TOPICS IN NUMBER THEORY:

An Olympiad-Oriented Approach

Masum Billal **Amir Hossein Parvardi**

Sample Chapters

Version 1.1.

July 2018

Dedicated to

Our regular studies, without which, we could have finished this book long time ago.
Fermat, the father of modern number theory.
Euler, without whom number theory probably wouldn't be so rich today.
Ramanujan, mathematician of mathematicians.
Paul Erdős, the man who loved only numbers.

Links

- The website of the book always contains the updates, errata, and new free materials that we regularly post on social media. Exclusive olympiad problem-sets will be released in the website in the near fuure:

  https:/TopicsInNumberTheory.com

- Facebook page:

  https://facebook.com/TopicsInNumberTheory/

  This is our main page for feedback and reviews on the book. Feel free to post any kind of review, comment, solution, or suggestion you have about this book. Amir Hossein will create a forum for the book on AoPS so everyone can post their solutions to be added to the book later on.

- If you find any mistake or typo in the book, we would be happy to hear it at Facebook or info@TopicsInNumberTheory.com.

- This is version 1.1. of the sample chapters, including chapters 4 (Primes) and 5 (Special Topics) plus the appendix. As we update the book, we also update these samples also on our website. To keep track of the latest updates, please keep this URL (from which you downloaded the file) somewhere safe:

  https://TopicsInNumberTheory.com/download/samplechapters/

  The password might be changed for the future updates, but we will always send the new passwords to our subscribers in Facebook and in the newsletter.

- The password for this edition is `Riemann`.

Copyright Notice

The cover shows a part of the famous paper of Bernhard Riemann in 1859 in Number Theory. It was taken from the website of Clay Mathematics Institute. You can read the original manuscript as well as the English translation of this wonderful paper by David Wilkins in their website:

http://www.claymath.org/publications/riemanns-1859-manuscript

This file was prepared by Masum Billal and Amir Hossein Parvardi, as a gift to all the kind people who were looking forward to reading our book. You can read this PDF, print the file on paper, share it with your friends, or discuss the problems on our Facebook page, but please do not upload this PDF file into the public. Keep it private!

Copyright © 2018 TopicsInNumberTheory.com
Masum Billal and Amir Hossein Parvardi
All rights reserved.

First Words by Masum

I would like to have a few words before diving into the discussion. First of all, from my personal experience, I have found that there is a common practice to learn1 by learning a lot of theories and then investigating how those theories are used to solve problems. As our primary audience would be students who are looking to get into mathematical olympiads, I highly discourage this. Please do not take number theory for a collection of theories just because the word theory is literally juxtaposed with it. That being said, one could say that our book itself is a collection of a lot of theorems as well. Sadly, that is partially true for multiple reasons even though it was not our intention at all.

When I first thought about writing this book, my intention was to make students realize that they do not need to know a lot of theorems in order to be able to solve problems. My primary target was to build confidence about this claim. But as we kept writing we had to increase the pace since we had to cover a lot (and that was discarding a lot of contents which we thought would ask for even discussion or we just felt lazy about it), we had to increase the pace.

I would like to address one more concern. Originally, my plan was to make this book a series of 5 volumes, this being the first one. In those volumes I wanted to discuss a lot of topics such as special numbers like *egyptian fraction* or even interesting numbers like *abundant number or deficient number* and their properties etc or crucial topics such as *Diophantine equations*. You will notice that we have left a lot of important topics like those out of this book. The reason is, I quickly realized I can hardly finish writing this first volume, and if I wanted to complete the series we will probably have to keep writing my whole life. So, I had to discard a lot of contents and make the book concise which resulted in squeezing in a lot of contents in a few hundreds of pages.

Finally, I would like to thank Amir to join me in this project. At one point I stopped writing the book. If he had not agreed to be a co-author, this book would have probably not been completed at all. More so because he agreed to follow the style I wanted to write in even when we had objection from reputed publisher like *Springer*.

Masum Billal
July 2018.

First Words by Amir Hossein

In the past three years, we have been always worried about this book. It's been a long and tedious job to manage everything and edit all we had written a very long time ago. After I studied higher level number theory concepts, there were times that I found errors/typos in my previous drafts for the book. And that sometimes happened two or more times in a short period, and so, it was getting annoying. Anyhow, we managed to finish it at this time of the summer. It is now 5:36 AM, Tuesday, July 17, 2018 that I'm writing this. You can imagine how crazy this process has made me!

BUT! a wise man once said "high quality math books are written in a series of editions in long term," and we are happy to hear that. Many of our friends helped us during the way to finish this book, as mentioned in the Acknowledgement, and we are so proud to have such friends.

I wouldn't be able to finish my part in this book if I didn't have the support of my wonderful, beautiful, and lovely wife **Nadia Ghobadipasha**. She gave me hope to choose mathematics and always believed in me. She was my only one in the hardest days of life.

Professor **Peyman Nasehpour**, whom I knew from the very first semester of my undergraduate studies in elelctrical englineering at University of Tehran, helped me a lot in the process of enhancing my mathematical abilities to change my field to mathematics (number theory) for my master's. He is an inspiration to me, and a great colleague when it comes to teamwork. I'm looking forward to working with him more ofter.

The idea behind the lattices in the (paperback) **cover** is a geometric proof of law of quadratic reciprocity. Our friends found other interpretations of it such as Pick's theorem (which is not the case here) or the sum of positive integers up to n, which you will realize is also not always true (for all primes p, q). Section (5.9) is dedicated to this proof and investigates why it is true using counting the lattice (grid) points. When we picked this idea for the cover, we chose quadratic reciprocity because its proof is geometrically visual and indeed very beautiful. Our hope was to make the reader curious because the design looks familiar. Stay excited until you read that proof! Or, maybe, go read it if you have the prerequisite knowledge and the puzzle is boggling your mind. I remember I found the idea of the proof in one of Kenneth H. Rosen's books on discrete mathematics, but I'm not sure which one, as it was a long time ago when I wrote it. I used TikZ package for LaTeXto write the codes and generate the graphs.

There are so many wonderful things to learn in this book. I hope you enjoy it!

Amir Hossein Parvardi,
University of British Columbia,
Vancouver, BC, Canada,
July 2018.

Acknowledgement

Here is a list of all the kind people who helped us review, edit, and improve this book. We could not decide who to thank more, hence an alphabetically (last name) ordered list:

1. Thanks to **Ali Amiri**, a kind friend who helped us in the cover design.

2. Thanks to **AnréC** from TeX.StackExchange who wrote the code for figure (1.1) in base conversion.

3. Thanks to **Kave Eskandari** for reading the whole book and commenting on the general points. He caught a good mistake in chapter 1.

4. Cheers to our mathematical friend **Leonard Mihai C. Giugiuc** from Romania who gave us positive and constructive feedback on the book. He also wrote us a wonderful review in the website.

5. Thanks to **Valentio Iverson** for proof-reading chapters 3 and 5, and pointing out the typo in figure (3.1).

6. Thanks to **Aditya Khurmi** for reading the book and giving us positive feedback.

7. We appreciate **Hesam Korki**'s comments on chapter 1. He mentioned a few very important typos, including grammatical. He also mentioned a mathematical change in that chapter, which was very helpful.

8. We appreciate **Kenji Nakagawa**'s precise points on chapters 4 and 5 that we sent to our website subscribers as samples of the book. He sent us a review a few hours after we sent the sample chapters! We are thankful for his quick and useful review.

9. Professor **Peyman Nasehpour** sent us the beautiful problem (4.6.11) and an amazing solution using Prime Number Theorem. He also gave us pretty useful comments on chapter 1. He also introduced in section (3.3.2) the amicable numbers to us with a brief historical note on it.

10. We are thankful to **Mohammadamin Nejatbakhshesfahani**, Iran National Olympiad Gold Medalist (2010) and winner of gold medals at IMS and IMC, who honored us toread and reviewe the whole book and gave us really instructive comments.

11. We would like to thank **Nur Muhammad Shafiullah Mahi** for his efforts to make this book better.

12. We are honored to thank Professor **Greg Martin**, a faculty member at the Mathematics Department of University of British Columbia. He happens to be Amir Hossein's Master's supervisor. He kindly reviewed a printed draft of the book and emailed us over 10 major points to correct in the book. We do appreciate his advice on improving the whole context of the book.

13. We are thankful to **Sohrab Mohtat** for his comments on chapter 1. Thanks to him, we avoided a fatal mistake in the beginning of the book. He also wrote a very useful and detailed review for our book in the website.

14. We are thankful to **Aditya Guha Roy** who reviewed the whole book and caught a few LaTeX typos, generalized lemma (6.28), fixing problems in chapter 7. Aditya wrote an amazing, educative review in our website.

15. **Navneel Singhal** carefully reviewed and proof-read the whole first part of the book (chapters 1 to 5) and gave us very constructive comments. We are thankful to him.

16. Thanks to **Amin Soofiani**, who is a Master's student of mathematics at University of British Columbia, we noticed there was a mistake in theorem (4.3.3). He did a perfect, precise, and detailed review on chapter 4.

17. We are thankful to **Sepehr Yadegarzadeh** for informing us about the correct *umlaut*[1] for Möbius among other grammatical and vocabulary points.

[1] *umlaut*: a mark (¨) used over a vowel, as in German or Hungarian, to indicate a different vowel quality, usually fronting or rounding.

Contents

Notations

- $\mathbb{N}, \mathbb{N}_0$, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{P}$, and $\mathbb{C}$ are the sets of positive integers, non-negative integers, integers, rational numbers, real numbers, primes and complex numbers, respectively.
- $|a|$ denotes the absolute value of a for any real number a.
- $\min(a, b)$ is the minimum of a and b and $\max(a, b)$ is the maximum of a and b.
- (a, b) and $[a, b]$ are greatest common divisor and least common multiple of a and b respectively.
- $a|b$ means b is divisible by a without any remainder.
- $a \perp b$ means $(a, b) = 1$.
- p_n is the n^{th} prime.
- $\pi(x)$ is the number of primes less than or equal to the real number x.
- $\varphi(n)$ is the number of positive integers less than n which are coprime to n.
- $d(n)$ is the number of divisors of n.
- $\sigma(n)$ is the sum of divisors of n.
- $\phi(n)$ is the *Euler function.*
- $\mu(n)$ is the *Möbius function.*
- $\lambda(n)$ is the *Carmichael function*
- $v_n(a)$ is the largest non-negative integer α so that $n^\alpha | a$ but $n^{\alpha+1} \nmid a$.
- $n! = 1 \cdot 2 \ldots n$.
- $\binom{n}{k}$ is the *binomial coefficient* indexed by non-negative integers n and k.
- $\left(\frac{a}{p}\right)$ is the *Legendre symbol* for integer a and prime p.
- $\lfloor x \rfloor$ is the largest integer not greater than x.
- $\lceil x \rceil$ is the smallest integer integer not less than x.

Chapter 4

Primes

Contents

4.1 Introduction

Prime numbers just might be the most mysterious topic in mathematics. There are already countless books on the topic. We have already defined prime numbers in chapter (1). Recall that a positive integer p is a prime if and only if it has exactly two positive divisors: only 1 and p itself (recall how this lets us deal with the case of 1 automatically). In this chapter, we are going to explore the properties of primes.

We will start with a widely discussed topic: **Infinitude of primes**. Besides providing Euclid's proof of the theorem, we will show some other proofs. Many of them are not very common these days. We try to provide precise history such as, who the

proof should be accredited to and when etc. As we go on, we will encounter the famous ingenious proof by Erdős, an elementary proof of *Bertrand's postulate*. We will also discuss primality testing and some relevant theorems. Most of them will be interconnected. But you may be surprised when you see that we have discussed some things at the end of this chapter which are not quite elementary or Olympiad style topics. Still, we decided to include them because they let us understand why numbers dance the way they do. Probably this will not make sense to many people, but we think so. We would feel really good if we could provide the elementary proof of **Prime Number Theorem** by **Erdős** and **Selberg**[1] as well but had we done so, we would be way off topic. Therefore, we will keep the analytic stuff as limited as possible, yet giving an insight to what make number theorists think that way or what drives them study so hard.

In section (4.8), we will discuss how to list primes efficiently or decide whether an integer is prime or not, and how to factorize an integer quickly. Now, there are a few points to clear out in the last statement.

1. Why do we need a list of primes?

2. Why do we need a way to detect primes?

3. Why do we care how quickly we can factorize an integer? Because we can just factorize 12 as $2^2 \cdot 3$ by hand, right?

If you remember, we asked you to factorize 357879581 (yes, we used this number because it had larger prime factors than we usually deal with and because we knew the factors[2]). If you actually tried doing that without using a computer, you must have cursed us all the way. Why? Because the smallest prime factor of 357879581 is 479, and the other one is 747139. As you can see, as the numbers get bigger, there prime factors get bigger as well. And of course we don't want to do all that by hand. We shouldn't do that either. Computers help us in the computing part, we just need to tell the computer how to do that. Now, this is where we introduce the idea of **algorithm**. We used this word back in chapter (1), where we first used *Euclidean Algorithm*. A funny way to say what algorithm is: *the word used by programmers when they don't want to explain what they did*. People sometimes say that because often algorithms are complex and not very understandable at first glance. However, algorithm actually means a set of operations which can define an entire process to do something, and this process is used for computer programs. Another question may strike you again. Why should we care about large numbers and determine if they are prime or not? The answer is not directly related to Olympiad or problem solving. This is necessary for programming purposes primarily, but they rely on number theoretic results to perform these factorizations or similar tasks. And they are used in a lot of area such as security. For example, every

[1] We accredit both of them, not only for avoiding any controversy, also because we believe they both had contributions. Specially, after reading some papers (such as [5]) from a close colleague of both of them, the authors are convinced they both had their parts in this proof.

[2] In fact, this is an integer the first author once thought was prime because he was using trial and error to determine if it is prime. After he exhausted a lot options, he thought it was actually a prime. But finally, it was revealed using a computer that it is not. And unless you like a lot of tedious calculation, you won't like the trial and error process by hand either

time you log ito Facebook, you use your password and this password is **encrypted**[3]. Now, for this encryption, often large integers with large prime factors are used[4]. And often encryption systems rely on the fact that, some integer that has been used in the process of encryption, can not be factorized. If they can be factorized the secret data that was used to turn your password into the code, would be revealed to the third party and thus, they would know your password. So from this perspective, it is pretty important. But even if you ignore this practical fact, you can just think about contributing to the literature of mathematics and enriching it, providing better ways to factorize so the process is not so tedious anymore. For this reason, we have decided to include some really nice results and algorithms for prime factorization or primality testing.

It would be appropriate to mention that, $\mathbb{P}$ is the set of primes and p_i is the i^{th} prime, starting with $p_1 = 2, p_2 = 3$ and so on unless mentioned otherwise[5]. Also, $\tau(n)$ is the number of positive divisors of n. *Riemann's Zeta function*, also simply called the Zeta function, is a very important subject of interest and has a long interesting history behind it. The usage and applications of Zeta function is beyond the scope of this book, but as it is a very useful tool in inspecting number theory problems, we will introduce a very simple definition of it. This definition needs precision, otherwise it may lead to confusing conclusions. Therefore, we will only assume the following definition solely for the use of this book, and not go into any complex details about the validity of the definition or similar stuff. And in this text, we do not need any such discussion either.

Definition 4.1.1 (Riemann's Zeta Function). Let s be a a real number larger than 1. The *Zeta function* of s is defined as

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \ldots = \sum_{i \geq 1} \frac{1}{i^s}$$

It is one of the most well known functions in number theory. Euler defined it first in 1737 but Riemann is known for his works on this function.

4.2 Infinitude Of Primes

Euclid first proved that the number of primes is infinite. Here we provide some proofs of this theorem, including a number theoretic version of Euclid. The idea is pretty interesting and the same thought works for similar types of problems.

Theorem 4.2.1. *The number of primes is infinite.*

Euclid's proof. Consider the converse: assume that number of primes is finite. Let $P = \{p_1, p_2, \ldots, p_k\}$ be the set of all primes. Euclid's idea was to construct a number

[3]meaning it is turned into a code so others don't recognize this if they ever see this data containing your password, so you should understand why it is so important.

