This theorem makes it easy to prove the main result.

THEOREM 21. *If* $m \geqslant 1$, *then* $E_m(\mathbb{Q})_{\text{tors}} = \mathcal{O}$.

Proof. The discriminant $\Delta(E_m) = -16(27m^4 - 4)$ is never divisible by 3 or 5, so E_m has good reduction at 3 and 5.

If $3 \mid m$, then E_m reduces to $y^2 = x^3 - x$ over $\mathbb{F}_3$, and $E_m(\mathbb{F}_3) = \{\mathcal{O}, (0,0), (1,0), (-1,0)\}$, the Klein four group. Since $E_m(\mathbb{Q})_{\text{tors}}$ injects into $E_m(\mathbb{F}_3)$, it follows that $E_m(\mathbb{Q})_{\text{tors}}$ is a subgroup of the rational points of order 2 of E_m. Such a point of E_m is necessarily of the form $(r, 0)$, where r is a rational root of $x^3 - x + m^2 = 0$, that is, a rational solution to $m^2 = (-x)^3 - (-x)$. But, by Lemma 4 there are no such rational roots. Hence $E(\mathbb{Q})_{\text{tors}} = \mathcal{O}$.

If $3 \nmid m$, then $m^2 \equiv 1 \pmod 3$ and E_m reduces to $y^2 = x^3 - x + 1$ over $\mathbb{F}_3$. Here, $|E_m(\mathbb{F}_3)| = 7$, so that $|E(\mathbb{Q})_{\text{tors}}| = 1$ or 7. In addition, E_m reduces over $\mathbb{F}_5$ to $y^2 = x^3 - x$, $y^2 = x^3 - x + 1$, or $y^2 = x^3 - x - 1$ according as $m \equiv 0, \pm 1$, or $\pm 2 \pmod 5$, respectively. In each case, $|E_m(\mathbb{F}_5)| = 8$. Hence, $|E(\mathbb{Q})_{\text{tors}}| = 1, 2, 4$, or 8. Thus, $|E(\mathbb{Q})_{\text{tors}}| = 1$, and we conclude that $E(\mathbb{Q})_{\text{tors}} = \mathcal{O}$. □

6.2.2 Computing the rank of E_m

There are several ways to find the rank of $E(\mathbb{Q})$, or at least a lower bound on the rank, but most of them are complicated and rely on lots of heavy machinery. The task is daunting, especially when the curve at hand has trivial rational torsion—as our curves do. But, Brown and Myers [2002] give a simple proof of the fact that $E_m(\mathbb{Q})$ has rank at least 2 for $m > 1$. It relies on only one piece of heavy machinery. We state the theorem for our special case; the full-blown result can be found in Cremona [1997]. Recall that an elementary abelian 2-group is an abelian group in which every nonidentity element has order 2.

THEOREM 22. *Let* $E(\mathbb{Q})$ *(respectively,* $2E(\mathbb{Q})$*) be the group of rational points (respectively, doubles of rational points) on an elliptic curve* E*, and suppose that* E *has trivial rational torsion. Then the quotient group* $E(\mathbb{Q})/2E(\mathbb{Q})$ *is an elementary abelian 2-group of order* 2^r*, where* r *is the rank of* $E(\mathbb{Q})$.

Our strategy is to show that the points P, Q, and $P + Q$ from (6.2) are not doubles of rational points. This implies that the set of cosets $\{[O], [P], [Q], [P+Q]\}$ is a four element subgroup of $E(\mathbb{Q})/2E(\mathbb{Q})$ and, together with Theorem 21, that P and Q are independent. We begin by describing sufficient conditions for a rational point A not to be the double of a rational point B on E_m.

THEOREM 23. *Let* $A = (u/s^2, v/s^3)$ *and* $B = (w/t^2, z/t^3)$ *be points on* E_m, *with* $\gcd(uv, s) = \gcd(wz, t) = 1$. *If either (a)* u *is even, (b)* u *and* s *are odd and* m *is even, (c)* $u = 1 \mod 4$ *and* s *and* m *are odd, or (d)* $u = -1, s = 1$, *and* $m > 1$, *then* $A \neq 2B$.

Proof. If $B = (x, y)$ and $A = (x_o, y_o) = 2B$, then (5.13) and (5.14) imply that

$$x_o = \frac{x^4 + 2x^2 + 1 - 8m^2x}{4(x^3 - x + m^2)}.$$

Substituting $x_o = u/s^2$ and $x = w/t^2$ and expanding leads to the equation

$$4u(wt^2(w^2 - t^4) + m^2t^8) = s^2((w^2 + t^4)^2 - 8m^2wt^6). \tag{6.4}$$

The proofs in cases (a), (b), and (c) are straightforward. As for (d), let $u = -1$ and $s = 1$, that is, $x_o = -1$. Then Equation (6.4) becomes

$$-4(wt^2(w^2 - t^4) + m^2t^8) = (w^2 + t^4)^2 - 8m^2wt^6,$$

which we can expand and rearrange, yielding

$$(w + t^2)^4 = 4t^4(w^2 + 2wt^2 + m^2t^2(2w - t^2)).$$

This implies that $t \mid (w + t^2)$, so that $t \mid w$. But t and w are relatively prime, and so $t = 1$. If we substitute $t = 1$, rearrange, and simplify, we are get the equation

$$(w^2 + 2w - 1)^2 = 4m^2(2w - 1).$$

This implies that $(2w - 1) \mid (w^2 + 2w - 1)^2$, so that $(2w - 1) \mid w^2$. But again, $\gcd(2w-1, w^2) = 1$, so we conclude that $w = 1$, and so $m = 1$. Thus, if $u = -1$, $s = 1$, and $m > 1$, then A is not the double of a rational point. □

Remark 1. As a corollary, we know that if $m \geqslant 1$ then $P = (0, m) \notin 2E_m(\mathbb{Q})$ (by (a)) and $P + Q = (1, -m) \notin 2E_m(\mathbb{Q})$ (by (b) and (c)); and if $m > 1$, then $Q = (-1, m) \notin 2E_m(\mathbb{Q})$ (by (d)).