[4]we are not going to discuss anything in deep since this is not a computer science or cryptography book, rather just a short note on why you should care about fast prime factorization

[5]Sometimes we may denote the canonical prime factorization as $p_1^{e_1} \cdots p_k^{e_k}$. It's important to distinguish between them.

which has a prime divisor not in P. Consider the number:

$$N = p_1 p_2 \cdots p_k + 1.$$

N is not a prime, because it is clearly bigger than all elements of P. So, N is composite and it has a divisor p in P (because P is the set of all primes). However,

$$(N, p) = (p_1 \cdots p_k + 1, p_i) = (1, p_i) = 1 \tag{4.1}$$

for some $p_i \in P$, which is in contradiction with $p|N$. Therefore, the set of primes is infinite. □

Note. The idea of Euclid was actually to construct a larger prime knowing previous ones. As you see in the above proof, the product of primes $p_1, p_2, \ldots, p_k$ plus one is relatively prime to all of those primes, meaning that it is a prime itself.

Kummer's proof[6]. Again, it suffices to prove that for any n, there is a larger prime than n. Consider $N = n! + 1$. Any prime less than n is coprime to N. Therefore, it must have a prime divisor greater than n. □

Goldbach's proof. We are done if we can show that there is a strictly increasing infinite sequence of positive integers $a_1, a_2, a_3 \ldots$ so that they are pair-wisely coprime. Since no prime can divide two terms of the sequence, each time a new term appears it will produce a new prime factor. So, all we have to do is find such a sequence. One way to do it is using *Fermat numbers*. The n^{th} Fermat number, F_n, is defined as $F_n = 2^{2^n} + 1$. In the following lemma, we will show that any two Fermat numbers are coprime to each other. □

Lemma 4.2.2. *If $m \neq n$, then $(F_m, F_n) = 1$.*

Proof. Note the identity:

$$\begin{aligned} F_n - 2 &= 2^{2^n} - 1 \\ &= \left(2^{2^{n-1}} + 1\right)\left(2^{2^{n-2}} + 1\right) \cdots \left(2^2 + 1\right)(2^1 + 1)(2 - 1) \\ &= F_{n-1} F_{n-2} \cdots F_0 \end{aligned}$$

Therefore, if $n > m$, then $F_m | F_n - 2$. If p is a prime so that $p|F_m$ and $p|F_n$, then $p|F_n - 2$ and so $p|2$, which is a contradiction since p has to be an odd prime. □

There are other proofs that use the same idea of coprime integers.

Schorn's Proof. First we will prove the following:

$$(j(n!) + 1, i(n!) + 1) = 1$$

for $1 \leq i < j < n + 1$. We can write $j = i + k$, so $1 \leq k < n$. By Euclidean algorithm,

$$\begin{aligned} ((i + k)(n!) + 1, i(n!) + 1) &= (i(n!) + 1 + k(n!), i(n!) + 1) \\ &= (k(n!), i(n!) + 1). \end{aligned}$$

We also know from proposition (1.2.6) that if $(a,b)=1$, then $(a,bc)=(a,c)$. Clearly $(n!, i(n!)+1)=1$ since $i(n!)+1$ leaves a remainder of 1 when divided by $n!$. Therefore,

$$\begin{aligned}((i+k)(n!)+1, i(n!)+1) &= (k(n!), i(n!)+1)\\ &= (k, i(n!)+1).\end{aligned}$$

Since $k<n$, we also have that k divides $n!$, so $i(n!)+1$ leaves a remainder of 1 when divided by k too. Finally, we have

$$(j(n!)+1, i(n!)+1) = ((i+k)(n!)+1, i(n!)+1) = (k, i(n!)+1) = 1.$$

From this we can say, the integers $i(n!)+1$ for $1\leq i\leq n$ are coprime. And so, we are done. □

This elegant proof is due to J. Braun (1896).

Proof by Braun. Assume that primes are finite, and $p_1, p_2 \ldots, p_k$ are all of them. Let $P = p_1 p_2 \cdots p_k$ and set

$$\frac{1}{p_1} + \cdots + \frac{1}{p_k} = \frac{a}{P}. \tag{4.2}$$

Note that

$$\begin{aligned}\frac{a}{P} &> \frac{1}{2}+\frac{1}{3}+\frac{1}{5}\\ &= \frac{31}{30} > 1.\end{aligned}$$

So $a>P$. Obviously, a has a prime divisor p. Since P is the product of all primes, p must divide P. Let $p=p_i$ for some $1\leq i\leq k$ and rewrite equation (4.2) to obtain

$$a = \frac{P}{p_1} + \cdots + \frac{P}{p_i} + \cdots + \frac{P}{p_k}. \tag{4.3}$$

Obviously, $p_i | \frac{P}{p_j}$ for all $j\neq i$. On the other hand, p divides a. Equation (4.3) now forces $p_i | \frac{P}{p_i}$, which is a contradiction. □

Here is a combinatorial proof by Perott, which dates back to almost $1801-1900$.

Perott's proof. We will use the fact that if $a>b$ then $\frac{1}{a}<\frac{1}{b}$, specially, $\frac{1}{n+1}<\frac{1}{n}$ for $n\geq 1$. Now

$$\begin{aligned}\sum_{i\geq 1}\frac{1}{i^2} &= 1+\sum_{i\geq 2}\frac{1}{i^2}\\ &< 1+\sum_{i\geq 2}\frac{1}{i(i-1)}\\ &= 1+\sum_{i\geq 2}\left(\frac{1}{i-1}-\frac{1}{i}\right)\\ &= 1+\left(1-\frac{1}{2}\right)+\left(\frac{1}{2}-\frac{1}{3}\right)+\left(\frac{1}{3}-\frac{1}{4}\right)+\cdots\\ &= 1+1=2.\end{aligned}$$

Therefore,

$$\sum_{i\geq 1} \frac{1}{i^2} = 2 - m, \tag{4.4}$$

for some positive real m. Let's get to the proof. Like before, we assume there are only k primes $p_1, p_2 \ldots, p_k$. Take $n = p_1 p_2 \cdots p_k$ and any integer $N > n$. Since there are no primes besides these k, any square-free number must be a divisor of n. Therefore, there are 2^k square-free numbers. Let p be a prime. The number of positive integers less than or equal to N which are divisible by p^2 is $\lfloor N/p^2 \rfloor$. So, the number of positive integers less than or equal to N which are divisible by any of $p_1^2, p_2^2, \ldots$, or p_k^2 [7] is less than

$$\left\lfloor \frac{N}{p_1^2} \right\rfloor + \left\lfloor \frac{N}{p_2^2} \right\rfloor + \cdots + \left\lfloor \frac{N}{p_k^2} \right\rfloor \;=\; \sum_{i=1}^{k} \left\lfloor \frac{N}{p_i^2} \right\rfloor.$$

Since any number is either square-free or non-square-free, we have

$$\begin{aligned} N &\leq 2^k + \sum_{i=1}^{k} \left\lfloor \frac{N}{p_i^2} \right\rfloor \\ &< 2^k + \sum_{i=1}^{k} \frac{N}{p_i^2} \\ &= 2^k + N \sum_{i=1}^{k} \frac{1}{p_i^2}. \end{aligned} \tag{4.5}$$

From equation (4.4), we get

$$\begin{aligned} \sum_{i=1}^{k} \frac{1}{p_i^2} &= \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{p_k^2} \\ &< \sum_{i=2}^{p_k} \frac{1}{i^2} < \sum_{i\geq 2} \frac{1}{i^2} \\ &= \sum_{i\geq 1} \frac{1}{i^2} - 1 \\ &= 1 - m. \end{aligned}$$

Substitute this into equation (4.5),

$$\begin{aligned} N &< 2^k + N \sum_{i=1}^{k} \frac{1}{p_i^2} \\ &< 2^k + N(1 - m). \end{aligned}$$

Rewriting the above inequality, we get $Nm < 2^k$. Note that 2^k is fixed, whereas we can make Nm as large as we want since N can be any integer larger than n. So, for those N, we get a contradiction, W^5 (Which Was What We Wanted). □

[7] These are actually non-square-free integers up to N.

The next proof uses Zeta function. But we need some more theorems to state it. The following theorem is due to Euler.

Theorem 4.2.3.

$$\zeta(1) = 1 + \frac{1}{2} + \frac{1}{3} + \cdots = \prod_{p \in \mathbb{P}} \frac{p}{p-1}.$$

Proof. Euler investigated the sum (which is known as the *Harmonic Series*):

$$S = \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n} + \cdots .$$

Consider the sum in terms of prime factorization. Obviously, $1, \frac{1}{2}, \frac{1}{2^2}, \ldots$ are part of the series. So are $\frac{1}{3}, \frac{1}{3^2}, \ldots$ and $\frac{1}{5}, \frac{1}{5^2}, \ldots$ and so on. If you understood the fact we showed above, note that $\frac{1}{2} \cdot \frac{1}{3}$ gives $\frac{1}{6}$. Similarly, $\frac{1}{2^2} \cdot \frac{1}{3} = \frac{1}{12}$ and $\frac{1}{3} \cdot \frac{1}{5} = \frac{1}{15}$ and so on.

We know that any number can be written as a product of primes in a unique way. Therefore, when we are multiplying some powers of primes, we will get a unique number. In other words, the same number won't appear twice. As an example, notice the following sum:

$$\begin{aligned} S_1 &= \left(1 + \frac{1}{2} + \frac{1}{2^2} + \cdots\right) \cdot \left(1 + \frac{1}{3} + \frac{1}{3^2} + \cdots\right) \\ &= 1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{3} + \frac{1}{2 \cdot 3} + \frac{1}{2^2 \cdot 3} + \frac{1}{3^2} + \frac{1}{2 \cdot 3^2} + \frac{1}{2^2 \cdot 3^2} + \cdots \\ &= 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{3} + \frac{1}{6} + \frac{1}{12} + \frac{1}{9} + \frac{1}{18} + \frac{1}{36} + \ldots \end{aligned}$$

Unique prime factorization guarantees that none of $2, 4, 6$ or 18 will appear anywhere in the series again. That is, any number of the form $2^i 3^j$ will appear exactly in this series. Similarly, if we considered all the numbers generated by $2^i 3^j 5^k$, we would have numbers like $30, 60$ or 90 exactly once in the series. So, going this way, we can see that the sum S is nothing but the product of sums $1 + \frac{1}{p} + \frac{1}{p^2} + \cdots$ for all primes p. So

$$\begin{aligned} S &= 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots \\ &= \left(1 + \frac{1}{2} + \frac{1}{2^2} + \cdots\right) \cdot \left(1 + \frac{1}{3} + \frac{1}{3^2} + \cdots\right) \cdot \left(1 + \frac{1}{5} + \frac{1}{5^2} + \cdots\right) \cdots \\ &= \prod_{p \in \mathbb{P}} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right), \end{aligned} \tag{4.6}$$

where $\mathbb{P}$ is the set of all primes. Back in high school, we learnt that the infinite geometric series $1 + r + r^2 + \cdots$ where the ratio r has absolute value less than 1, has a finite sum

$\frac{1}{1-r}$. Here, $r = \frac{1}{p} < 1$, and hence

$$\begin{aligned} 1 + \frac{1}{p} + \frac{1}{p^2} + \cdots &= \frac{1}{1 - \frac{1}{p}} \\ &= \frac{p}{p-1}. \end{aligned}$$

Replacing this in equation (4.6), we get the desired result

$$\begin{aligned} S &= 1 + \frac{1}{2} + \frac{1}{3} + \cdots \\ &= \prod_{p \in \mathbb{P}} \frac{p}{p-1}. \end{aligned}$$

□

Euler found a general result for $\zeta(s)$ for any positive integer s. We have stated this result in the following theorem. The proof is analogous to the proof of the previous theorem.

Theorem 4.2.4.

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots = \prod_{p \in \mathbb{P}} \frac{p^s}{p^s - 1}$$

Theorem 4.2.5. *The series $S = 1 + \frac{1}{2} + \frac{1}{3} + \cdots$ diverges, i.e., it does not have a finite sum.*

Proof. We can write S as

$$\begin{aligned} S &= \frac{1}{1} + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) + \cdots \\ &> \frac{1}{1} + \frac{1}{2} + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) + \cdots \\ &= 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \cdots \\ &= 1 + 1 + \cdots \end{aligned}$$

So the sum diverges. □

You may think that $\zeta(2), \zeta(3), \ldots$ all diverge too. Wrong! Using calculus Euler also proved the following theorem:

Theorem 4.2.6 (Euler's $\zeta(2)$ theorem). $\zeta(2) = \frac{\pi^2}{6}$. *In other words,*

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6}.$$

We are now ready to prove the infinitude of primes using Zeta function.

Proof using Zeta Function. In theorem (4.2.5), it is already proved that S is infinite. A series diverges if it has an infinite sum. If the number of primes is finite, then the product of all $\frac{p}{p-1}$ would be finite too. But it gives us a contradiction. Thus, the number of primes must be infinite. □

We provide yet another proof due to Euler. The proof was published after his death. The proof uses multiplicative property of Euler's Totient function.

Proof using Euler function. Let P be the product of all primes (since they are finite, P is finite too). Assume that the primes are $p_1, p_2, \ldots, p_k$ and they are sorted, i.e., $2 = p_1 < 3 = p_1 < \cdots$. Then $P = p_1 \cdot p_2 \cdots p_k$ and P is square-free as well. Using the formula of Euler function,

$$\begin{aligned}\varphi(P) &= (p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1) \\ &\geq 1 \cdot 2 \cdots 2 \\ &\geq 2^{k-1} \\ &\geq 2\end{aligned}$$

if $k > 1$. Since $2, 3$ are primes, evidently, $k \geq 2$. So the last line holds true. This implies that $\varphi(P)$ is at least 2, and there are at least two positive integers less than or equal to P which are coprime to P. If we discard 1, there is at least one other positive integer which is coprime to P. That positive integer must have another prime divisor which does not divide P. Now the claim follows. □

In the previous discussion, we have shown that there are infinitely many primes in several different ways.

Theorem 4.2.7. *There are infinitely many primes of the form $4m + 3$.*

Proof. We proceed the same way as Euclid did. Let $p_1, p_2, \ldots, p_k$ be all the primes of the form $4m + 3$. Consider the number $N = 4p_1p_2 \cdots p_k - 1$. Clearly, $N \equiv 3 \pmod 4$. According to theorem (1.4.14) in chapter (1), N has at least one prime factor p which is of the form $4m + 3$. This prime p divides N, so it is coprime to $N - 1 = 4p_1p_2 \cdots p_k$, which means that p is none of those $p_1, p_2, \ldots, p_k$. Therefore, another prime p of the form $4m+3$ exists. This is a contradiction. So, the number of such primes is infinite. □

Theorem 4.2.8. *There are infinitely many primes of the form $4n + 1$.*

Proof. Let's say the number of primes of this form is finite. Call these primes $p_1, p_2, \ldots, p_k$. Consider the number $N = 4p_1^2 \cdots p_k^2 + 1$. Using corollary (2.8.12) of chapter (2), we get that every divisor of N is of the form $4t + 1$. Thus, a prime divisor p of N must be of the same form. The contradiction follows. □

Theorem 4.2.9. *Let p be a prime. There are infinitely many primes of the form $pn+1$.*

Proof. The theorem is obvious for $p = 2$ since all primes are odd. Assume that p is odd. Let us rephrase the theorem: for each prime p, there are infinitely many primes q such that $q \equiv 1 \mod p$. Let $X \geq 2$ be an integer. We know from theorem (2.12.9) that any prime divisor $q \neq p$ of $\frac{X^p-1}{X-1}$ is either p or $1 \pmod p$.

For the sake of argument, suppose that $q_1, q_2, \ldots, q_n$ are the only primes which are $1 \mod p$. Set $X = pq_1q_2\cdots q_n$ and consider the number

$$\begin{aligned} N &= \frac{X^p - 1}{X - 1} \\ &= \frac{(pq_1q_2\cdots q_n)^p - 1}{pq_1q_2\cdots q_n - 1} \end{aligned}$$

N is an integer which is not divisible by any of the q_i or p and is greater than 1. So N has a prime divisor, say r. This r must be congruent to 1 modulo p. Contradiction! □

Theorem 4.2.10. *let $p > 2$ is a prime, then there are infinitely many primes q such that q is a quadratic residue modulo p.*

Proof. According to previous theorem, there are infinitely many primes q such that $q \equiv 1 \pmod p$. So, all these primes are quadratic residues modulo p and we are done. □

You might have already conjectured that there are infinitely many primes of the form $an + 1$. Even more generally $an + b$, where a and b are coprime positive integers. And luckily, this is true and *Dirichlet* was the first one to prove it. Though the proof of this theorem is way beyond the scope of this book. It is even accepted in many mathematics competitions. You should still try to avoid using it. Use it only if you find no other way. For most of the problems, there is a solution to that does not require a high level theorem like this. Readers are highly encouraged to try for a different solution even if it makes their lives a lot harder.

Theorem 4.2.11 (Dirichlet's Theorem on Arithmetic Progressions). *If a and b are two coprime positive integers, then there are infinitely many primes the arithmetic progression*

$$a + b, 2a + b, 3a + b, \ldots$$

In other words, there are infinitely many primes of the form $an + b$.

4.3 Formula For Primes

Mathematicians have been trying to find a closed form for primes for a long time. But this was such a mystery that many mathematicians thought it is not possible to find a formula for primes. You may have thought so too! Whenever someone tries to find a formula for primes, they tend to go for polynomials first. Our sympathies for them. Because the following theorem tells us that we can not find a non-constant polynomial which will always output a prime (for positive integer inputs of course).

Theorem 4.3.1. *There is no non-constant polynomial $P(x)$ with integer coefficients such that $P(n)$ is a prime for all integers n.*

Proof. Let P be a polynomial that generates only primes. Then $P(0) = p$ for some prime p. That is, $P(x)$ looks like

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + p.$$

Put $x = kp$ in the above equation. We find that $p|P(kp)$ for all integers k. However, since $P(kp)$ is a prime, we must have $P(kp) = p$ for all integers k. Now consider the polynomial $Q(x) = P(px) - p$. All integers are roots of $Q(x)$, which is impossible unless $Q(x)$ is the zero polynomial. So $P(px) = p$ for all real numbers x. Hence, $P(x)$ is constant. □

Back to the original question: are there any closed form for p_n? Is there an expression which always generates a prime? The answer is yes for both of them. However, here we will concentrate on the number of primes mostly[8]. It makes sense that the formula for primes and the prime counting function are close to each other. Because if you get a good formula for $\pi(n)$, the number of primes less than or equal to n, you can replace n with p_k for some k and get a recursive formula for primes, that is in terms of previous primes or positive integers less than p_k. However, recursive formulas do not look pretty at all. Therefore, we focus on finding $\pi(n)$ rather than a direct formula for p_n. The following theorem is one of those ideas which can give us a formula for the prime counting function, due to the first author (unpublished). Let's see the theorem and then explain the idea behind it.

Theorem 4.3.2 (Masum Billal). *The number of primes less than or equal to n can be obtained as*

$$\pi(n) = \sum_{i=2}^{n} \left\lfloor \frac{2}{\sum_{j=1}^{i} \left\lfloor \frac{i}{j} \right\rfloor - \left\lfloor \frac{i-1}{j} \right\rfloor} \right\rfloor$$

Don't frown just because it looks ugly! It is actually very simple. Let us slowly proceed how we can get to this expression.

Proof. First idea: assume $f(i) = 1$ if i is prime, otherwise 0. Then we will have

$$\pi(n) = \sum_{i=2}^{n} f(i)$$

This is pretty obvious. Each time we get a prime we are just adding 1 to the sum. All we have to do is find a good expression for $f(i)$ that is computable in terms of i. Remember that a prime has exactly 2 divisors. And any positive integer greater than 1 has at least two divisors. Therefore, if $\tau(i)$ is the number of divisors of i, $\tau(i) \geq 2$ for

[8] We would like to discuss the second question as well but it requires some analytical number theory, which of course is out of our scope. If you are an interested reader, you can study *Ingham's theorem*,[6] *Mill's theorem*[7] and *Niven's theorem*[8].

$i > 1$. This gives us $\lfloor 2/\tau(i) \rfloor = 0$ if i is composite, otherwise 1. Since for composite i, $\tau(i) > 2$. Now, the formula for $f(i)$ becomes

$$f(i) = \left\lfloor \frac{2}{\tau(i)} \right\rfloor$$

But this is still not computable in terms of i. We employ the same idea again, we add 1 to $\tau(n)$ each time we get a divisor of n. How do we do that? Assume that if i is a divisor of n then $t_n(i) = 1$, otherwise 0. Then,

$$\tau(n) = \sum_{i=1}^{n} t_n(i)$$

Finding $t_n(i)$ can be easy. For $i < n$, we need to add 0 when i doesn't divide n, otherwise 1. Assume that $n = ik + r$ with $r < i$ and $n - 1 = il + s$ with $s < i$. If i divides n then $r = 0$ and we would have that $n - 1 = il + s = ik - 1$. Thus, $ik - il = s + 1$ with $s + 1 \leq i$. But $i(k - l) = s + 1$ gives us $s + 1 \geq i$ since $i|s + 1$ and $s + 1$ is a positive integer, $k > l$ (why?). This forces $s + 1 = i$ and $k - l = 1$. The nicer news is that $k - l = 1$. And if i didn't divide n, we would have $k = l$ (prove it) or $k - l = 0$. Okay, that's good news. We have found our characteristic function $t_n(i)$. What is the meaning of k and l in terms of i and n? $k = \lfloor n/i \rfloor$ and $l = \lfloor (n-1)/i \rfloor$, so we get

$$t_n(i) = \left\lfloor \frac{n}{i} \right\rfloor - \left\lfloor \frac{n-1}{i} \right\rfloor.$$

This completes the proof. □

Have you ever thought about finding the number of primes not exceeding n yourself? This is actually a very intriguing question for most of the people interested in number theory, even for curious school students. At first it seems impossible to find a closed form in such a case. However, as you think more, you can find different ways to proceed. The above one is an example. This should enable you to find one as well. Here is another example, and you may be surprised at this approach. In fact, we have used it before when we tried to find the number of coprime integers less than or equal to n. The idea is similar, in a sense that it is recursive in a way. Since it is troublesome to directly find the number of primes, we will do exactly the opposite. We will find the number of **non-primes** not exceeding n. Then we can just subtract it from n. Now, we intend to find the number of positive integers m such that $m = ab$ with $a, b > 1$. More specifically, we can say that the smallest prime divisor does not exceed $\sqrt{n}$ (recall this from chapter (1)). Let $p_1, p_2, \ldots, p_k$ be the primes not exceeding $\sqrt{n}$ in increasing order. That is, p_k is the largest prime less than or equal to $\sqrt{n}$ (this is why we said this approach is recursive). Any composite positive integer not exceeding n must have a prime divisor from this set $\{p_1, p_2, \ldots, p_k\}$.

Again, this is a repetitive problem we encountered before. How many positive integers not exceeding n are divisible by p_1? The number is $\lfloor n/p_1 \rfloor$. The same goes for $p_2, \ldots, p_k$. So, the total number of non-prime positive integers should be

$$\left\lfloor \frac{n}{p_1} \right\rfloor + \left\lfloor \frac{n}{p_2} \right\rfloor + \cdots.$$

However, the positive integers that are multiple of both p_1 and p_2 were counted twice in this sum. So, we need to subtract them. Now it becomes

$$\left\lfloor \frac{n}{p_1} \right\rfloor + \left\lfloor \frac{n}{p_2} \right\rfloor + \cdots - \left\lfloor \frac{n}{p_1 p_2} \right\rfloor - \left\lfloor \frac{n}{p_1 p_3} \right\rfloor - \cdots \text{ all possible pairs}$$

Again, when we subtracted them all, the multiples of $p_1p_2p_3$ or $p_3p_4p_k$ all vanished from the calculation. To rectify that mistake, we need to add the number of multiples of three primes (all possible combinations of course). Now it looks like

$$\left\lfloor \frac{n}{p_1} \right\rfloor + \left\lfloor \frac{n}{p_2} \right\rfloor + \cdots - \left\lfloor \frac{n}{p_1 p_2} \right\rfloor - \left\lfloor \frac{n}{p_1 p_3} \right\rfloor - \cdots + \left\lfloor \frac{n}{p_1 p_2 p_3} \right\rfloor + \left\lfloor \frac{n}{p_1 p_3 p_4} \right\rfloor + \cdots$$

Going this way, we see that, if the number of primes taken into account is even, we add it, subtract otherwise. Hence, we get the following theorem[9].

Theorem 4.3.3. *Let n be a positive integer and $p_1, p_2, \ldots, p_k$ be the primes less than or equal to $\sqrt{n}$. If the number of primes not exceeding n is $\pi(n)$, then $\pi(n) - \pi(\sqrt{n}) + 1$ is*

(4.7)
$$n - \left\lfloor \frac{n}{p_1} \right\rfloor - \left\lfloor \frac{n}{p_2} \right\rfloor - \left\lfloor \frac{n}{p_3} \right\rfloor + \cdots + \left\lfloor \frac{n}{p_1 p_2} \right\rfloor + \left\lfloor \frac{n}{p_1 p_3} \right\rfloor + \cdots + (-1)^k \left\lfloor \frac{n}{p_1 p_2 \cdots p_k} \right\rfloor .$$

In other words, and more generally, if $\pi(x)$ for any positive real $x \geq 2$ is the number of primes not exceeding x, then,

$$\pi(x) - \pi(\sqrt{x}) + 1 = \lfloor x \rfloor - \sum_{p_i} \left\lfloor \frac{x}{p_i} \right\rfloor + \sum_{p_i < p_j} \left\lfloor \frac{x}{p_i p_j} \right\rfloor - \sum_{p_i < p_j < p_k} \left\lfloor \frac{x}{p_i p_j p_k} \right\rfloor + \cdots , \tag{4.8}$$

where the sums are taken over all primes less than or equal to $\sqrt{x}$.

Notice that there is a $\pi(\sqrt{n})$ here. Because when we used primes less than or equal to $\sqrt{n}$, we missed all the primes that are below $\sqrt{n}$. So we should subtract the number of primes less than $\sqrt{n}$, which is $\pi(\sqrt{n}) - 1$. Let us discuss this a bit further. We claim that

$$\pi(n) - \pi(\sqrt{n}) + 1 = \sum_{i=1}^{P} \mu(i) \left\lfloor \frac{n}{i} \right\rfloor , \tag{4.9}$$

where $P = p_1 p_2 \cdots p_k$. This is probably not obvious to you, so we explain how the above fomula is obtained[10]. It is now a very good time to mention a point the importance of the Mőbius μ function defined in defintion (3.5.3) as:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \text{ is divisible by } p^2 \text{ for some prime } p, \\ (-1)^k & \text{if } n = p_1 p_2 \cdots p_k. \end{cases}$$

[9] In the final examination of senior year, Masum faced the following question: Provide an approximation formula for the number of primes not exceeding N. He proved theorem (4.3.3) instead as an exact formula in the exam.

[10] Thanks to **Amin Soofiani** for reminding us to add some more explanation here.

We stated in the previous chapter that Mőbius comes handy when dealing with inclusion–exclusion arguments. Here, we have a nice one. We will investigate equation (4.9) term by term. The first term is n, obtained from $i = 1$. For $i = p_j$, the contribution is $\mu(p_j)\lfloor n/p_j \rfloor = -\lfloor n/p_j \rfloor$ (here, $1 \leq j \leq k$). That's exactly the first group of terms in equation (4.7). But what about the case when i is not a prime? Well, if it's a square-free number, i.e., if it is of the form $i = p_{i_1} p_{i_2} \cdots p_{i_s}$, where $\{i_1, i_2, \ldots, i_s\} \subseteq \{1, 2, \ldots, k\}$, then, we get a contribution of

$$\mu(p_{i_1} p_{i_2} \cdots p_{i_s}) \left\lfloor \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_s}} \right\rfloor = (-1)^s \left\lfloor \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_s}} \right\rfloor.$$

Otherwise, if i is not square-free, then $\mu(i) = 0$ and there would be no contribution from that term. Therefore, we get exactly the same sum as in the long (4.7).

While on the topic, we should mention the *Meissel-Lehmer Method*. It is a sieve method based on this theorem, that ultimately provides a way to compute p_n in $O(\sqrt{n})$ complexity i.e. a function that does not grow faster than $\sqrt{n}$. This is a very good improvement for computing $\pi(x)$ and p_n.

Note. The study of finding number of primes has gradually morphed into a new branch called *Sieve theory*. This is an interesting part of analytical number theory but not only it is out of our scope, the authors have yet to study a lot in that area. Regardless, it makes an interesting point for the readers to be interested in. Curious minds should try going deeper in analytic number theory.

4.4 Bertrand's Postulate and A Proof

Bertrand's postulate is a very nice and influential theorem in number theory. *Joseph Bertrand* first conjectured it, but he couldn't prove it entirely. Later, *Chebyshev* proved it, using analytic number theory tools. *S. Ramanujan* proved it (see [3]) using properties of *Gamma function*, which is beyond the scope of this book. However, *Erdős* proved it in an elementary way. We will see that proof here. On another note, this elementary proof given by Erdős (see [4]) was the first paper he published! The proof is so beautiful that we could not keep this theorem along with others, instead we gave it a separate section!

There are many formulations of this theorem. All of them are equivalent.

Theorem 4.4.1 (Bertrand's Postulate). *For all integers $n > 1$, there is a prime p so that $n < p < 2n$.*

Theorem 4.4.2 (Alternative Formulations of Bertrand's Postulate).

- *Let p_n denote the n^{th} prime number, starting from $p_1 = 2$. Then*

$$p_{n+1} < 2p_n.$$

- *For any integer $n > 1$, we have*

$$\pi(n) - \pi\left(\frac{n}{2}\right) \geq 1.$$

We need to show some lemmas in order to prove Bertrand's postulate. At first they all seem to be unrelated. Keep reading back and forth until you see the motivation behind all these lemmas. When you realize, see if you feel thunderstruck. You should! If this does not make you wonder how a human being can think that far, we do not know what will. And then you will probably understand why *Erdős* is our most favorite.

Lemma 4.4.3. *For any positive integer n,*

$$\binom{2n}{n} \geq \frac{4^n}{2n+1}.$$

Proof. From binomial theorem, we already know that

$$(1+1)^{2n} = 1 + \binom{2n}{1} + \cdots + \binom{2n}{n} + \cdots + \binom{2n}{2n}.$$

Since the binomial coefficients exhibit a symmetry , i.e., since $\binom{2n}{k} = \binom{2n}{2n-k}$, all terms in the above sum are smaller than $\binom{2n}{n}$. Therefore

$$2^{2n} \leq (2n+1)\binom{2n}{n},$$

which is what we wanted.

□

In section (3.2.2) of previous chapter, we defined $v_p(n)$ to be the highest power of a prime p which divides n.

Lemma 4.4.4. *Let n be a positive integer and let $2n/3 < p \leq n$ be a prime. Then $p \nmid \binom{2n}{n}$.*

Proof. We have

$$v_p\left(\binom{2n}{n}\right) = v_p\left(\frac{(2n)!}{(n!)^2}\right) = v_p((2n)!) - v_p((n!)^2) = v_p((2n)!) - 2v_p((n!)).$$

Note that $2n/3 < p$ means $2n < 3p$, and so the only multiples of p which appear in $(2n)!$ are p and $2p$. Hence $v_p((2n)!) = 2$. Also, $p < n$ immediately gives $v_p((n!)) = 1$. Therefore

$$v_p\left(\binom{2n}{n}\right) = v_p((2n)!) - 2v_p((n!)) = 2 - 2 \cdot 1 = 0.$$

□

Lemma 4.4.5. *Let n be a positive integer. Let p be any prime divisor of $N = \binom{2n}{n}$. Then $p^{v_p(N)} \leq 2n$.*

Proof. Let α be the positive integer for which $p^\alpha \leq 2n < p^{\alpha+1}$. Then using theorem (3.2.14) of chapter (3),

$$\begin{aligned} v_p(N) = v_p((2n)!) - 2v_p(n!) &= \sum_{i=1}^{\alpha} \left\lfloor \frac{2n}{p^i} \right\rfloor - 2\sum_{i=1}^{\alpha} \left\lfloor \frac{n}{p^i} \right\rfloor \\ &= \sum_{i=1}^{\alpha} \left(\left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor \right) \leq \sum_{i=1}^{\alpha} 1 = \alpha. \end{aligned}$$

The last line is true because for a rational x, $\lfloor 2x \rfloor - 2\lfloor x \rfloor \in \{0, 1\}$. Therefore, $p^{v_p(N)} \leq p^\alpha \leq 2n$. □

Lemma 4.4.6. *Let n be a positive integer. Any prime p with $n + 2 \leq p \leq 2n + 1$ divides $\binom{2n+1}{n}$.*

Proof. Since $p > n + 1$,

$$\nu_p\left(\binom{2n+1}{n}\right) = v_p\left(\frac{(2n+1)!}{(n!)(n+1)!}\right) = v_p((2n+1)!) - v_p(n!) - v_p((n+1)!) = 1.$$

□

Lemma 4.4.7. *For any positive integer n,*

$$\binom{2n+1}{n} \leq 2^{2n}.$$

Proof. From binomial theorem and the fact that $\binom{2n+1}{n} = \binom{2n+1}{n+1}$,

$$\begin{aligned} (1+1)^{2n+1} &= 1 + \binom{2n+1}{1} + \cdots + \binom{2n+1}{n} + \binom{2n+1}{n+1} + \cdots + \binom{2n+1}{2n+1} \\ &\geq \binom{2n+1}{n} + \binom{2n+1}{n+1} = 2\binom{2n+1}{n}. \end{aligned}$$

This finishes the proof. □

The following lemma is really a nice one, and the proof requires a good insight.