LEMMA 5. *Let* $m > 1$, *with* $P = (0, m)$ *and* $Q = (-1, m)$. *Then* $H = \{[\mathcal{O}], [P], [Q], [P + Q]\}$ *is a four-element subgroup of* $E_m(\mathbb{Q})/2E_m(\mathbb{Q})$.

Proof. By the preceding remark, we know that $[P] \neq [\mathcal{O}]$, $[Q] \neq [\mathcal{O}]$, and $[P+Q] \neq [\mathcal{O}]$. If $[P] = [Q]$, then $[P + Q] = [P] + [Q] = [P] + [P] = [2P] = [O]$, which is impossible. In a similar way, we can show that $[P]$ and $[P + Q]$ are distinct (else $[Q] = [\mathcal{O}]$), and that $[Q]$ and $[P + Q]$ are distinct (else $[P] = [O]$). We conclude that $[\mathcal{O}]$, $[P]$, $[Q]$, and $[P + Q]$ are distinct classes of $E_m(\mathbb{Q})/2E_m(\mathbb{Q})$, so H is a 4-element subgroup of $E_m(\mathbb{Q})/2E_m(\mathbb{Q})$. □

The following lemma proves that the points P and Q are independent, and that will prove the Theorem 20.

LEMMA 6. *P and Q are independent points in $E_m(\mathbb{Q})$ for $m = 2$.*

Proof. Suppose that, to the contrary, there exist integers n and k such that $nP + kQ = \mathcal{O}$. Without loss of generality, we may assume that n is positive and minimal among all such representations. If n is even and k is odd, then $[\mathcal{O}] = [nP + kQ] = [Q]$, contrary to Lemma 5. Similarly, n odd and k even imply that $[O] = [P]$, and both n and k odd imply that $[\mathcal{O}] = [P + Q]$, both contrary to Lemma 5. Finally, if $n = 2n'$ and $k = 2k'$, then $2(n'P+k'Q) = \mathcal{O}$, which implies that $n'P + k'Q$ is a rational 2-torsion point. But E_m has trivial rational torsion by Theorem 21, so that $n'P + k'Q = \mathcal{O}$, contrary to the minimality of n. □

Theorem 20(b), which is the main result that $\mathrm{rank}(E_m(\mathbb{Q})) = 2$ for $m = 2$, now follows from Lemma 6 and the fact that the rank of $E_m(\mathbb{Q})$ is just the size of a maximal independent subset of $E_m(\mathbb{Q})$.

6.2.3 Rank 3 and beyond

The strategy for finding curves of rank at least 3 is based on the following generalization of Lemma 6.

LEMMA 7. *Let R be a rational point on $E(\mathbb{Q})$, and let $P_1, \ldots, P_k$ be independent points in $E(\mathbb{Q})$. If $[R] \notin \langle [P1], \ldots, [Pk] \rangle$ in $E(\mathbb{Q})/2E(\mathbb{Q})$ and if E has trivial rational 2-torsion, then $P_1, \ldots, P_k$, and R are independent in $E(\mathbb{Q})$.*

Proof. Suppose that there exist integers $a_0, a_1, \ldots, a_k$, not all zero, such that

$$a_0R + a_1P_1 + \ldots + a_kP_k = \mathcal{O} \tag{6.5}$$

without loss of generality, we may assume that a_0 is positive and minimal among all such representations.

If a_0 is odd, then $[a_0R] = [R]$ and Equation (6.5) implies that $[R] = [a_1P_1 + \ldots + a_kP_k]$, contrary to the assumption.

If a_0 is even, then $[a_0R] = [\mathcal{O}]$, and Equation (6.5) implies that $[a_1P_1 + \ldots + a_kP_k] = [\mathcal{O}]$; since the P_i are independent, this means that all the a_i are even. Writing $a_i = 2b_i$, we see that Equation (6.5) implies that

$$2(b_0R + b_1P_1 + \ldots + b_kP_k) = \mathcal{O}.$$

This means that $b_0R+b_1P_1+\ldots+b_kP_k = \mathcal{O}$, since $E(\mathbb{Q})$ has only trivial 2-torsion; but this contradicts the minimality of a_0. □

Since our curves E_m have trivial torsion for $m > 0$, Lemma 7 applies to these curves. All we need now is one more result, similar to Theorem 23, about certain points not being doubles of other points.

LEMMA 8. *Let* $A = (u/s^2, v/s^3)$ *and* $B = (w/t^2, z/t^3)$ *be points on* E_m, *with* $\gcd(uv, s) = \gcd(wz, t) = 1$. *If* $m \equiv 0 \pmod 3$ *and* $s \not\equiv 0 \pmod 3$, *then* $A \neq 2B$.