Lemma 4.4.8. *The product of all primes less than or equal to n is less than or equal to 4^n.*

Proof. We will use induction. The proof is trivial for $n = 1$ and $n = 2$. Assume it is true for all positive integers up to $n - 1$. We will show that it is also true for n.

If n is even and greater than 2, n is definitely not a prime. Thus,

$$\prod_{p \leq n} p = \prod_{p \leq n-1} p \ \leq 4^{n-1} < 4^n.$$

Now, assume that n is odd. Take $n = 2m + 1$. We have

$$\prod_{p \leq n} p = \prod_{p \leq 2m+1} = \prod_{p \leq m+1} p \ \cdot \prod_{m+2 \leq p \leq 2m+1} p.$$

By induction hypothesis, the first product, $\prod_{p\leq m+1} p$, is less than or equal to 4^{m+1}. From lemma (4.4.6), we know that any prime p such that $m+2 \leq p \leq 2m+1$ divides $\binom{2m+1}{m}$. Therefore, the second product, $\prod_{m+2\leq p\leq 2m+1} p$, is less than or equal to $\binom{2m+1}{m}$. Combining these results with lemma (4.4.7), we get

$$\prod_{p\leq n} p \leq 4^{m+1}\binom{2m+1}{m} \leq 4^{m+1}2^{2m} = 4^{2m+1} = 4^n.$$

Hence, the lemma is also true for n and we are done. □

We are ready to prove Bertrand's postulate.

Proof of Bertrand's postulate. We want to show that for any positive integer n, there exists a prime p such that $n < p \leq 2n$. Assume the converse, i.e., suppose that there exists some n for which there is no prime p with $n < p \leq 2n$. We will find an upper bound for $N = \binom{2n}{n}$ and seek for a contradiction. Let us divide the prime divisors of N into two groups:

- Consider all prime divisors of N, say p, such that $p \leq \sqrt{2n}$. Let $p_1, p_2, \ldots, p_k$ be such primes. Clearly, $k \leq \sqrt{2n}$. According to lemma (4.4.5), $p_i^{v_{p_i}(N)} \leq 2n$ (for $1 \leq i \leq k$). Therefore,

$$\prod_{i=1}^{k} p_i^{v_{p_i}(N)} \leq (2n)^{\sqrt{2n}}.$$

- Consider all prime divisors of N which are larger than $\sqrt{2n}$. Let $q_1, q_2, \ldots, q_m$ be such primes. Again, by lemma (4.4.5), we must have $q_i^{v_{q_i}(N)} \leq 2n$ (where $1 \leq i \leq m$). However, since $q_i > \sqrt{2n}$, we find that $v_{q_i}(N) = 1$ for all i.

  Now, by our hypothesis, there are no primes p such that $n < p \leq 2n$. On the other hand, lemma (4.4.4) says that there are no prime divisors of N such that $2n/3 < p \leq n$. Altogether, we find that $\sqrt{2n} < q_i \leq 2n/3$ for $1 \leq i \leq m$. Hence,

$$\prod_{i=1}^{m} q_i^{v_{q_i}(N)} = \prod_{i=1}^{m} q_i = \prod_{\substack{\sqrt{2n}<p\leq 2n/3 \\ p|N}} p.$$

We now use the fact that $N = \prod_{i=1}^{k} p_i^{v_{p_i}(N)} \cdot \prod_{i=1}^{m} q_i^{v_{q_i}(N)}$, where p_i and q_i are as defined above. According to what we have found,

$$\begin{aligned} N = \prod_{i=1}^{k} p_i^{v_{p_i}(N)} \cdot \prod_{i=1}^{m} q_i^{v_{q_i}(N)} &\leq (2n)^{\sqrt{2n}} \cdot \prod_{\substack{\sqrt{2n}<p\leq 2n/3 \\ p|N}} p \\ &\leq (2n)^{\sqrt{2n}} \cdot \prod_{p\leq 2n/3} p \\ &\leq (2n)^{\sqrt{2n}} \cdot 4^{2n/3}. \end{aligned}$$

Note that we have used lemma (4.4.8) for writing the last line.

Combining this with the result of lemma (4.4.3), we see that

$$\frac{4^n}{2n+1} \leq (2n)^{\sqrt{2n}} \cdot 4^{2n/3}. \tag{4.10}$$

However, this inequality can hold only for small values of n. Actually, one can check that the inequality fails for $n \geq 468$. For $n < 468$, one can check that

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631$$

is a sequence of primes, each term of which is less than twice the term preceding it. Therefore, any interval $\{n+1, n+2, \ldots, 2n\}$ with $n < 468$ contains one of the primes in this sequence.

Hence, we have reached the contradiction we were looking for. This means that there always exist a prime p such that $n < p \leq 2n$ for any positive integer n. The proof is complete. □

Theorem 4.4.9. *For any positive integer n, the set $S = \{1, 2, \ldots, 2n\}$ can be partitioned into n pairs (a_i, b_i) so that $a_i + b_i$ is a prime.*

Before we show the proof, readers are highly encouraged to prove it themselves. This is the kind of theorem that shows how good human thinking can be.

Proof. We will proceed by induction. The theorem is clearly true for $n = 1$ since $1 + 2 = 3$, a prime. Assume that the theorem is true for all $k < n$ and we can split the set $\{1, 2, \ldots, 2k\}$ into pairs with a prime sum. By Bertrand's postulate, there is a prime p with $2n < p < 4n$. Let $p = 2n + m$, where m must be odd since p is odd. Consider the set $\{m, m+1, \ldots, 2n\}$. It has an even number of elements. Also, we can make pairs of $(m, 2n), (m+1, 2n-1), \ldots$ with sum p, which is a prime. Now we only have to prove that the set $\{1, 2, \ldots, m-1\}$ can be paired into elements with a prime sum. This is true by induction hypothesis because $m - 1 < 2n$. The proof is complete. □

Problem 4.4.10. Let $n > 5$ be an integer and let $p_1, p_2, \ldots, p_k$ be all the primes smaller than n. Show that $p_1 + p_2 + \cdots + p_k > n$.

Solution. We first show by induction that $\sum_{i=1}^{k} p_i > p_{k+1}$ for $k \geq 3$. The base case, $k = 3$ is true because $2 + 3 + 5 > 7$. Assume that $\sum_{i=1}^{k} p_i > p_{k+1}$, then by the first alternative form of Bertrand's postulate stated in theorem (4.4.2),

$$\sum_{i=1}^{k+1} p_i = p_{k+1} + \sum_{i=1}^{k} p_i > 2p_{k+1} > p_{k+2},$$

and the induction is complete. Now, since $p_k < n \leq p_{k+1}$, we have

$$\sum_{i=1}^{k} p_i > p_{k+1} \geq n.$$

Problem 4.4.11 (China 2015). Determine all integers k such that there exists infinitely many positive integers n satisfying

$$n+k \nmid \binom{2n}{n}.$$

Solution. We will show that the problem statement holds for all integers $k \neq 1$. Note that for $k = 1$, we have

$$\binom{2n}{n} - \binom{2n}{n+1} = \frac{1}{n+1}\binom{2n}{n},$$

and therefore $n+1 | \binom{2n}{n}$. Assume that $k > 1$. By Bertrand's postulate, there exists an odd prime p such that $k < p < 2k$. Choose $n = (p-k) + p^m$ for any positive integer m. From theorem (3.2.16), we can write

$$\begin{aligned} v_p\left(\binom{2n}{n}\right) &= v_p((2n)!) - 2v_p((n!)) \\ &= \frac{2n - s_p(2n)}{p-1} - 2 \cdot \frac{n - s_p(n)}{p-1} \\ &= \frac{2s_p(n) - s_p(2n)}{p-1}. \end{aligned}$$

Since $2n = 2(p-k) + 2p^m$ and $2(p-k) < p$, it follows that $s_p(2n) = 2(p-k) + 2 = 2s_p(n)$ (try to write the base p representation of n and $2n$ to see why). Consequently, $v_p\left(\binom{2n}{n}\right) = 0$. However, $p \mid n+k$, so we have $n+k \nmid \binom{2n}{n}$ for infinitely many n, as desired.

For negative k, one can choose $n = -k + p^m$ for an odd prime $p > |2k|$ (which exists by Bertrand's postulate) and any positive integer m. In a similar manner as above, one obtains $v_p\left(\binom{2n}{n}\right) = 0$, but $p \mid n+k$. Consequently, $n+k \nmid \binom{2n}{n}$. The proof is complete.

After the theorem was proved, number theorists tried to tighten the interval. Also, a question was raised regarding the general case.

Problem 4.4.12. Let c be a real number. What is the minimum value of c such that, there is always a prime between n and $n + cn$ for positive integers $n > 1$?

Nagura [18] proved the case for $c = 1/5$.

Theorem 4.4.13 (Nagura). *For $x \geq 25$, there is always a prime number between x and $6x/5$.*

The proof uses a property of Gamma function (a function involving gamma function turns out to be a prime counting function). We will not be proving the improvements or generalizations, but they are worth mentioning. The general case of this theorem would be like this:

Problem 4.4.14. Let k be a positive integer. Does there always exist a prime between kn and $(k+1)n$?

Bachraoui [19, Thm 1.3] proved the case $k = 2$. The idea is a variation of Erdős's proof.

Theorem 4.4.15 (Bachraoui). *For a positive integer $n > 1$, there is always a prime in the interval $[2n, 3n]$.*

Andy Loo [20] proved the case for $k = 3$ without using prime number theorem or any deep analytical method.

Theorem 4.4.16 (Loo). *For a positive integer $n \geq 2$, there is always a prime in the interval $(3n, 4n)$.*

Conjecture 4.1 (General Bertrand's Postulate). *For a positive integer $n \geq 2$ and a positive integer $k \leq n$, there always exists a prime p in the interval $[kn, (k+1)n]$.*

If conjecture (4.1) can be proven, we can prove some other conjectures using it. Let us assume that the conjecture is true and it is in fact a theorem. Let us see how we could use it to prove other conjectures. The ideas are due to *Sambasivarao* [21].

Theorem 4.4.17 (Legendre's theorem). *Assuming general Bertrand's postulate is true, there always exists a prime in the interval $[n^2, (n+1)^2]$.*

As we stated before, it has an improvement and we will prove that instead.

Theorem 4.4.18 (Mitra's theorem). *Assume the general Bertrand's postulate. There exists at least two primes in the interval $[n^2, (n+1)^2]$.*

Proof. From theorem (4.1), we know that there exists a prime in the interval $[kn, (k+1)n]$. Set $k = n$ and we get a prime p such that $n^2 \leq p \leq n^2+n$. Again, there is a prime in the interval $[k(n+1), (k+1)(n+1)]$. Let q be a prime such that $k(n+1) \leq q \leq (k+1)(n+1)$ and set $k = n$. Now we have $n^2 \leq p \leq n^2+n$ and $n^2+n \leq q \leq (n+1)^2$. Combining them we have $n^2 \leq p \leq q \leq (n+1)^2$ since $n^2+n \leq (n+1)^2$. There will always be two but not one. The reason is $p = q$ can not occur. That would only be possible if $n^2 + n = p = q$ which is not prime for $n > 1$ (why?). For $n = 1$, we can check manually that $2, 3$ are between 1 and 4. Therefore, the theorem holds true for all n. □

Theorem 4.4.19 (Brocard theorem). *Assume the general Bertrand's postulate. For each $n > 1$, there are at least 4 primes in the interval $[p_n^2, p_{n+1}^2]$.*

Proof. We will keep using theorem (4.1) repeatedly. There are primes q, r, s, t such that

$$\begin{aligned} p_n^2 \leq q \leq p_n(p_n+1), \\ p_n(p_n+1) \leq r \leq (p_n+1)^2, \\ (p_n+1)^2 \leq s \leq (p_n+1)(p_n+2), \\ (p_n+1)(p_n+2) \leq t \leq (p_n+2)(p_n+2). \end{aligned}$$

See the clever usage of the theorem. Now,

$$(p_n+2)^2 \leq p_{n+1}^2$$

because for $n > 1$, $p_{n+1} \geq p_n + 2$. By the same argument as above, no two of q, r, s, t are equal. Therefore, we are done. □

Theorem 4.4.20 (Andrica theorem). *Assume the general Bertrand's postulate holds true. For any positive integer n, $\sqrt{p_{n+1}} - \sqrt{p_n} < 1$.*

Proof. Fix the primes p_n, p_{n+1} and think about the intervals they belong to. Like we did in the proof of Mitra's conjecture, assume that $km \leq p_n \leq (k+1)m$. Obviously, we are looking for *suitable* values of k and m which fulfill our purpose. Consider the following proof. We have

$$\begin{aligned} km \leq p_n \leq (k+1)m, \\ (k+1)m \leq p_{n+1} \leq (k+1)(m+1). \end{aligned}$$

Now, set $k = m$ and we have $k^2 \leq p_n < p_{n+1} \leq (k+1)^2$. Therefore,

$$k \leq \sqrt{p_n} < \sqrt{p_{n+1}} < k+1,$$

which means $\sqrt{p_{n+1}} - \sqrt{p_n} < 1$. Is this proof correct or faulty? We will leave it to the reader. Here is the original proof. Consider the intervals $A = [k(k-1), k^2], B = [k^2, k(k+1)], C = [k(k+1), (k+1)^2]$. We can certainly pick k such that p_n belongs to at least one of A, B or C. So we have three cases here.

i. p_n is in A. Then p_{n+1} is in B (or A possibly)[11]. Whichever it is, we have the conclusion.

ii. p_n is in B. Again, p_{n+1} is either in B or C. Same argument.

iii. p_n is in C. If p_{n+1} is in C too, we are done. Otherwise, p_{n+1} is not in any of A, B, C. However, since p_n, p_{n+1} are consecutive primes and $(k+1)^2 < p_{n+1} < (k+1)(k+2)$, we have $\sqrt{p_{n+1}} - \sqrt{p_n} < 1$. If you are not sure why, take a look at this:

$$\begin{aligned} & k^2 + k + \frac{1}{4} < p_n < p_{n+1} < k^2 + 3k + 2 + \frac{1}{4} \\ \iff & (2k+1)^2 < 4p_n < 4p_{n+1} < (2k+3)^2 \\ \iff & 2k+1 < 2\sqrt{p_n} < 2\sqrt{p_{n+1}} < 2k+3 \\ \iff & 2\sqrt{p_{n+1}} - 2\sqrt{4p_n} < 2 \\ \iff & \sqrt{p_{n+1}} - \sqrt{p_n} < 1. \end{aligned}$$

□

There are still many open questions left regarding prime numbers. We will describe some later. You don't have to necessarily find an answer to them, just try them! You may learn something new by yourself, or even find new theorems. In many cases, mathematicians develop theories this way.

[11] Because A might contain more than one primes.

4.5 Miscellaneous

Theorem 4.5.1. *For any positive integer n, there are n consecutive integers none of which are prime. In other words, there are arbitrarily large gaps in the sequence of primes.*

Proof. Let's just look at the numbers $(n+1)!+2, \ldots, (n+1)!+n+1$. These are $(n+1)-(2)+1 = n$ consecutive integers and none of them are prime since $(n+1)!+i$ is divisible by i for $1 < i < n+2$. □

Theorem 4.5.2. *For any positive integer n, there are n consecutive integers so that none of them are prime powers (not necessarily the power of same prime).*

Proof. We will use *Chinese Remainder Theorem* to proceed. But how do we understand we need CRT here? A basic idea is to show that n consecutive integers have at least two different prime factors. That way, we can guarantee none of them is a prime power. So we need x to be divisible by p_1p_2, $x+1$ to be divisible by p_3p_4 and likewise, $x+(n-1)$ to be divisible by $p_{2n-1}p_{2n}$. In other words, we need a solution to the system of congruences

$$\begin{aligned} x &\equiv \quad 0 \pmod{p_1p_2},\\ x &\equiv -1 \pmod{p_3p_4},\\ &\vdots\\ x &\equiv -(n-1) \pmod{p_{2n-1}p_{2n}}. \end{aligned}$$

If we write shortly, we need $x \equiv -i \pmod{p_{2i-1}p_{2i}}$ for $0 \le i \le n-1$. By CRT, we do have such an x as a solution to those congruences. So, none of n consecutive integers $x, x+1, \ldots, x+(n-1)$ are prime powers and the claim is proved. □

Theorem 4.5.3. *Let a, n, and d be positive integers so that $a, a+d, \ldots, a+(n-1)d$ are all primes. Then any prime p less than n divides d.*

Proof. If $p < n$ and p does not divide d, then $(d,p) = 1$. Therefore, by theorem (2.4.11), d has a unique inverse modulo p, say e. So $de \equiv 1 \pmod{p}$, where $0 < e < p < n$. Let $-ae \equiv i \pmod{p}$. Then

$$-a \equiv -ade \equiv id \pmod{p}.$$

Note that $i < p < n$. Thus $p|a+id$ for some $i < n$. This now gives $p|a+(p-i)d$ and $p|a+(i-p)d$. It is clear that either $0 < p-i < n$ or $0 < i-p < n$. In either case, p divides two terms of the sequence. Since all terms of the sequence are primes, those two terms which are divisible by p must equal p. But this is a contradiction since the sequence is strictly increasing. Hence, p must divide d. □

Remark. The sequence $a, a+d, a+2d, \ldots$ is called an *arithmetic sequence* or *arithmetic progression* (and briefly, AP) with initial term a and common difference d. The n^{th} term of the sequence is $a+(n-1)d$. The above theorem shows that if all terms of an AP with n terms and common difference d are primes, then d is divisible by any prime less than d.

We are going to explain and prove some inequalities about primes. In 1907, Bonse found and proved the following two theorems:

Theorem 4.5.4. *For $n \geq 4$, $p_1 \cdots p_n > p_{n+1}^2$.*

Theorem 4.5.5. *For $n \geq 5$, $p_1 \cdots p_n > p_{n+1}^3$.*

In 1960, Pósa proved a more general form of Bonse's theorems:

Theorem 4.5.6 (Pósa's Inequality on Primes). *For any integer k, there is a constant m so that*

$$p_1 \cdots p_n > p_{n+1}^k$$

for all $n > m$.

We need some lemmas to prove this theorem.

Lemma 4.5.7. *For $n \geq 5$, $p_n > 2n$.*

Proof. We proceed by induction. For $n = 5$, $p_5 = 11 > 2 \times 5$. Assume $p_n > 2n$ is true for some n and now we prove it for $n + 1$. Since $n > 5$, p_n is odd and hence $p_n + 1$ is even, and is not a prime. So

$$p_{n+1} \geq p_n + 2 > 2n + 2 = 2(n + 1).$$

□

Lemma 4.5.8. *For $n \geq 1$, $p_1 \cdots p_n > 2^{n-1} n!$.*

Proof. Check the truth for $n = 1, 2, 3$, and 4. Note that $p_1 p_2 p_3 p_4 = 2 \cdot 3 \cdot 5 \cdot 7 = 210$. From lemma (4.5.7), $p_i > 2i$ for $i \geq 5$. Thus

$$\begin{aligned} \prod_{i=5}^{n} p_i > \prod_{i=5}^{n} 2i &> \frac{\prod_{i=1}^{n} 2i}{\prod_{i=1}^{4} 2i} \\ &= \frac{2^n \cdot n!}{2^4 \cdot 4!} \\ &= 2^{n-7} \cdot \frac{n!}{3}. \end{aligned}$$

Now, we have

$$\begin{aligned} p_1 \cdots p_n &= p_1 p_2 p_3 p_4 \cdot \prod_{i=5}^{n} p_i \\ &> 210 \cdot 2^{n-7} \frac{n!}{3} \\ &= 35 \cdot 2^{n-6} n! \\ &> 32 \cdot 2^{n-6} n! \\ &= 2^{n-1} n!. \end{aligned}$$

□

Lemma 4.5.9. *The sequence* $u_n = \sqrt[n]{\frac{n!}{2}}$, *for* $n = 1, 2, \ldots$, *is strictly increasing.*

Proof. We are done if we can prove $\sqrt[n]{\frac{n!}{2}} < \sqrt[n+1]{\frac{(n+1)!}{2}}$, which is equivalent to

$$\left(\frac{n!}{2}\right)^{n+1} < \left(\frac{(n+1)!}{2}\right)^{n}.$$

Simplifying, we find

$$(n!)^n n! < 2(n!)^n (n+1)^n,$$

or $n! < 2(n+1)^n$, which is evident! □

Lemma 4.5.10. *For all positive integers* n, $p_n \leq 2^n$. *Equality occurs if and only if* $n = 1$, *otherwise* $p_n < 2^n$.

Proof. If $n = 1$, $p_1 = 2 = 2^1$. We know that $p_2 = 3 < 2^2$. Thus we induct on n using the first alternative of Bertrand's postulate stated in theorem (4.4.2). Let's assume that $p_n < 2^n$. Since p is odd, we have $p_{n+1} < 2p_n < 2^{n+1}$. □

We are ready to prove Pósa's theorem.

Proof of Pósa's Theorem. The case $k \leq 0$ is trivially true. So we focus on $k > 0$.

Note that using lemma (4.5.10), we find $p_{n+1}^k < 2^{(n+1)k}$. So we need to show that

$$p_1 \cdots p_n > 2^{(n+1)k}.$$

On the other hand, using lemma (4.5.8), we have $p_1 \cdots p_n > 2^{n-1} n!$, we are done if we can prove that there is a n_0 so that

$$2^{n-1} n! > 2^{(n+1)k}$$

holds for all $n \geq n_0$. We can write this as

$$\frac{n!}{2} > \frac{2^{(n+1)k}}{2^n} = 2^{n(k-1)} \cdot 2^k,$$

and so,

$$\sqrt[n]{\frac{n!}{2}} > 2^{k-1} \cdot 2^{\frac{k}{n}}.$$

Note that 2^{k-1} is a constant and $2^{k/n}$ decreases as n increases. However, by lemma (4.5.9), $\sqrt[n]{\frac{n!}{2}}$ increases when n gets larger. This means that the expression on the left hand side of above inequality is a strictly increasing sequence, however the right hand side sequence is strictly decreasing. It is obvious there is a smallest n_0 so that the left hand side gets bigger than the right hand side for all $n \geq n_0$. The proof is complete. □

Theorem 4.5.11. *The probability of two random positive integers being coprime is* $\frac{6}{\pi^2}$.

Proof. Two positive integers are coprime if they do not share any prime divisor. So we can do just the opposite. We will find out the probability of them not being coprime. Fix a prime p. What is the probability that both a and b are divisible by p? Think on this for a bit.

Let us focus on what a and b leave as remainders when divided by p. There can be p remainders $(0, 1, \ldots, p-1)$. Both for a and b, there are p possibilities. The probability that a leaves remainder 0 when divided by p is $\frac{1}{p}$. Similarly, the probability that b leaves remainder 0 when divided by p is $\frac{1}{p}$ as well. Therefore[12], both a and b leave remainder 0 when divided by p is $\frac{1}{p} \cdot \frac{1}{p}$. Thus, the probability of a and b not being divisible by p is $1 - \frac{1}{p^2}$. Now, this is only for a fixed prime p. Since p can be any prime, the probability should be multiplied for all primes. The probability is

$$\left(1 - \frac{1}{p_1^2}\right) \cdot \left(1 - \frac{1}{p_2^2}\right) \cdots = \prod_{i \geq 1} \left(1 - \frac{1}{p_i^2}\right) = \prod_{i \geq 1} \left(\frac{p_i^2 - 1}{p_i^2}\right) = \prod_{i \geq 1} \frac{1}{\frac{p_i^2}{p_i^2 - 1}}$$
$$= \frac{1}{\prod_{i \geq 1} \left(\frac{p_i^2}{p_i^2 - 1}\right)} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

We used Euler's $\zeta(2)$ theorem (4.2.6). □

4.6 Distribution of Prime Numbers

Distribution of prime numbers is the topic which encouraged number theorist to start a new branch called *Analytic Number Theory*. We have in fact discussed a little bit about distribution of prime numbers already when we proved Bertrand's theorem. Let us focus on it a bit more.

There are 4 primes less than 10, 25 primes less than 100, 168 less than 1000 and so on. And finding a formula for the number of primes less than n has always fascinated mathematicians. Well, Gauss did not exactly provide a formula for the number of primes, but he noticed that the value of $\frac{n}{\ln n}$ and the number primes less than n, $\pi(n)$, gets closer as n tends to infinity. This gave birth to the *Prime Number Theorem or PNT*, conjectured by Gauss. It was unproven for like, 100 years. Then Chebyshev provided a partial proof using his functions (which were later known as, Chebyshev function of type 1 and 2), and that was only the start of analytical number theory. There is a huge underlying significance here. Gauss did not conjecture any exact formula for $\pi(n)$. But since he was unable to provide one, he estimated instead. Analytical number theory does not provide exact formulas like elementary number theory, rather it shows some

[12] We assume you know that, the probability of two independent events is the product of the probability of those events. That is if A and B are independent, then $P(A \cap B) = P(A)P(B)$. And certainly a being divisible by p has nothing to do with b being divisible by p. So they are independent.

estimation, and mathematicians tend to prove the estimates or improve them. This is because, most of the times providing exact formulas for the functions are either very hard or not so pretty. For example, one can find an exact formula for finding the nth prime number, but one will not like it.

We will start with some functions and analyzing their properties. The obvious question is, why do mathematicians define such functions? In this case, why are these functions and their properties important? The reason is simple. If you can not understand primes directly, understand some functions that can characterize them or tell us something about them, some function that we can analyze. At first, they can be intimidating. So, we will try to show examples in order to make sense why these functions have something to do with primes.

4.6.1 Chebyshev Functions

Definition 4.6.1. Let $x > 0$ be a real number. We define *Chebyshev's ϑ-function* as

$$\vartheta(x) = \sum_{p \leq x} \ln p,$$

where the sum extends over all primes p less than or equal to x.

Example. Take $x = 142.61$. The primes less than x are $2, 3, 5, \ldots, 137, 139$. So

$$\vartheta(142.61) = \sum_{p \leq 142} \ln p = \ln 2 + \ln 3 + \cdots + \ln 137 + \ln 139$$

Corollary 4.6.2. *If $p_1, p_2, \ldots, p_k$ are primes less than or equal to x, then*

$$\vartheta(x) = \ln (p_1 p_2 \cdots p_k) .$$

Lemma 4.6.3. *Let k and n be positive integers such that $k < n < 2k + 1$. Then*

$$\binom{n}{k} \geq \prod_{k < p \leq n} p.$$

The sum extends over all primes p between k and n.

Proof. Write $\binom{n}{k}$ as

$$\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(k+2)(k+1)}{(n-k)!}. \tag{4.11}$$

Let $p_1, p_2, \ldots, p_m$ be the primes between $k+1$ and n (including). Since $n \leq 2k+1$ can be represented as $n - k < k + 1$, we have

$$n - k < k + 1 \leq p_i \leq n$$

for $i = 1, 2, \ldots, m$. So $n - k < p_i$, which means that p_i is relatively prime to all positive integers less than or equal to $n - k$. In other words, $(p_i, (n-k)!) = 1$ for all i. The

rest is easy: the numerator of (4.11) can be regarded as the product of $p_1p_2\cdots p_m$ and another integer, say, s. Since $\binom{n}{k}$ is an integer and also $(p_i,(n-k)!)=1$ for all i, we conclude that s must be divisible by $(n-k)!$. Thus,

$$\binom{n}{k}=\frac{p_1p_2\cdots p_m\cdot s}{(n-k)!}=p_1p_2\cdots p_m\cdot\frac{s}{(n-k)!}\geq p_1p_2\cdots p_m=\prod_{k<p\leq n}p,$$

as claimed. □

Proposition 4.6.4. *Let $x>0$ be a real number. Then*

$$\vartheta(x)\leq 2x\ln 2. \tag{4.12}$$

Proof. We induct on $\lfloor x\rfloor$. For our base cases, we note that for $0\leq x<2$, we have $\vartheta(x)=0\leq 2x\ln 2$.

Now suppose that $x\geq 2$. Let $n=\lfloor x\rfloor$ and suppose that the inequality holds for all reals y such that $\lfloor y\rfloor<n$. Note that

$$\begin{aligned}2^x\geq 2^n=(1+1)^n&=\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{\lfloor n/2\rfloor}+\cdots+\binom{n}{n-1}+{}^{\circ}\binom{n}{n}\\&\geq\binom{n}{\lfloor n/2\rfloor}\geq\prod_{\lfloor n/2\rfloor<p\leq n}p,\end{aligned}$$

where we have used lemma (4.6.3) to write the last line. Taking logarithms from the above inequality, we find

$$\begin{aligned}x\ln 2&\geq\sum_{\lfloor n/2\rfloor<p\leq n}\ln p\\&=\vartheta(x)-\vartheta(\lfloor n/2\rfloor)\\&\geq\vartheta(x)-2\lfloor n/2\rfloor\ln 2\\&\geq\vartheta(x)-x\ln 2,\end{aligned}$$

by the inductive hypothesis. Therefore

$$2x\ln 2\geq\vartheta(x),$$

as desired. □

Definition 4.6.5. Let $x>0$ be a real number. We define *Chebyshev's ψ-function* as

$$\psi(x)=\sum_{p^a\leq x}\ln p,$$

where p^a ranges over all the powers of primes $p_1,p_2,\ldots,p_k$ which do not exceed x. In other words, $\ln p$ appears in the sum each time a power of p is less than or equal to x.

Example. Let's find $\psi(10.5)$. The primes which do not exceed 10.5 are $2, 3, 5$, and 7. The powers of these primes which do not exceed 10.5 are $2, 2^2, 2^3, 3, 3^2, 5$, and 7. Therefore

$$\begin{aligned}\psi(10.5) &= \ln 2 + \ln 2 + \ln 2 + \ln 3 + \ln 3 + \ln 5 + \ln 7 \\ &= \ln(2^3 \times 3^2 \times 5 \times 7) \\ &= \ln(2520) \\ &\approx 7.83.\end{aligned}$$

Corollary 4.6.6. *Let $p_1, p_2, \ldots, p_k$ be primes not exceeding a positive real number x. Also, assume that $p_1^{a_1}, p_2^{a_2}, \ldots, p_k^{a_k}$ are the largest powers of these primes which do not exceed x. Then*

$$\psi(x) = \ln\left(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}\right).$$

Corollary 4.6.7. *Let x be a positive real number. Then*

$$\psi(x) = \operatorname{lcm}([1, 2, \ldots, \lfloor x \rfloor]).$$

Proof. Let $p_1, p_2, \ldots, p_k$ be primes which do not exceed x. Let $p_1^{a_1}, p_2^{a_2}, \ldots, p_k^{a_k}$ be the largest powers of these primes which do not exceed x. Each number in the set $A = \{1, 2, \ldots, \lfloor x \rfloor\}$ is of the form $p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$, where b_i is an integer and $0 \leq b_i \leq a_i$ (for $i = 1, 2, \ldots, k$). It is easy to check (see proposition (1.2.9)) that the least common multiple of all such integers is $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. The previous corollary proves the claim now. □

Proposition 4.6.8. *For any real $x > 0$, we have*

$$\psi(x) = \sum_{p \leq x} \left\lfloor \frac{\ln x}{\ln p} \right\rfloor \ln p.$$

Proof. Let p be a prime not exceeding x. We just need to show that the power of p appearing in $\psi(x)$ equals $\lfloor \ln x / \ln p \rfloor$. This is rather obvious. Let a be the power of p we are searching for. Then $p^a \leq x < p^{a+1}$. Taking logarithms and dividing by $\ln p$, we find the desired result. □

Chebyshev attempted to prove the Prime Number Theorem, and he succeeded in proving a slightly weaker version of the theorem. In fact, he proved that if the limit $\pi(x)\ln(x)/x$ as x goes to infinity exists at all, then it is equal to one. He showed that this ratio is bounded above and below by two explicitly given constants near 1, for all sufficiently large x. Although Chebyshev was unable to prove PNT completely, his estimates for $\pi(x), \vartheta(x)$, and $\psi(x)$ were strong enough to prove Bertrand's postulate at his time. We will state these estimations but hesitate to provide the proofs as they need some calculus background.