Proof. Putting $A = 2B$ and expanding leads, as in the proof of Theorem 23, to equation Equation (6.4):

$$4u(wt^2(w^2 - t^4) + m^2t^8) = s^2((w^2 + t^4)^2 - 8m^2wt^6).$$

Considerations modulo 3 imply that if $m \equiv 0 \pmod 3$ and $s \not\equiv 0 \pmod 3$, then

$$4uwt^2(w^2 - t^4) \equiv (w^2 + t^4)^2 \pmod 3. \tag{6.6}$$

Now w and t cannot both be divisible by 3, since they are relatively prime; hence, the right side of Equation (6.6) is nonzero mod 3. But for all w and t, $wt^2(w^2 - t^4)$ is a multiple of 3. This is impossible, and so A is not the double of a rational point. □

Finally, using Lemma 8 in conjunction with other results, we can construct some infinite families of curves with rank at least 3. For example, if $R = (36n + 17, 54n^2 + 267n + 114)$ and $m = 54n^2 - 165n - 90$, then R is a point on E_m with $m \equiv 0 \mod 3$. It is easy to show that none of the points $R, P + R, Q + R$, and $P + Q + R$ is in $2E_m$:

- R and $P + R = (-36n - 127, -54n^2 + 607n - 1434)$ are integer points, so $s = 1$; by Lemma 8, $R \notin 2E_m$ and $P + R \notin 2E_m$.
- The x-coordinate of $Q + R$ has even numerator and a denominator that is a divisor of $9(2n + 1)^2$, so u is even and s is odd. By Theorem 23, $Q + R \notin 2E_m$.
- The denominator of the x-coordinate of $P+Q+R$ is a divisor of $(36n+16)^2$; hence, $s \not\equiv 0 \mod 3$, and so by Lemma 8, $P + Q + R \notin 2E_m$.

Since P and Q are independent, E_m has trivial rational torsion, and $[R] \notin \langle [P], [Q] \rangle$ in $E(\mathbb{Q})/2E(\mathbb{Q})$, now by applying Lemma 7 we get that P, Q, and R are independent points. This implies that for $m = 54n^2 - 165n - 90$, E_m has rank at least 3. Hence there are infinitely many values of m such that E_m has rank at least 3.

6.3 Yamagishi approach

In 1999, Yamagishi suggested a unified method to generate elliptic curves with high ranks. We here give the idea behind the method, for details please see Yamagishi [1999]. The development given here also follows the same paper.

6.3.1 Generic case and its specialisation

In this subsection, we construct an elliptic curve with rank n defined over the function field of an algebraic variety. Let E be an elliptic curve over a field k of characteristic $\neq 2$ defined by the following equation

$$E : y^2 = ax^3 + bx^2 + cx + d, \tag{6.7}$$

and let $f(x)$ be the right hand side of Equation (6.7). Then we can express E^n by the simultaneous equation:

$$y_i^2 = f(x_i) \text{ for } i = 1, \ldots, n. \tag{6.8}$$

Let ι_i be the involution on E^n defined by $\iota((x_i, y_i)) = (x_i, -y_i)$ for $i = 1, \ldots, n$. The variety V_n is defined as the points of E^n that remain invariant under the action of the involutions defined above, so $V_n = E^n/\langle(\iota_1, \ldots, \iota_n)\rangle$. Then the function field of V_n is the set of the invariant elements of the function field of E^n under the action of $\langle(\iota_1, \ldots, \iota_n)\rangle$.

Note that x and y stand for a pair of independent transcendentals, and also for a pair of variables related by Equation (6.7). We can write the function field of E by $L = k(x, y)$. The field L can also be described as the quadratic extension $k(x)(y)$ of the rational function field $k(x)$ defined by the polynomial quadratic in y; alternatively, $L = k(y)(x)$ is the cubic extension of the simple transcendental extension $k(y)$ of k. When several generic points $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$ are needed, as in the case of E^n, we can take the field $k(x_1, y_1, x_2, y_2, \ldots, x_n, y_n)$ where $x_1, x_2, \ldots, x_n$ are independent transcendentals and each y_i defines a quadratic extension by the equation $y_i^2 - f(x_i) = 0$.

Consequently,

$$\mathcal{K}(V_n) = \mathcal{K}(E^n)^{\langle(\iota_1, \ldots, \iota_n)\rangle} = k(y_1y_2, \ldots, y_1y_n, x_1, \ldots, x_n).$$

Since $(y_1y_{i+1})^2 = f(x_1)f(x_{i+1})$ holds for $i = 1, \ldots, n-1$, we find that V_n is defined by

$$y_i^2 = f(x_1)f(x_{i+1}) \text{ for } i = 1, \ldots, n-1. \tag{6.9}$$

Here we rename y_1y_{i+1} as y_i.

Definition 36. For $d \in k^*$, the *quadratic twist* by d of E, denoted by E_d, is given by

$$y^2 = x^3 + da_2x^2 + d^2a_4x + d^3a_6, \tag{6.10}$$

Replacing x, y with dx, d^2y we get the equivalent form

$$E_d : dy^2 = x^3 + a_2x^2 + a_4x + a_6.$$

Let E_1 and E_2 be elliptic curves. An *isogeny* between E_1 and E_2 is a morphism

$$\phi : E_1 \longrightarrow E_2$$

satisfying $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$. E_1 and E_2 are *isogenous* if there is an isogeny ϕ between them $\phi(E_1) \neq \{\mathcal{O}_{E_2}\}$. Then

$$\mathrm{Hom}(E_1, E_2) := \{\text{isogenies } \phi : E_1 \longrightarrow E_2\}.$$

$\mathrm{Hom}(E_1, E_2)$ is a group under the addition law

$$(\phi + \psi)(P) = \phi(P) + \psi(P) \text{ for } \phi, \psi \in \mathrm{Hom}(E_1, E_2).$$

If $E_1 = E_2$, then we can also compose isogenies.

Definition 37. Let E be an elliptic curve. Then

$$\mathrm{End} = \mathrm{Hom}(E, E),$$

be the ring with addition as above and multiplication given by composition

$$(\phi\psi)(P) = \phi(\psi(P)).$$

Let E_b be the twist of E by the quadratics extension $k(E^n)/k(V_n)$. It is defined by the equation

$$f(x_1)y^2 = f(x).$$

Let $E_b(\mathcal{K}(V_n))$ be the group of $\mathcal{K}(V_n)$-rational points on E_b.