Theorem 4.6.9 (Chebyshev Estimates). *If the following limits exist, they are all equal to* 1.

$$\lim_{x\to\infty} \frac{\vartheta(x)}{x}, \quad \lim_{x\to\infty} \frac{\psi(x)}{x}, \quad \textit{and} \quad \lim_{x\to\infty} \frac{\pi(x)\ln(x)}{x}. \tag{4.13}$$

The inequalities in the next theorem show that $n/\ln(n)$ is the correct order of magnitude for $\pi(n)$. In fact, these inequalities are pretty weak and better inequalities can be obtained with greater effort but the following theorem is of our interest because of its elementary proof.

Theorem 4.6.10. *For all integers $m \geq 2$,*

$$\frac{1}{6}\frac{m}{\ln m} < \pi(m) < 4\frac{m}{\ln m}. \tag{4.14}$$

Proof. Let's prove the leftmost inequality first. Assume that $n \geq 1$ is an intger. One can easily show by induction that

$$2^n \leq \binom{2n}{n} < 4^n. \tag{4.15}$$

Using the fact that $\binom{2n}{n} = (2n)!/(n!)^2$, we can take logarithms from (4.15) to obtain

$$n\ln 2 \leq \ln(2n)! - 2\ln n! < n\ln 4. \tag{4.16}$$

We must now find a way to compute $\ln(2n)!$ and $\ln n!$. Let k be a positive integer. By theorem (3.2.14), we have

$$v_p(k!) = \sum_{i=1}^{\alpha} \left\lfloor \frac{k}{p^i} \right\rfloor, \tag{4.17}$$

where α is some positive integer. Here, we need to find α. See proof of theorem (3.2.14) to realize that $\alpha+1$ is actually the number of digits of k in base p. On the other hand, we know that the number of digits of a positive integer x in base y is $\lfloor \log_y x \rfloor + 1$ (prove this as an exercise). So, in our case, $\alpha + 1 = \lfloor \log_p k \rfloor + 1$, or simply $\alpha = \lfloor \log_p k \rfloor$. Since we are working with natural logarithms (i.e., logarithms in base e), it would be better to write $a = \lfloor \frac{\ln k}{\ln p} \rfloor$. Finally, substituting n and $2n$ for k in equation (4.17), we get

$$v_p(n!) = \sum_{i=1}^{\lfloor \frac{\ln n}{\ln p} \rfloor} \left\lfloor \frac{n}{p^i} \right\rfloor, \quad v_p\left((2n)!\right) = \sum_{i=1}^{\lfloor \frac{\ln 2n}{\ln p} \rfloor} \left\lfloor \frac{2n}{p^i} \right\rfloor.$$

It is clear that $n! = \prod_{p \leq n} p^{v_p(n!)}$, where the product is extended over all primes p less than or equal to n. After taking logarithms in the latter equation, the product turns into a sum:

$$\ln n! = \sum_{p \leq n} v_p(n!)\ln p = \sum_{p \leq n} \sum_{i=1}^{\lfloor \frac{\ln n}{\ln p} \rfloor} \left\lfloor \frac{n}{p^i} \right\rfloor \ln p.$$

Similarly,

$$\ln(2n)! = \sum_{p \leq n} v_p\left((2n)!\right)\ln p = \sum_{p \leq 2n} \sum_{i=1}^{\lfloor \frac{\ln 2n}{\ln p} \rfloor} \left\lfloor \frac{2n}{p^i} \right\rfloor \ln p.$$

Hence, the left hand side of inequality (4.16) becomes

$$\begin{aligned} n\ln 2 \le \ln(2n)! - 2\ln n! &= \sum_{p\le 2n}\sum_{i=1}^{\lfloor \frac{\ln 2n}{\ln p}\rfloor} \left\lfloor \frac{2n}{p^i}\right\rfloor \ln p - 2\sum_{p\le n}\sum_{i=1}^{\lfloor \frac{\ln n}{\ln p}\rfloor} \left\lfloor \frac{n}{p^i}\right\rfloor \ln p \\ &= \sum_{p\le 2n}\sum_{i=1}^{\lfloor \frac{\ln 2n}{\ln p}\rfloor} \left\lfloor \frac{2n}{p^i}\right\rfloor \ln p - \sum_{p\le 2n}\sum_{i=1}^{\lfloor \frac{\ln 2n}{\ln p}\rfloor} 2\left\lfloor \frac{n}{p^i}\right\rfloor \ln p \\ &= \sum_{p\le 2n}\sum_{i=1}^{\lfloor \frac{\ln 2n}{\ln p}\rfloor} \left(\left\lfloor \frac{2n}{p^i}\right\rfloor - 2\left\lfloor \frac{n}{p^i}\right\rfloor \right) \ln p. \end{aligned} \tag{4.18}$$

Since for all rationals x, $\lfloor 2x\rfloor - 2\lfloor x\rfloor$ is either 0 or 1, we can write

$$\begin{aligned} n\ln 2 &\le \sum_{p\le 2n}\left(\sum_{i=1}^{\lfloor \frac{\ln 2n}{\ln p}\rfloor} 1\right) \ln p \\ &\le \sum_{p\le 2n} \ln 2n \\ &= \pi(2n)\ln 2n. \end{aligned}$$

The proof is almost finished. Note that $\ln 2 \approx 0.6931 > 1/2$ and therefore

$$\pi(2n) \ge \frac{n\ln 2}{\ln 2n} > \frac{1}{2}\frac{n}{\ln 2n} = \frac{1}{4}\frac{2n}{\ln 2n} > \frac{1}{6}\frac{2n}{\ln 2n}.$$

So the left side inequality of (4.14) is proved for even positive integers $m = 2n$. We now prove it for $m = 2n+1$. Since $2n/(2n+1) \ge 2/3$, we get

$$\pi(2n+1) \ge \pi(2n) > \frac{1}{4}\frac{2n}{\ln 2n} > \frac{1}{4}\frac{2n}{2n+1}\frac{2n+1}{\ln(2n+1)} \ge \frac{1}{6}\frac{2n+1}{\ln(2n+1)},$$

and this proves the left hand inequality of (4.14) for all $m \ge 2$.

We will now prove the other inequality of (4.14). We shall make use of proposition (4.6.4). Let α be an arbitrary real number such that $0 < \alpha < 1$. Then $n > n^\alpha$ and so $\pi(n) \ge \pi(n^\alpha)$. Using equation (4.12), one can write

$$\begin{aligned} \Big(\pi(n) - \pi(n^\alpha)\Big)\ln n^\alpha &= \Big(\sum_{p\le n} 1 - \sum_{p\le n^\alpha} 1\Big)\ln n^\alpha \\ &= \sum_{n^\alpha \le p\le n} \ln n^\alpha \\ &\le \sum_{n^\alpha \le p\le n} p \\ &\le \vartheta(n) \\ &< 2n\ln 2. \end{aligned}$$

This already means that

$$\begin{aligned}\pi(n) &< \frac{2n\ln 2}{\alpha \ln n} + \pi(n^\alpha) \\ &< \frac{2n\ln 2}{\alpha \ln n} + n^\alpha \\ &= \frac{n}{\ln n}\Big(\frac{2\ln 2}{\alpha} + \frac{\ln n}{n^{1-\alpha}}\Big).\end{aligned}$$

We use a bit calculus to finish the proof. Let $f(x) = \frac{\ln x}{x^{1-\alpha}}$. You can easily calculate the derivative $f'(x)$ of f and find that it equals zero for $x = e^{1/1-\alpha}$. Putting this value into f, you will see that $\frac{\ln n}{n^{1-\alpha}} \leq 1/e(1-\alpha)$. Since α is an arbitrary number, choosing $\alpha = 2/3$ helps us finish the proof:

$$\pi(n) < \frac{n}{\ln n}\Big(3\ln 2 + \frac{3}{e}\Big) < 4\frac{n}{\ln n}.$$

□

Here is an interesting problem which combines several concepts. This problem appeared in Theorem 137 of [24], and we are going to provide an elegant solution by Professor Peyman Nasehpour [25].

Problem 4.6.11. Let r be a real number whose decimal representation is

$$r = 0.r_0r_1 \ldots r_n \ldots = 0.011010100010 \ldots,$$

where $r_n = 1$ if when n is prime and $r_n = 0$ otherwise. Show that r is irrational.

Solution. We will prove a more general statement: such a number r in any base $b > 1$ is irrational. First, we define the *average of digits of* r *in base* b, denoted by $\mathrm{Av}_b(r)$, as

$$\mathrm{Av}_b(r) = \lim_{n\to\infty} \frac{r_1 + r_2 + \cdots + r_n}{n}.$$

It is clear that $\mathrm{Av}_b(r)$ is well-defined if the above limit exists. It is a good exercise for you to prove that if $\mathrm{Av}_b(r) = 0$, then r is irrational. The latter result is true because if r is rational, $\mathrm{Av}_b(r)$ exists and is positive. If you have doubts about it, see [25]). Now, with the definition of r and by Prime Number Theorem,

$$\mathrm{Av}_b(r) = \lim_{n\to\infty} \frac{\pi(n)}{n} = \lim_{n\to\infty} \frac{n/\log n}{n} = \lim_{n\to\infty} \frac{1}{\log n} = 0,$$

and so r is irrational!

Theorem 4.6.12 (Euler). *The sum* $S = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \ldots = \sum_{p\in\mathbb{P}} \frac{1}{p}$ *diverges i.e. does not have a finite summation.*

The proof is due to Dustin J. Mixon, which appeared at American Mathematical Monthly[23].

Proof. Let p_i be the ith prime number and the sum does not diverge. Then there must be a k such that

$$\sum_{i=k+1}^{\infty} \frac{1}{p_i} < 1$$

We let A be the set of positive integers which has all prime factors less than or equal to p_k, and B be the set of positive integers with all prime factors greater than or equal to p_{k+1}. From the fundamental theorem of arithmetic, each positive integer can be uniquely expressed as a product ab where $a \in A$ and $b \in B$. We have

$$\begin{aligned}\sum_{a\in A} \frac{1}{a} &= \sum_{x_1=0}^{\infty} \cdots \sum_{x_k=0}^{\infty} \frac{1}{p_1^{x_1} \cdots p_k^{x_k}} \\ &= \left(\sum_{x_1=0}^{\infty} \frac{1}{p_1^{x_1}}\right) \cdots \sum_{x_k=0}^{\infty} \frac{1}{p_k^{x_k}} \\ &< \infty\end{aligned}$$

Moreover, assume that B_i is the set of positive integers with exactly i distinct prime factors. This yields,

$$\begin{aligned}\sum_{b\in B} \frac{1}{b} &= \sum_{i=0}^{\infty} \sum_{b\in B_i} \frac{1}{b} \\ &\leq \sum_{i=1}^{\infty} \left(\sum_{j=k+1}^{\infty} \frac{1}{p_j}\right)^j < \infty\end{aligned}$$

Since every positive integer greater than 1 belongs to exactly one of A or B, we have

$$\begin{aligned}\frac{1}{2} + \cdots + \frac{1}{n} + \cdots &= \sum_{n=2}^{\infty} \frac{1}{n} \\ &= \sum_{a\in A} \sum_{b\in B} \frac{1}{ab} \\ &= \sum_{a\in A} \frac{1}{a} \sum_{b\in B} \frac{1}{b} \\ &< \infty.\end{aligned}$$

The claim follows from this (how?).

□

4.7 The Selberg Identity

Alte Selberg and *Paul Erdős* together first proved the **Prime Number Theorem** in an elementary way. Selberg found an interesting identity in the process of the proof,

known as the *Selberg Identity*. As we stated before, there was a dispute regarding who proved prime number theorem elementarily. After we read the paper *The elementary proof of the prime number theorem: An historical perspective* [1] by *D. Goldfeld*, we have decided that we trust what Goldfeld said in this paper and conclude that both Erdős and Selberg had contributions in this proof. To be more precise, we believe that Selberg proved *the fundamental identity*[13] but could not proved PNT at the time. Later Erdős proved PNT with the help of fundamental identity, and probably Selberg proved PNT on his own as well (possibly afterwards)[14]. However, as mentioned in paper [1], one must recognize that Erdős could immediately catch the fact that the fundamental identity implies $\lim_{n\to\infty} \frac{p_{n+1}}{p_n} = 1$. This alone demonstrates the magnitude of Erdős's thinking ability. While we are on this point, we would also like to clarify the magnitude of proving PNT elementarily. *G. H. Hardy* said this about PNT in 1921 [2]:

> No elementary proof of the prime number theorem is known, and one may ask whether it is reasonable to expect one. Now we know that the theorem is roughly equivalent to a theorem about an analytic function, the theorem that Riemann's zeta function has no roots on a certain line. A proof of such a theorem, not fundamentally dependent on the theory of functions, seems to me extraordinarily unlikely. It is rash to assert that a mathematical theorem cannot be proved in a particular way; but one thing seems quite clear. We have certain views about the logic of the theory; we think that some theorems, as we say 'lie deep' and others nearer to the surface. If anyone produces an elementary proof of the prime number theorem, he will show that these views are wrong, that the subject does not hang together in the way we have supposed, and that it is time for the books to be cast aside and for the theory to be rewritten.

We need some definitions before stating the Selberg identity. We will use functions defined in chapter (3). The following theorem is almost trivial.

Theorem 4.7.1 (Invariance Theorem). *Let f be an arithmetic function and I be the identity function. Then*

$$f * I = I * f = f.$$

Theorem 4.7.2. *Let f be an arithmetic function and F is its summation function. Then*

$$f = \mu * F.$$

Proof. This is immediately resulted from Mőbius inversion theorem (theorem (3.5.6)). □

[13] The identity we are discussing here can be thought of as a basis of what Selberg calls *the fundamental identity*.

[14] We are not making any assertion here, only expressing our thoughts. One should not draw any conclusion from ours. You can read the papers and think for yourself what you want to decide.

Definition 4.7.3 (Dirichlet Derivative). For an arithmetic function f, we define its *Dirichlet derivative* as

$$f'(n) = f(n) \ln n.$$

Example. $I'(n) = I(n) \ln n = 0$ for all positive integers n. Also, $u'(n) = \ln n$ and $u''(n) = \ln n \cdot \ln n = \ln^2 n$.

We can easily check that some usual properties of differentiation hold true for Dirichlet derivative as well. For instance:

Proposition 4.7.4. *Let f and g be arithmetic functions. Then*[15]

$$(f+g)' = f' + g',$$
$$(f*g)' = f'*g + f*g'.$$

Proof. The first one is obvious. For the second one, we can write

$$\begin{aligned}
(f*g)'(n) &= \left(\sum_{d|n} f(d) g\left(\frac{n}{d}\right)\right) \cdot \ln n \\
&= \left(\sum_{d|n} f(d) g\left(\frac{n}{d}\right)\right) \cdot \left(\ln d + \ln \frac{n}{d}\right) \\
&= \left(\sum_{d|n} f(d) g\left(\frac{n}{d}\right)\right) \cdot \ln d + \left(\sum_{d|n} f(d) g\left(\frac{n}{d}\right)\right) \cdot \ln \frac{n}{d} \\
&= \sum_{d|n} f(d) \cdot \ln d \cdot g\left(\frac{n}{d}\right) + \sum_{d|n} f(d) g\left(\frac{n}{d}\right) \cdot \ln \frac{n}{d} \\
&= \sum_{d|n} f'(d) \cdot g\left(\frac{n}{d}\right) + \sum_{d|n} f(d) g'\left(\frac{n}{d}\right) \\
&= (f'*g)(n) + (f*g')(n).
\end{aligned}$$

□

Definition 4.7.5 (Von Mangoldt Function). For any positive integer n, the von Mangoldt function, denoted by $\Lambda(n)$[16] is defined as

$$\Lambda(n) = \begin{cases} \ln p & \text{if } n = p^m \text{ for some prime } p \text{ and positive integer } m, \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 4.7.6. *Let n be a positive integer. Then $\ln n = \sum_{d|n} \Lambda(d)$.*

[15] You can see it follows some properties of the usual derivative (if you are familiar with calculus, you should know what derivative is. However, for this purpose you do not need any calculus.)

[16] Λ is the upper case of the symbol lambda (λ) in Greek.

Proof. Let $n = \prod_{i=1}^{k} p_i^{e_i}$, where p_i are primes $(1 \leq i \leq k)$. Then,

$$\begin{aligned}\ln n &= \ln\left(\prod_{i=1}^{k} p_i^{e_i}\right) \\ &= \sum_{i=1}^{k} \ln p_i^{e_i} \\ &= \sum_{i=1}^{k} e_i \ln p_i.\end{aligned}$$

On the other hand, if p is a prime, for $d \neq p^m$ we have $\Lambda(d) = 0$ by definition. Therefore, only prime powers p^e contribute a $\ln p$ to the sum $\sum_{d|n} \Lambda(d)$. So, if p_i is a prime divisor of n, $p_i^1, \ldots, p_i^{e_i}$ contribute $e_i \cdot \ln p_i$ to the sum. Thus,

$$\sum_{d|n} \Lambda(d) = \sum_{i=1}^{k} e_i \ln p_i.$$

□

Now we are ready to state and prove the Selberg's identity.

Theorem 4.7.7 (Selberg's Identity). *Let n be a positive integer. Then*

$$\Lambda(n) \ln n + \sum_{d|n} \Lambda(d)\Lambda\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \ln^2 \frac{n}{d}.$$

Proof. We proved in theorem (4.7.6) that $\ln n = \sum_{d|n} \Lambda(d)$. We also found that $u'(n) = \ln n$. This can be written as

$$\Lambda * u = u'.$$

Take derivative of both sides of the above equation to obtain

$$\Lambda' * u + \Lambda * u' = u''.$$

Using $\Lambda * u = u'$ again,

$$\Lambda' * u + \Lambda * (\Lambda * u) = u''.$$

Now multiply both side by $u^{-1} = \mu$ (as proved in theorem (3.5.8)) to get

$$\Lambda' * (u * u^{-1}) + \Lambda * (\Lambda * (u * u^{-1})) = u'' * u'.$$

Now, since $u * u^{-1} = I$ and $f * I = f$ for any arithmetic function f, we have

$$\Lambda' + \Lambda * \Lambda = u'' * \mu.$$

Replacing the functions with their definitions, one easily finds

$$\Lambda(n) \log n + \sum_{d|n} \Lambda(d)\Lambda\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \log^2 \frac{n}{d},$$

as desired. □

4.8 Primality Testing

Depending on the guarantee whether our algorithm can say for sure if a number is a prime or not, we can divide the algorithms for prime testing in two:

1. Deterministic Primality Test
2. Non-deterministic or Probabilistic or Randomized Primality Test

First we will discuss some deterministic approach, then some probabilistic approach.

The first one is based on a theorem we have already established in chapter (1).

Theorem 4.8.1 (Trial Division until $\sqrt{n}$). *If n is a composite number, it has at least one prime factor q with $q \leq \sqrt{n}$.*

This is the simplest way to check whether a positive integer n is a prime. That is, given n, you check weather any prime $2 \leq p \leq \sqrt{n}$ divides n. If n is not divisible by any such p, it is a prime. We take this opportunity to introduce a notion of **runtime**, which will roughly mean the number of operations someone or a computer will have to do in order to determine whether n is prime or not using a particular algorithm. In this algorithm, you can see that we are dividing n by primes less than $\sqrt{n}$ and so, if the number of such primes is k then we could say, runtime is $R(k)$. Here, assume that $R(k)$ denotes the runtime of the whole operation, though it is not rigorous at all. But it will do for our purpose very nicely. Let's look at the following theorem now.

Theorem 4.8.2 (Lucas Test). *Let $n > 1$ be a positive integer. Then n is a prime if and only if there is an integer $1 < a < n$ for which*

$$a^{n-1} \equiv 1 \pmod{n},$$

and for every prime factor p of $n-1$,

$$a^{(n-1)/p} \not\equiv 1 \pmod{n}.$$

Proof. We will show the if part first. If n is a prime, then by theorem (2.12.19), it has a primitive root. That is, there exists some integer a such that $a^{\varphi(n)} = a^{n-1} \equiv 1 \pmod{n}$ and $a^d \not\equiv 1 \pmod{n}$ for all $d < n$.

On the other hand, assume that given conditions hold for a positive integer n. The first condition asserts that $(a, n) = 1$. Let d be the order of a modulo n. That is, d is the smallest positive integer less than n such that $a^d \equiv 1 \pmod{n}$. By theorem (2.12.2), $d|n-1$. This means that $dx = n - 1$ for some x. Choose a prime q which divides x so that $x = qy$ for some integer y. Therefore, $n - 1 = dqy$ or $(n-1)/q = dy$. But then

$$a^{(n-1)/q} \equiv a^{dy} \equiv \left(a^d\right)^y \equiv 1 \pmod{n},$$

which is in contradiction with the second condition since q is a prime such that $q|x|n-1$. Thus the order of a modulo n is $n - 1$. So $\varphi(n) = n - 1$ which implies that n is a prime. □

The next theorem is taken from [11].

Theorem 4.8.3 (Pocklington's Theorem). *Let $n > 1$ be an integer and suppose that there exist an integer a and a prime q such that the following conditions hold:*

1. $q|n-1$ *and* $q > \sqrt{n}-1$,
2. $a^{n-1} \equiv 1 \pmod{n}$, *and*
3. $\left(a^{\frac{n-1}{q}} - 1, n\right) = 1$.

Then n is a prime.

Proof. Assume n is not prime. Then n has a prime divisor p such that $p \leq \sqrt{n}$. By first condition, $q > p-1$ and so $(q, p-1) = 1$. We can deduce by theorem (2.4.11) that there exists an integer x such that $qx \equiv 1 \pmod{p-1}$. This means that $qx - 1 = (p-1)k$ or $qx = (p-1)k + 1$ for some k. Since $p|n$, the second condition gives $a^{n-1} \equiv 1 \pmod{p}$ and so

$$\begin{aligned}
1 &\equiv a^{n-1} \\
&\equiv \left(a^{n-1}\right)^{x} \\
&\equiv \left(a^{(n-1)/q}\right)^{qx} \\
&\equiv \left(a^{(n-1)/q}\right)^{(p-1)k+1} \\
&\equiv \underbrace{\left(\left(a^{(n-1)/q}\right)^{k}\right)^{p-1}}_{\equiv 1} \cdot \left(a^{(n-1)/q}\right) \\
&\equiv a^{(n-1)/q} \pmod{p}.
\end{aligned}$$

This gives $p|a^{(n-1)/q} - 1$. Combining the latter result with $p|n$, we have

$$p \Big| \left(a^{\frac{n-1}{q}} - 1, n\right) = 1,$$

a contradiction. Hence n is prime. □

Note. Depending on the implementation of a result, a deterministic test can be converted into a non-deterministic one. For example, the above theorem can be both deterministic and probabilistic. Because you can iterate over all possible a modulo a. Or you could use some random a that are coprime to n. For a randomized test, we would check only for some random $a \perp n$ because $a^{n-1} \equiv 1 \pmod{n}$ must hold. If the result was in favor for all a, we would say, n is a *probable prime*. Otherwise, n is a *definite composite*.

In 1977, *Robert Martin Solovay* and *Volker Strassen* developed a method called *Solovay–Strassen primality testing* which is based on Euler's criterion.

Definition 4.8.4. Let $n > 1$ be an odd integer. Assume that $a > 1$ is a positive integer such that $(a, n) = 1$ and

$$a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) \pmod{n},$$

where $\left(\frac{a}{n}\right)$ is the Jacobi symbol defined in (2.8.19). Then a is called an *Euler witness for compositeness of* n, or simply an *Euler witness for* n.

Theorem 4.8.5 (Solovay–Strassen Primality Test). *Let $n > 1$ be an odd integer. Then n is composite if it has an Euler witness.*

Proof. By Euler's criterion, we know that if n is a prime, then for every integer a coprime to n,

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}. \tag{4.19}$$

So, if for some a coprime to n, the above congruence equation does not hold, n cannot be a prime. Thus it is composite. □

Remark. We discussed different classes of pseudoprimes, integers which share a common property with all primes but are composite, in section (2.14). If equation (4.19) holds true for a composite integer n and an integer $a > 1$ coprime to it, then n is called an Euler pseudoprime to base a, abbreviated as epsp(a). The Solovay–Strassen test is closely related to Euler pseudoprimes. In fact, if an odd integer n is composite and an integer a such that $1 < a < n$ and $(a, n) = 1$ is not an Euler witness for n, then n is an epsp(a). On the other hand, if an odd n is an epsp(a) for some a, then a is not an Euler witness for n.

As explained in that section, a well-known class of pseudoprimes are strong pseudoprimes. *Gary Lee Miller* developed *Miller's primality test* which involves the congruences used in the definition of strong pseudoprimes. *Michael Oser Rabin* later modified Miller's primality test and obtained *Miller–Rabin* test which we will now explain. To formulate Miller-Rabin primality test, it would be convenient to use the terminology introduced by Rabin as below:

Definition 4.8.6. Let $n = 2^s d + 1$ where s and d are positive integers and d is odd. Let $a > 1$ be an integer coprime to n. Then a is said to be a *witness for compositeness of* n, or simply a witness for n when

$$\begin{aligned} a^d &\not\equiv \quad 1 \pmod{n}, \text{ and} \\ a^{2^r d} &\not\equiv -1 \pmod{n}, \text{ for every integer } 0 \le r < s. \end{aligned}$$

Theorem 4.8.7 (Miller–Rabin Primality Test). *Let $n > 1$ be an odd integer. Then n is composite if it has a witness.*

Proof. Assume that n has a witness a. Then by definition $(a, n) = 1$ and

$$\begin{aligned} a^d &\not\equiv 1 \pmod{n}, \\ a^d &\not\equiv -1 \pmod{n}, \\ a^{2d} &\not\equiv -1 \pmod{n}, \\ a^{4d} &\not\equiv -1 \pmod{n}, \\ &\vdots \\ a^{2^{s-1}d} &\not\equiv -1 \pmod{n}. \end{aligned}$$

It follows that the following product is not divisible by n:

$$\left(a^d - 1\right)\left(a^d + 1\right)\left(a^{2d} + 1\right) \cdots \left(a^{2^{s-1}d} + 1\right) = a^{2^s d} - 1.$$

But $a^{2^s d} - 1 = a^{n-1} - 1$ and so $n \nmid a^{n-1} - 1$. We know by Fermat's little theorem that if p is a prime, then $p | a^{p-1} - 1$ for any a such that $(a, p) = 1$. So, n cannot be a prime and is therefore a composite number. □

Note. If an odd integer n is composite and an integer a such that $1 < a < n$ and $(a, n) = 1$ is not a witness for n, then n is a spsp(a). On the other hand, if an odd n is a spsp(a) for some a, then a is not a witness.

The most well known deterministic algorithm known for primality testing is *AKS* primality test. It was introduced by *Manindra Agrawal, Neeraj Kayal, and Nitin Saxena* in 2002. The core idea of AKS primality test is the following theorem.

Theorem 4.8.8. *Let a be an integer and n be a positive integer such that $(a, n) = 1$. Then n is prime if and only if*

$$(x + a)^n \equiv x^n + a \pmod{n},$$

for all integers x.

Proof. Let $P(x) = (x + a)^n - (x^n + a)$. Then

$$\begin{aligned} P(x) &= (x + a)^n - (x^n + a) \\ &= \sum_{i=0}^{n} \binom{n}{i} x^i a^{n-i} - (x^n + a) \\ &= \sum_{i=1}^{n-1} \binom{n}{i} x^i a^{n-i} - (a - a^n). \end{aligned}$$

If n is prime, then n divides $\binom{n}{i}$ for all $0 < i < n$ by theorem (1.4.29) and also $a^n \equiv a \pmod{n}$ by Fermat's little theorem. So $P(x) \equiv 0 \pmod{n}$ and the condition holds.

If n is composite, take a prime divisor p of n. Let v be the greatest power of p that divides n. That is, $p^v | n$ but $p^{v+1} \nmid n$. Then q^i does not divide $\binom{n}{i}$ (why?) and therefore n does not divide the term $\binom{n}{p} x^q a^{n-p}$ in $P(x)$. This means that $P(x) \not\equiv 0 \pmod{n}$ and the proof is complete. □

As you can see, the runtime of deterministic primality tests are not that great. Even the best of them, AKS test has a runtime around $(\log_2 n)^{12}$, which was later reduced to $(\log_2 n)^6$ by mathematicians such as *C. Pomerance*. But it still is not very good for running as a program. This runtime means, if $n = 2^{100}$, we would have to do around $100^6 = 10^{12}$ operations, which is really costly. If we assume the best case scenario, an average computer may perform 10^9 operations per second (in fact it is far less effectively when it's down to computing because there are many related calculations as well), so it would require around 1000 seconds to test primality of a number of that magnitude. But in practice, numbers around 1024 bits are used which are as large as $2^{1023} - 1$. This makes this test obsolete. In turn, this gives rise to *probabilistic primality test*. In a probabilistic test, one can not guarantee that the input n is definitely a prime. But it can say if it is a *probable prime* or not. And if we use a good enough algorithm the probability of having a false prime is really small, of the magnitude 2^{-k} where k is some iteration number or something else depending on the algorithm. But if k is around 100, you can see how small this gets. This means the chances of getting a false result is really really slim. Let's first use Fermat's little theorem as a probabilistic test. We already know that for a prime and a positive integer x, we must have $x^{p-1} \equiv 1 \pmod{p}$. Using this, we can make the test for input n this way.

i. Choose a random number x.

ii. Compute r as $x^{n-1} \equiv r \pmod{n}$ (this needs to be done efficiently since n is large).

iii. If $r \neq 1$ then n is surely composite.

iv. Otherwise n is probably a prime. Probably, because the reverse of Fermat's little theorem is not true, as we discussed on chapter (2) before.

But this doesn't make a very reliable test. To make it a bit more reliable, we can iterate this process for k times. And each time we have to choose another random x. The more we iterate, the more the accuracy is.

The most popular and used method for probabilistic testing is *Rabin-Miller* primality test. This makes clever use of Fermat's little theorem.

4.8.1 Primality Testing for Famous Classes of Primes

We have explained theorems which help us find out whether a number is prime. For numbers having special forms, we can develop much better methods to test their primality. The first special type of numbers where $2^k + 1$ for an integer $k \geq 0$.

Definition 4.8.9. Let $n \geq 0$ be an integer. The numbers of the form $F_n = 2^{2^n} + 1$ are called *Fermat numbers*. If F_n is prime for some n, it is called a *Fermat prime*.

Proposition 4.8.10. *If $2^k + 1$ is prime for an integer $k \geq 0$, then it is a Fermat prime.*

Proof. This is a special case of theorem (1.4.23). □

Fermat conjectured that all Fermat numbers are actually primes. He computed F_n for $n = 0, 1, 2, 3$, and 4 and found out they are all primes. However, he was unable to show that F_5 is prime. Euler later showed that for $n \geq 2$, every factor of F_n should be of the form $m \cdot 2^{n+2} + 1$ and thus found 641 to be a divisor of F_5 and factorized it as

$$F_5 = 641 \cdot 6700417.$$

Since F_n increases too rapidly with n, it is too difficult to check its primality. In 1877, Pepin developed a test for checking the primality of Fermat numbers:

Theorem 4.8.11 (Pepin's Primality Test for Fermat Numbers). *Let $n \geq 2$ be an integer and assume F_n denotes the n^{th} Fermat number. Also, let $k \geq 2$ be any integer. Then the following conditions are equivalent:*

1. *F_n is prime and $\left(\frac{k}{F_n}\right) = -1$.*
2. *$k^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.*

Proof. Assume that condition 1 holds. Then by Euler's criterion (theorem (2.8.7)),

$$k^{(F_n-1)/2} \equiv \left(\frac{k}{F_n}\right) \equiv -1 \pmod{F_n}.$$

To prove the other side of the theorem, assume that $k^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Choose an integer m such that $1 \leq m < F_n$ and $m \equiv k \pmod{F_n}$. Then

$$m^{(F_n-1)/2} \equiv k^{(F_n-1)/2} \equiv -1 \pmod{F_n}.$$

Note that the only prime divisor of $F_n - 1 = 2^{2^n}$ is 2. Hence we can use Lucas test (with $a = m$ and $p = 2$, using notation of theorem (4.8.2)) and deduce that F_n is a prime. Furthermore, we have by Euler's criterion that

$$\left(\frac{k}{F_n}\right) \equiv k^{(F_n-1)/2} \equiv -1 \pmod{F_n}.$$

The proof is complete. □

Pepin's test is usually done with $k = 3, 5$, or 10. In practice, mathematicians have not been able to show that any Fermat number F_n for $n > 4$ is a prime using Pepin's test. On the other hand, nobody has yet proved that all Fermat numbers larger than F_4 are composite.

Another type of numbers are Mersenne numbers, named after Marin Mersenne who studies them back in 17^{th} century.