Theorem 24. *If* $\mathrm{End}_k \cong \mathbb{Z}$, *then the rank of* $E_b(\mathcal{K}(V_n))$ *is* n, *and its generators are the following:*

$$(x_1, 1)\left(x_{i+1}, \frac{y_i}{f(x_1)}\right) \text{ for } i = 1, \ldots, n-1.$$

Now, we can obtain a given elliptic curve with its generators by specialising the above twisted generic elliptic curve at a certain k-rational point on V_n as follows:

Lemma 9. *Let* E *be a given elliptic curve defined by the following equation*

$$E : y^2 = ax^3 + bx^2 + cx + d, \tag{6.11}$$

and let (α_i, β_i) *for* $i = 1, \ldots, n$ *be its independent generators. Let* E_b *be the twist of* E *by* $\mathcal{K}(E^n)/\mathcal{K}(V_n)$. *Then* E *with these generators is obtained by specialization at the point* $(x_1, \ldots, x_n, y_1, \ldots, y_{n-1}) = (\alpha_1, \ldots .\alpha_n, \beta_1\beta_2, \ldots, \beta_1\beta_n)$ *on* V_n.

Proof. Please see Yamagishi [1999]. □

6.3.2 Case of rank 2

We give the details for case of rank 2. In the original paper the proof is not given. The variety V_2 is defined by the equation $(y_1y_2)^2 = f(x_1)f(x_2)$. By renaming (y_1y_2) as z we get the defining equation of V_2 as

$$z^2 = f(x_1)f(x_2). \tag{6.12}$$

We consider V_2 over the field $K = k(x_1, x_2)$. It is a three dimensional subvariety in the projective space $\mathbb{P}^4$ with coordinates (a, b, c, d, z). The variety V_2 is defined by one quadratic equation with a rational point $P_1(a, b, c, d, z) = (0, 0, 0, 1, 1)$. Hence we can show that V_2 is birationally equivalent to $\mathbb{P}^3$, or in other words V_2 is K-rational. We can parametrise K-rational points on V_2 as follows:

THEOREM 25. *The variety V_2 is rational and each K-rational point on V_2 is expressed as*

$$((S + T)p_1, (S + T)p_2, (S + T)p_3, (S + T)p_4 - ST, -ST),$$

where $(p_1, p_2, p_3, p_4) \in \mathbb{P}^3$ and

$$S = p_1x_1^3 + p_2x_1^2 + p_3x_1 + p_4, T = p_1x_2^3 + p_2x_2^2 + p_3x_2 + p_4.$$

Proof. First we want to get the mapping from $\mathbb{P}^3$ to V_2 and to find this mapping we want to find the general equation of a line passing through the point $P_1 = (a_0, b_0, c_0, d_0, z_0) = (0, 0, 0, 1, 1)$. A line passing through this point will intersect V_2 in one more point. In this way we will get parametrisation of V_2. We can write the equations defining the line as follows:

$$\begin{aligned} (a - a_0) &= p_1(z - z_0) \\ (b - b_0) &= p_2(z - z_0) \\ (c - c_0) &= p_3(z - z_0) \\ (d - d_0) &= (p_4 + 1)(z - z_0) \end{aligned} \tag{6.13}$$

where p_1, p_2, p_3 and p_4 are independent parameters. By substituting the values of a_0, b_0, c_0, d_0, z_0 and simplifying we get the equations defining the line.

$$\begin{aligned} a &= p_1(z - 1) \\ b &= p_2(z - 1) \\ c &= p_3(z - 1) \\ d &= p_4(z - 1) + z \end{aligned} \tag{6.14}$$

Now we want to eliminate four variables from Equation (6.12) and Equation (6.14) to get an equation in one variable, namely z. Substituting the values of variables a, b, c and d in terms of z, and writing S and T for $p_1x_1^3 + p_2x_1^2 + p_3x_1 + p_4$

and $p_1x_2^3 + p_2x_2^2 + p_3x_2 + p_4$, respectively, in Equation (6.12) we get a quadratic equation in z.

$$z^2 = ((S+1)z - S) \cdot ((T+1)z - T)\,.$$

We know that $z = 1$ is a solution of the quadratic equation, as the point P_1 has z coordinate 1. We get the other root by dividing the quadratic equation by $z - 1$;

$$z = \frac{ST}{ST + S + T}.$$

Substituting this in the expressions for a, b, c and d we get the values of them in the parameters $(p_1, p_2, p_3, p_4) \in \mathbb{P}^3$.

$$a = \frac{-p_1(S+T)}{ST+S+T}, \quad b = \frac{-p_2(S+T)}{ST+S+T}, \quad c = \frac{-p_3(S+T)}{ST+S+T},$$
$$d = \frac{-p_4(S+T)+ST}{ST+S+T}, \quad z = \frac{ST}{ST+S+T}.$$

By adjusting the negative sign and canceling the denominators we get the parametrisation as in the statement of the theorem.

To prove that it is K-rational we also need a mapping from V_2 to $\mathbb{P}^3$. Take the ratio of p_1, p_2, p_3 and p_4 where we get the value of p_is from Equation (6.14).

$$(p_1, p_2, p_3, p_4) = \left(\frac{a}{z-1}, \frac{b}{z-1}, \frac{c}{z-1}, \frac{d-z}{z-1}\right).$$

We get the mapping as follows:

$$\begin{aligned} p_1 &= a \\ p_2 &= b \\ p_3 &= c \\ p_4 &= d - z. \end{aligned} \tag{6.15}$$

We proved that the variety V_2 is birationally equivalent to $\mathbb{P}^3$. □

In the proof we have used an ad hoc idea for determining a parametrisation of the variety V_2. In recent years the parametrisation problem for algebraic curves and surfaces has been investigated in great detail, please see Sendra and Winkler [1997] and Schicho [1998].

CHAPTER 7

Computational results

> In theory, there is no difference between theory and practice; In practice, there is.
>
> CHUCK REID

We give the details of the findings from the implementation of Yamagishi's method mentioned in the previous chapter. In the original paper, it is not mentioned that the method does not always gives the desired result. We give, so to say, counterexamples for the method and suggest the values of parameters, which will give the desired result. Also we give the results of the other rank computations on the curves considered in Brown-Meyers approach.

7.1 Dimension of V_n is 3

In Yamagishi [1999], the author gives a proof of the fact that the dimension of V_n is 3. The proof is very complicated and requires very specialised results. We have found a way to find the dimension of V_n using Macaulay for $n = 2, 3, \ldots, 10$. Also there is an easy way to prove that the dimension of this variety is greater than or equal to 3.

We first prove that the dimension of V_n given by Equation (6.9) is greater than or equal to 3 for all n. We use the following theorem to prove the result, please see Shafarevich [1994, Corollary 5, page 71] for the proof and further details.

THEOREM 26. *The variety of common zeros of* r *forms* $F_1, \ldots, F_r$ *on an* m*-dimensional projective variety has dimension* $\geqslant m - r$.

THEOREM 27. *For* $n \geqslant 2, \dim V_n \geqslant 3$.

Proof. From Equation (6.9) we know that V_n is defined using $n-1$ equations. These $n-1$ equations are homogeneous equations of order 2 over $k(x_1,\ldots,x_n)$. So there are $n-1$ forms and the variety is defined over $\mathbb{P}^{n+2}$ with coordinates $(a,b,c,d,y_1,\ldots,y_{n-1})$. Applying Theorem 26 we get that the dimension of the variety $V_n \geqslant n+2-n+1=3$. □

We proved that the dimension of V_n is exactly 3 for $n=2,3,\ldots,10$ using Macaulay. We give the details of the experiment for $n=3$. The variety V_3 is defined by two equations, namely $y_1^2=(ax_1^3+bx_1^2+cx_1+d)(ax_2^3+bx_2^2+cx_2+d)$ and $y_2^2=(ax_1^3+bx_1^2+cx_1+d)(ax_3^3+bx_3^2+cx_3+d)$.

```
i1 : R=QQ[x_1,x_2,x_3]
```

Here, `i1 :` is the first input prompt of Macaulay for the user. In response to the prompt, we enter the arithmetic expression to be evaluated.

```
o1 = R
o1 : PolynomialRing
```

The answer to the input is displayed to the right of the output label `o1 =` and its type, or class, is displayed on the next line.

```
i2 : S=frac R
o2 = S
o2 : FractionField

i3 : T=S[a,b,c,d,y_1,y_2]
o3 = T
o3 : PolynomialRing

i4 : I=ideal(
   y_1^2-((a*x_1^3+b*x_1^2+c*x_1+d)*(a*x_2^3+b*x_2^2+c*x_2+d)),
   y_2^2-((a*x_1^3+b*x_1^2+c*x_1+d)*(a*x_3^3+b*x_3^2+c*x_3+d))
   )
o4 : Ideal of T

i5 : J=Proj(T/I)
o5 = J
o5 : ProjectiveVariety

i6 : dim(J)
o6 = 3
```

Our coefficient ring is $\mathbb{Q}(x_1,x_2,x_3)$, which we generate using first two commands. Then we define our $\mathbb{P}^5$ space. Then using command `Proj` we define the

projective variety V_n and lastly get the dimension of the variety. The computations took few seconds for $n = 2, 3$ and in the end for $n = 10$ it took about 2 hours.

7.2 Implementation results of Yamagishi's algorithm

We give the function written in Maple 8 to generate elliptic curves with rank 2 using Yamagishi's method. The analysis of the results, namely checking the ranks of the generated curves was time consuming. We give examples of parameter values where the method does not generate an elliptic curve or generates elliptic curve with lower rank than stated in the method. We suggest the values of the parameters which in all experiments generated the curves with rank greater than or equal to the desired rank, namely 2. We have also implemented this for rank 3 but could only test this for rank 2, as the testing, namely the rank determination is time consuming.

7.2.1 Maple code

```
ECRankY:=proc()
local S,T,p,i,rand010, rand110;
rand010:=rand(0..10);
rand110:=rand(1..10);
if nargs=0 then
   print("There is nothing to compute");
   return NULL;
fi;
if (args[1]=2) then
   for i from 1 to 6 do
      p[i]:=rand110();
   od;
   if (1<nargs) then
      for i from 2 to min(nargs,7) do
         p[i-1]:=args[i];
      od;
   fi;
   if (2<nargs and args[2]=args[3]) then
      print("x1 and x2 cannot be equal,
           choosing a random value for x2<>x1");
   fi;
   if (7<nargs) then
      print("Maximum 7 arguments are accepted, you provided",
           nargs);
```

```
      print("Only first 7 arguments will be considered");
   fi;
   while p[1]=p[2] do
     p[2]:=rand010();
   od;
   printf("Chosen parameters are: x1=\%d, x2=\%d,p1=\%d,
         p2=\%d,p3=\%d,p4=\%d\\n",p[1],p[2],p[3],
         p[4],p[5],p[6]);
   S:=(p[3]*p[1]^3)+(p[4]*p[1]^2)+(p[5]*p[1])+p[6];
   T:=(p[3]*p[2]^3)+(p[4]*p[2]^2)+(p[5]*p[2])+p[6];
   return p[3]*(S+T),0,p[4]*(S+T),0,p[5]*(S+T),p[6]*(S+T)-S*T
fi;
if (args[1]<>2) then
   print("The method is implemented for n=2 for now,
        therefore first argument should be 2");
fi;
end proc;
```

The function ECRankY takes 1 to 7 inputs. It returns 6 values, which can directly be plugged in as input to Ein0 command from apecs package. Ein0 defines the elliptic curve with the six arguments where the first argument is the coefficient of the x^3 term. The remaining arguments are a_1, a_2, a_3, a_4 and a_6 from Weierstrass form of elliptic curve equation. As can be seen in Equation (6.7), the method generates elliptic curves that do not contain terms xy and y. So, $a_1 = a_3 = 0$.

The first input is the rank, it will use the method for that particular rank. Currently only method for rank 2 is incorporated in this general function, therefore the first argument has to be 2. All other arguments are optional. If no other argument is provided the function will generate them randomly from integers 0 to 10, or 1 to 10, as some of the arguments should be greater than 1 for the desired results. We choose the random numbers from integers 0 to 10 as these numbers rapidly increase the size of the coefficients of the resulting elliptic curve. Note that we have cubic terms in some of the inputs, like $S = p_1x_1^3 + p_2x_1^2 + p_3x_1 + p_4$. This in turn makes the determination of the rank difficult and time consuming.

Next two arguments, x_1 and x_2, if equal, produce curves with rank 1. We will give example in the next subsection. Therefore if these arguments are equal, we choose x_2 randomly from integers 0 to 10.

The next four arguments are the parameters p_1, p_2, p_3, p_4. If not provided, we choose them randomly from integers 1 to 10. If some of the parameters are 0 we might not even get an elliptic curve, that is why we choose them from positive integers.

7.2.2 Bad choices for the input arguments

Yamagishi's method does not give the desired result for every choice of input parameter values. We give here some examples where we even do not get elliptic curve. We give the results for the method for rank 2 and 3. For higher rank, it is time consuming to determine the rank of the resulting curve.

Rank 2		
Parameter values $x_1, x_2, p_1, p_2, p_3, p_4$	Generated elliptic curve $a_0, a_1, a_2, a_3, a_4, a_6$	Rank
1, 2, 0, 0, 0, 1	0, 0, 0, 0, 0, 1	-
1, 2, 0, 1, 0, 0	0, 0, 5, 0, 0, -4	-
0, 1, 1, 0, 1, 0	2, 0, 0, 0, 2, 0	0
0, 1, 1, 0, 0, 1	3, 0, 0, 0, 0, 1	1^*
Rank 3		
Parameter values $x_1, x_2, x_3, p_1, p_2, p_3, p_4$	Generated elliptic curve $a_0, a_1, a_2, a_3, a_4, a_6$	Rank
0, 1, 2, 1, 1, 1, 1	0, 0, 0, 0, 0, 4	-
0, 1, 2, 0, 1, 1, 1	0, 0, 0, 0, 0, 4	-
1, 2, 3, 0, 1, 1, 1	0, 0, 4, 0, -4, 12	-
3, 1, 2, 1, 1, 1, 1	504, 0, -1467, 0, 873, 112	2^*
0, 1, 2, 1, 2, 3, 4	-8, 0, 172, 0, 0, 16	2^*

TABLE 85: Examples of parameter values for Yamagishi's method where we do not get the elliptic curves with the desired rank

In Table 85, a_0 denotes the coefficient of x^3 in the equation of elliptic curve and a_1, a_2, a_3, a_4, a_6 denote the coefficients as in Equation (5.1). We can transform this equation into Weierstrass form using the transformation $U = x/a_0$ and $V = y/a_0$, where the original equation is in x and y. 1^* and 2^* denote that the rank 1 or 2, respectively, was determined based on some of the conjectures from Taniyama conjecture, Birch and Swinnerton-Dyer conjecture and Riemann Hypothesis, in `apecs`. Further details can be found in help for `apecs` and Milne [1996]. The examples given in Table 85 are not mentioned in the original paper Yamagishi [1999], the author does not even mention their existence.

7.2.3 Results with good input arguments

We randomly generated more than 200 curves using our implementation of Yamagishi's method for rank 2. Table 86 gives the number of generated elliptic

curves with the corresponding rank. As above * shows that the rank was determined on the basis of some of the conjectures. The range for ranks, like 2-4, is given when the system returns the answer like the range is between 2 and 4. Table 86 shows that we could only determine the range of the rank in most of the cases. But the most important thing is all the curves have rank greater than or equal to 2. We have introduced two constraints on the input arguments:

1. $x_1 \neq x_2$,
2. p_1, p_2, p_3, p_4 are nonzero.

With these constraints, all the curves we generated randomly by our implementation have the ranks greater than or equal to 2. In the case of rank 3, we could not find any such constraints. This was also due to the fact that the rank determination for the curves generated in the case of rank 3 took considerably more time.

Rank	Number of elliptic curves
2*	4
3*	10
4*	8
2 - 4	27
2 - 6	45
2 - 8	10
3 - 5	45
3 - 7	50
3 - 9	1
4 - 6	16
4 - 8	1
5 - 7	1

TABLE 86: Ranks of curves generated randomly using implementation of Yamagishi's method for rank 2

7.3 Results from other rank computations

We determined the ranks of curves given by Equation (6.1) for $m = 1$ to $m = 10,000$. We list the number of curves for each rank up to 1000 and 10,000. Also we checked the ranks of the curves of the type $y^2 = x^3 - t^2x + 1$ for $t = 1$ to $t = 4000$. In Brown and Myers [2002] it is mentioned without proof that the curves of this type have rank greater than or equal to 3 for $t > 3$. We list the number of curves for each rank up to 1000 and 4000.

We used the program `mwrank` for the determination of the rank. Please see Cremona [2004] for further details and to get `mwrank`. As can be seen from

Table 87 there are many curves whose rank could only be determined to be in the certain range, like 2-4. As the value of m or t increases the rank determination takes few hours for each curve. So there are more curves with the rank values in intervals, like 2-4, when we consider higher values for m or t. The percentage of number of curves of higher ranks increases with the values of m and t. For example, there are 93 curves with rank 6 if we consider curves with m up to 10,000, as compared to only 5 curves when we consider m up to 1000.

Ranks	Number of elliptic curves up to 1000	up to 10,000
1	1	1
2-3	-	15
2-4	8	210
2	225	2017
3-5	1	69
3	458	4167
4-6	1	16
4	248	2683
5	53	727
6	5	93
7	-	2

(i) $y^2 = x^3 - x + m^2$

Ranks	Number of elliptic curves up to 1000	up to 4000
1	1	1
2	2	2
3-4	-	1
3-5	3	35
3	218	737
4-6	2	18
4	412	1600
5	271	1164
6	82	375
7	9	66
8	-	1

(ii) $y^2 = x^3 - t^2x + 1$

TABLE 87: Ranks of elliptic curves of type $y^2 = x^3 - x + m^2$ and $y^2 = x^3 - t^2x + 1$

Bibliography

Rahul Ramesh Athale. *Verifying the jumping champion conjecture*. Technical Report 02-17, Research Institute for Symbolic Computation, Johannes Kepler University, Linz, Austria, 2002. The report is electronically available as `ftp://ftp.risc.uni-linz.ac.at/pub/techreports/2002/02-17.ps.gz`.

Rahul Ramesh Athale. Prime gaps modulo a perfect number. 2003. The talk at the Journées Arithmétiques, Graz, Austria, July 6–12, 2003.

Rahul Ramesh Athale and Franz Winkler. *Curves in Cryptography*. Technical Report 02-16, Research Institute for Symbolic Computation, Johannes Kepler University, Linz, Austria, 2002. The report is electronically available as `ftp://ftp.risc.uni-linz.ac.at/pub/techreports/2002/02-16.ps.gz`.

C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier. *User's Guide to PARI/GP*, November 2000. `http://www.parigp-home.de`.

Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart. *Elliptic Curves in Cryptography*. Number 265 in London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 1999.

Richard P. Brent. The Distribution of Small Gaps Between Successive Primes. *Mathematics of Computation*, 28(125): 315–324, January 1974. The article is electronically available from `http://web.comlab.ox.ac.uk/oucl/work/richard.brent/pub/pub021.html`.

Richard P. Brent. Irregularities in the Distribution of Primes and Twin Primes. *Mathematics of Computation*, 29(129): 43–56, January 1975. The article is electronically available from `http://web.comlab.ox.ac.uk/oucl/work/richard.brent/pub/pub024.html`.

Ezra Brown and Bruce T. Myers. Elliptic Curves from Mordell to Diophantus and Back. *American Mathematical Monthly*, 109(7): 639–649, August-September 2002. The article is electronically available from author's web site as `http://www.math.vt.edu/people/brown/doc/dioellip.pdf`.

J. W. S. Cassels. *Lectures on Elliptic Curves*. Number 24 in London Mathematical Society Student Texts. Cambridge University Press, Cambridge, 1991.

Bruce W. Char, Keith O. Geddes, Gaston H. Gonnet, Benton L. Leong, Michael B. Monagan, and Stephen M. Watt. *Maple V Library Reference Manual*. Springer, 1991.

Denis Xavier Charles. *Sieve Methods*. Master's thesis, University at Buffalo, The State University of New York, 2000. Available electronically as `http://www.cs.wisc.edu/~cdx/Sieve.pdf`.

Henry Cohen. *A Course in Computational Algebraic Number Theory*. Number 138 in Graduate Texts in Mathematics. Springer-Verlag, New York, 1993.

Ian Connell. Elliptic Curve Handbook. The first five chapters of the lecture notes are electronically available from the author's web site `http://www.math.mcgill.ca/connell/`, 1999.

David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1998. Corrected second printing.

John E. Cremona. *Algorithms for Modular Elliptic Curves*. Cambridge University Press, second (online) edition, 1997. The book is available online from `http://www.maths.nott.ac.uk/personal/jec/book/fulltext/index.html`.

John E. Cremona. mwrank. The program and further information can be obtained from `http://www.maths.nottingham.ac.uk/personal/jec/packages.html`, 2004.

Pamela Cutter. Finding prime pairs with particular gaps. *Mathematics of Computation*, 70(236): 1737–1744, 2001.

Harvey Dubner. Personal communication, 2003.

Harvey Dubner and Harry Nelson. Seven consecutive primes in arithmetic progression. *Mathematics of Computation*, 66(220): 1743–1749, October 1997.

David Eisenbud, Daniel R. Grayson, Michael E. Stillman, and Bernd Sturmfels, editors. *Computations in algebraic geometry with Macaulay 2*. Number 8 in Algorithms and Computations in Mathematics. Springer-Verlag, 2001. The book is available electronically from the book's web site `http://www.math.uiuc.edu/Macaulay2/Book/`.

Paul Erdős and E. G. Straus. Remarks on the differences between consecutive primes. *Elemente der Mathematik*, 35(5): 115–118, 1980.

Stéfane Fermigier. Elliptic Curves. http://www.fermigier.com/fermigier/elliptic.html.en.

William Fulton. *Algebraic Curves*. Advanced Book Classics. Addison-Wesley, reprint edition, 1989.

Richard K. Guy. *Unsolved Problems in Number Theory*. Problem Books in Mathematics. Springer-Verlag, New York, 1981.

G. H. Hardy and J. E. Littlewood. Some problems of 'Partitio Numerorum' III: On the expression of a number as a sum of primes. *Acta Mathematica*, 44: 1–70, 1922.

G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, Ely House, London W. 1, fourth edition, 1975.

Rob Harley. Some estimates due to Richard Brent applied to the "high jumpers" problem. The article is electronically available at http://pauillac.inria.fr/~harley/wnt.html, 1994.

Robin Hartshorne. *Algebraic Geometry*. Number 52 in Graduate Texts in Mathematics. Springer-Verlag, New York, 1977.

Richard Lowry. Inferential Statistics. http://faculty.vassar.edu/lowry/webtext.html.

William Mendenhall and Terry Sincich. *Statistics For Engineering and the Sciences*. Prentice Hall, Englewood Cliffs, New Jersey 07632, fourth edition, 1995.

James S Milne. Elliptic Curves. The lecture notes are electronically available from the author's web site http://www.jmilne.org/math/index.html, 1996.

James S Milne. Algebraic Geometry. The lecture notes are electronically available from the author's web site http://www.jmilne.org/math/index.html, 2003.

Thomas R. Nicely. http://www.trnicely.net/gaps/gaplist.html.

Thomas R. Nicely. New maximal prime gaps and first occurrences. *Mathematics of Computation*, 68(227): 1311–1315, July 1999. The updated electronic version is available at http://www.trnicely.net/gaps/gaps.html.

Speech Group NIST. Wilcoxon Signed-Rank Test. http://www.nist.gov/speech/tests/sigtests/wilcoxon.htm, 2000.

Bertil Nyman and Thomas R. Nicely. New prime gaps between 10^{15} and $5 * 10^{16}$. *Journal of Integer Sequences*, 6(3): 1–6, 2003. The article is electronically available as http://www.math.uwaterloo.ca/JIS/VOL6/Nicely/nicely2.pdf.

Andrew Odlyzko, Michael Rubinstein, and Marek Wolf. Jumping Champions. *Experimental Mathematics*, 8(2): 107–118, 1999. The article is electronically available as `http://www.dtc.umn.edu/~odlyzko/doc/jumping.champions.pdf`.

Andrew M. Odlyzko. Sieve Methods. 1971. Senior thesis California Institute of Technology, Pasadena, California. The thesis is available electronically from `http://mimosa1.incubator.uiuc.edu/jba/BOOKS_Historical/`.

Andrew M. Odlyzko. Iterated absolute values of differences of consecutive primes. *Mathematics of Computation*, 61(203): 373–380, 1993. The article is electronically available as `http://www.dtc.umn.edu/~odlyzko/doc/arch/gilbreath.conj.pdf`.

Paul Pollack. Not Always Buried Deep: Selections from Combinatorial and Analytic Number Theory. The notes are available electronically as `http://www.princeton.edu/~ppollack/notes/notes.pdf`, 2004.

John Renze, Stan Wagon, and Brian Wick. The Gaussian Zoo. *Experimental Mathematics*, 10(2): 161–173, 2001.

Dave Rusin. The Mathematical Atlas. `http://www.math.niu.edu/~rusin/known-math/index/14H52.html`.

Josef Schicho. Rational Parametrization of Surfaces. *Journal of Symbolic Computation*, 26(1): 1–29, 1998.

J. Rafael Sendra and Franz Winkler. Parametrization of Algebraic Curves over Optimal Field Extensions. *Journal of Symbolic Computation*, 23(2&3): 191–207, 1997.

Igor R. Shafarevich. *Basic Algebraic Geometry 1*. Springer-Verlag, Berlin Heidelberg, second, revised and expanded edition, 1994. Translated from the original Russian text into English by Miles Reid.

David J. Sheskin. *Handbook of Parametric and Nonparametric Statistical Procedures*. Chapman & Hall/CRC, third edition, 2004.

Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Number 106 in Graduate Texts in Mathematics. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Number 151 in Graduate Texts in Mathematics. Springer-Verlag, New York, 1994.

Joseph H. Silverman and John Tate. *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

William Arthur Stein. An Explicit Approach to Number Theory. In progress book, available electronically from http://modular.fas.harvard.edu/edu/Fall2001/124/utm/.

Helena A. Verrill. Group Law for Elliptic Curves. The article is available electronically from http://www.math.ku.dk/~verrill/grouplaw/.

Helena A. Verrill. Elliptic curves with H. A. Verrill. The article is available as http://www.math.lsu.edu/~verrill/teaching/math7280/index.html, 2004.

Eric W. Weisstein. Chinese Remainder Theorem. From MathWorld–A Wolfram Web Resource. Available electronically as http://mathworld.wolfram.com/ChineseRemainderTheorem.htm.

Franz Winkler. Commutative Algebra and Algebraic Geometry. Lecture Notes, Research Institute for Symbolic Computation, Johannes Kepler Universität, 1999–2000.

Marek Wolf. http://www.ift.uni.wroc.pl/~mwolf/.

Stephen Wolfram. *The Mathematica Book*. Wolfram Media, Inc.& Cambridge University Press, 1999.

Hizuru Yamagishi. A unified method of construction of elliptic curves with high Mordell-Weil rank. *Pacific Journal of Mathematics*, 191(1): 189–200, 1999. The article is electronically available from the journal's web site as http://nyjm.albany.edu:8000/PacJ/1999/191-1-12.html.

Horst G. Zimmer. Basic algorithms for elliptic curves. The article is available electronically from SIMATH web site http://tnt.math.metro-u.ac.jp/simath/.