Definition 4.8.12. Let n be an integer. The numbers of the form $M_n = 2^n - 1$ are called *Mersenne numbers*. If M_n is prime for some n, it is called a *Mersenne prime*.

Proposition 4.8.13. *If M_n is a prime for an integer $n > 1$, then n is a prime.*

Proof. See theorem (1.4.22). □

Mersenne stated that

$$M_2, M_3, M_5, M_7, M_{13}, M_{17}, M_{19}, M_{31}, M_{67}, M_{127}, M_{257}$$

are the only Mersenne primes less than M_{258}. Although he was wrong about M_{67}[17] and

[17] $M_{67} = 193707721 \times 761838257287$.

M_{257}[18] and he missed M_{61}, M_{89}, and M_{107} in the list, his work is considered astonishing because these numbers are astronomically large. Interested readers may study [14] and [15] for more details about Mersenne primes.

Theorem 4.8.14. *Let $q > 2$ be a prime. For every divisor n of M_q, we have*

$$\begin{aligned} n &\equiv \pm 1 \pmod 8, \text{ and} \\ n &\equiv 1 \pmod q. \end{aligned}$$

Proof. It suffices to prove the theorem for prime n (why?). Let p be a prime divisor of $M_q = 2^q - 1$. Then $2^q \equiv 1 \pmod p$ and so $\text{ord}_p(2)|q$, which means that $\text{ord}_p(2) = q$ since q is a prime. By corollary (2.12.3), $q = \text{ord}_p(2)|\varphi(p) = p-1$. Thus $p \equiv 1 \pmod q$. Since p and q are both odd, we can write the latter relation as $p - 1 = 2kq$. By Euler's criterion,

$$\begin{aligned} \left(\frac{2}{p}\right) &\equiv 2^{(p-1)/2} \\ &\equiv 2^{kq} \\ &\equiv (2^q)^k \\ &\equiv 1 \pmod p. \end{aligned}$$

Theorem (2.8.15) now verifies that $p \equiv \pm 1 \pmod 8$. □

The above theorem can be used to factorize Mersenne numbers. It will be tough to use this theorem for large Mersenne number though. To realize whether a Mersenne number is prime or composite, one may use the so-called Lucas–Lehmer primality test, introduced by *Édouard Lucas* in 1856 and improved by *Derrick Henry Lehmer* later in 1930s. The proof is a bit difficult and we refuse to write it. The reader may see [16] for a proof if interested.

Theorem 4.8.15 (Lucas–Lehmer Primality Test for Mersenne Numbers). *Define the recursive sequence $S(n)$ by $S(1) = 4$ and $S(n+1) = S(n)^2 - 2$ for any integer $n \geq 1$. Also, let $p > 2$ be a prime. Then M_p is prime if and only if it divides $S(p-1)$.*

Example. We will apply Lucas–Lehmer test to factorize $M_{11} = 2^{11} - 1 = 2047$. We must check whether $S(10)$ is divisible by 2047. Table 4.1 shows values of $S(n)$ for $n = 1, 2, \ldots, 10$. As seen in the table, $S(10)$ is not zero modulo 2047 which means that M_{11} is not a prime. In fact, $2047 = 23 \cdot 89$.

As the last class of primes, we will mention Proth numbers.

Definition 4.8.16. Let k and h be positive integers such that k is odd and $k < 2^h$. A number of the form $n = k \cdot 2^h + 1$ is called *Proth number* and if it is a prime, it is said to be a *Proth prime*.

The following primality test for Proth numbers was published by François Proth around 1878 and is known as Proth's theorem.

[18] Lehmer and Kraïtchik showed that M_{257} is composite.

n	$S(n) \pmod{2047}$
1	4
2	14
3	194
4	788
5	701
6	119
7	1877
8	240
9	282
10	1736

Table 4.1: Applying Lucas–Lehmer test to test the primality of 2047.

Theorem 4.8.17 (Proth's Primality Test for Proth Numbers). *Let n be a Proth number. Then n is prime if an integer a for which*

$$a^{(n-1)/2} \equiv -1 \pmod{n}.$$

We will prove a stronger result in the following lemma which was proposed by Pocklington.

Lemma 4.8.18. *Let a, b and n be positive integers such that $0 < a \leq b+1$ and $n = ab+1$. Assume that for every prime divisor p of b there exists an integer x for which*

$$\begin{aligned} x^{n-1} &\equiv 1 \pmod{n}, \text{ and} \\ x^{(n-1)/p} &\not\equiv 1 \pmod{n}. \end{aligned}$$

Then n is prime.

Proof. Assume on the contrary that n is composite and take the smallest prime factor q of n. Theorem (4.8.1) implies that $q \leq \sqrt{n}$. Let p be a prime factor of b. Write $b = p^k s$, where $k \geq 1$ and s are positive integer such that $(s, p) = 1$. Let x be an integer which satisfies the given conditions. Then

$$x^{n-1} \equiv 1 \pmod{q}, \text{ and} \tag{4.20}$$

$$x^{(n-1)/p} \not\equiv 1 \pmod{q}. \tag{4.21}$$

because $q|n$. We claim that $\text{ord}_q(x^a) = b$. To prove the claim, we notice that

$$\begin{aligned} (x^a)^b &= x^{ab} \\ &= x^{n-1} \\ &\equiv 1 \pmod{q}. \end{aligned}$$

We must now show that $(x^a)^m \not\equiv 1 \pmod{q}$ for any integer $0 < m < b$. Assume on the contrary that there exists a positive integer $m < b$ such that $x^{ma} \equiv 1 \pmod{q}$. If

$d = \text{ord}_q(x)$, then $d|ma$. On the other hand, the congruence relation (4.20) shows that $d|n-1 = p^k sa$. This implies $d|(ma, p^k sa)$. Suppose that $m = p^l t$. Then

$$\begin{aligned}\left(ma, p^k sa\right) &= \left(p^l ta, p^k sa\right)\\ &= a\left(p^l t, p^k s\right)\\ &= ap^{\min(l,k)}(t, s).\end{aligned}$$

(We have used propositions (1.2.2) and (1.2.9) in writing second and third lines.) Now, the congruence equation (4.21) implies that $d \nmid \frac{n-1}{p} = p^{k-1}as$, which is in contradiction with $d|ap^{\min(l,k)}(t, s)$. We have thus shown that $\text{ord}_q(x^a) = b$. It follows that $b \leq \varphi(q) = q - 1$ and hence,

$$\begin{aligned}q^2 &\geq (b+1)^2\\ &\geq a(b+1)\\ &= ab + a\\ &\geq n.\end{aligned}$$

Since we first chose q so that $q \leq \sqrt{n}$, all inequalities above must be equalities. In particular, $n = q^2, a = 1$, and $a = b + 1$, which is a contradiction. □

Remark. The Proth's theorem is now a special case of above lemma where $a = k$ and $b = 2^n$. The converse of Poth's theorem is also true if x is a quadratic non-residue modulo n.

4.9 Prime Factorization

Finding prime numbers has been a challenge for mathematicians since very long time ago. Consider the following question:

Question 4.9.1. Given a real number X, find all primes less than X.

The very first answer to this question dates back to 200 B.C., when *Eratosthenes* developed the *Sieve* method. This method is very simple but it is still used, after 2000 years of its birth! To apply sieve method of finding primes to an integer n, we write down all the positive integers less than or equal to n. Put aside 1. The first number in the list is 2, which we know is a prime. We start by erasing the multiples of 2 from the list. Let's simulate the process for $X = 40$:

	2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~
31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~

Now, choose the first number after 2 in the list. It is 3, a prime. Erase all multiples of 3 from the list and choose the next number. The point is that the next number we choose is always a prime because it is not divisible by any integer less than it in the list (otherwise it would have been erased). We continue this method until we find the largest prime less than or equal to n. The final list for $n = 40$ would look like this:

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~

The remaining numbers are primes less than or equal to n. In fact, we have *sieved* all the primes in the list, hence the name sieve method. The sieve method is not time efficient specially when n is large (can you find the reason?).

An algorithm for Sieve method of prime factorization

1. Generate the sieve up to $m = \sqrt{n}$.
2. Assume that, the primes generated from the sieve are $p_1, \cdots, p_k$.
3. For a prime p_i where $1 \leq i \leq k$, as long as $p_i | n$, set $n' \longleftarrow \dfrac{n'}{p_i}$. The number of times you could divide n by p_i is the exponent of p_i in n.
4. When $i = k$, stop and check if $n > 1$.
5. If $n' > 1$ then this n' itself is a prime factor of the original n (which we used for factoring at the first step, and it will be decreasing since we keep dividing by a prime if n is composite). And in this case, the exponent will be 1 (why?).

The last statement needs a bit clarification. In the steps before that, we divided n by all prime factors of n less than or equal to m. Therefore, if all prime factors of n are less than or equal to m, the n we will have after all these divisions is 1, since it is all divided up by $p \leq m$. But if $n' > 1$ then we have this $n' > m$, so n can not have two such n'. Because the product of two integer greater than m is greater than m^2, so greater than $m^2 = n$. That would be impossible. Therefore, for the case $n' > 1$, n' must be a prime and it would be the largest prime factor of n. And if $n' = 1$ then the largest $i \leq k$ for which $p_i | n$, p_i would be the largest prime factor of n.

4.9.1 Fermat's Method of Factorization

Fermat found a method for factorizing odd numbers. The idea behind his method is very simple. Suppose that we want to factorize an integer $n > 1$. If we find positive integers a and b such that

$$n = a^2 - b^2,$$

and $a - b > 1$, then $n = (a - b)(a + b)$ is a proper factorization of n. Remember that a proper factorization is one in which neither of the factors are trivial (1 or n).

We already know a factorization for even integers $n = 2m$ because 2 is a factor of n in that case. Given an odd positive integer n, we try some value of a, hoping that $a^2 - n$ is a perfect square. If this condition holds, we have found a factorization

Step	1	2	3	4	5	6	7	8
a	60	61	62	63	64	65	66	67
x	11	132	255	380	507	636	767	900
$\sqrt{x}$	3.31	11.48	15.96	19.49	22.51	25.21	27.69	30

Table 4.2: Applying Fermat's method of factorization to 3589.

for n. Otherwise, increment a and check again. The point here is that if an odd n is composite, i.e. if $n = cd$ for some odd positive integers c and d, then

$$n = \left(\frac{c+d}{2}\right)^2 - \left(\frac{c-d}{2}\right)^2.$$

This means that Fermat's method of factorization always works when n is composite. Fermat's factorization is generally more time efficient than trial division. However, it might be even slower than trial division in some cases.

An algorithm for Fermat's method of factorization

1. Choose $a = \lceil n \rceil$, and put $x = a^2 - n$.
2. While x is not a perfect square, set $a \longleftarrow a + 1$ and compute $x = a^2 - n$ for the new a.
3. If x is a perfect square, $n = (a - \sqrt{x})(a + \sqrt{x})$ is a factorization for x.

Example. We will use Fermat's method of factorization to factorize $n = 3589$. Table 4.2 shows the steps of the algorithm. We have started from $a = \lceil \sqrt{3589} \rceil = 60$ and increase a by 1 at each step. When $a = 67$, we find $x = 900$, which is a perfect square. The algorithm stops here and we have

$$\begin{aligned} n &= (a - \sqrt{x})(a + \sqrt{x}) \\ &= (67 - 30)(67 + 30) \\ &= 37 \cdot 67, \end{aligned}$$

which is a non-trivial factorization.

4.9.2 Pollard's Rho Factorization

As already mentioned, prime factorization by sieve method is not time efficient. In fact, most deterministic factorization methods are not. Therefore, we again use probabilistic method. There are two crucial steps for probabilistic factorization methods.

- Finding a non-trivial factor of n (that is, a factor other than 1 and n).
- Using a time efficient primality test in order to check if the non-trivial factor d is prime or not. If d is prime, we can just factorize $\frac{n}{d}$ only. Otherwise, we can repeat the same process for d and $\frac{n}{d}$. Mostly Rabin-Miller test is used widely these days.

Randomized tests vary mainly on the first step. Finding the non-trivial factor is the crucial step here. Here we discuss Pollard's method to find such a factor.

Let $n > 1$ be the composite integer which we want to factorize. Consider the following sequence:

$$\begin{aligned} x_0 &= c, \text{ and} \\ x_{i+1} &\equiv g(x_i) \pmod{n} \text{ for } i = 0, 1, 2, \ldots \end{aligned}$$

Here, $g(x)$ is a polynomial with integer coefficients. Notice that this sequence will eventually become periodic. That is, there exists a positive integer T such that $x_i \equiv x_{i+T} \pmod{n}$ for all $i \geq i_0 \geq 0$, where i_0 is some integer. The reason is that there are exactly n residues modulo n and the sequence is infinite, so by pigeonhole principle, there are two terms x_i and x_j (with $j > i$) of the sequence for which $x_i \equiv x_j \pmod{n}$. Suppose that $g(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where $a_0, a_1, \ldots, a_n$ are integers. Then

$$\begin{aligned} x_{i+1} &\equiv g(x_i) \\ &= a_n x_i^n + a_{n-1}x_i^{n-1} + \cdots + a_1 x_i + a_0 \\ &\equiv a_n x_j^n + a_{n-1}x_j^{n-1} + \cdots + a_1 x_j + a_0 \\ &= g(x_j) \\ &\equiv x_{j+1} \pmod{n}. \end{aligned}$$

therefore $x_{i+k} \equiv x_{j+k} \pmod{n}$ for any k. Thus $T = j - i$ is the period of the sequence. It is clear now that $T \leq n$.

The only thing that needs clarification is how to choose $g(x)$ and x_0. It has been practically shown that taking $g(x) = x^2 + a$ (for some integer a) is a good choice for finding a non-trivial factor quickly. In 1975, John Pollard developed *Pollard's rho method of factorization* which takes $g(x) = x^2 - 1$ and $x_0 = 2$. [19]

Here is how Pollard's rho method of factorization work: assume that $n = st$, where s and t are unknown factors of n such that $t > s > 1$. Suppose that we have found integers $j > i \geq 0$ such that $x_i \equiv x_j \pmod{s}$ but $x_i \not\equiv x_j \pmod{n}$. Since s divides both n and $x_i - x_j$, it must also divide $(x_i - x_j, n)$. So $(x_i - x_j, n) \geq s > 1$. On the other hand, $(x_i - x_j, n)$ is a factor of n and since it is larger than 1, it is a proper factor of n (it is not equal to 1 or n). This means that we have found $(x_i - x_j, n)$ to be a factor of n.

So the problem now reduces to find indices $j > i \geq 0$ such that $x_i \equiv x_j \pmod{s}$ but $x_i \not\equiv x_j \pmod{n}$. Pollard suggested that we take $i = k$ and $j = 2k$ for $k = 1, 2, \ldots, n$. You will see why in the following lines.

When we first discussed the periodicity of the sequence, we showed that the sequence is periodic modulo n. However, one can show using Chinese Remainder Theorem that the sequence is also periodic modulo s (why?). Assume that the sequence will be periodic modulo s after x_{i_0} with period T. Select an index $k \geq i_0$ such that $T|k$. Then obviously $T|2k$ and because of the periodicity, $x_k \equiv x_{2k} \pmod{s}$. But now how do we know that $x_k \not\equiv x_{2k} \pmod{n}$. We don't know that for sure. There is just a

[19] Mathematicians later found out that $g(x) = x^2 + 1$ work better for almost all the cases.

likelihood that it will happen. The reason for this is that the sequence $\{x_i \pmod s\}_{i=0}^{\infty}$ is periodic modulo T, and as proved above, we have $T \leq s$. Similarly, the sequence $\{x_i \pmod n\}_{i=0}^{\infty}$ is periodic with a period $T' \leq n$. Now, since s is a divisor of n, we have $s \leq n$ so that the maximum value of period of the first sequence is smaller than that of the second sequence. Because of this, it is likely that $T < T'$. If this latter condition holds and we have $x_k \equiv x_{2k} \pmod s$, then we can deduce that $x_k \not\equiv x_{2k} \pmod n$, which is what we were searching for.

You might ask now what happens if the given condition, $T < T'$, does **not** hold? Well, in that case, you cannot factorize n using Pollard's method. In such cases, it is usual to change the polynomial $g(x)$ or the initial value x_0 and then apply the method.

To summarize, in Pollard's rho factorization method, starting with $i = 1$, we check if $\gcd(x_{2i} - x_i, n)$ is a factor of n. If it is, we have found a factor for n. If not, increment i and repeat the process. It is possible that we do not find any factor for n (even if n is composite) and the process does not terminate in such cases, as explained above.

An algorithm for Pollard's Rho method of prime factorization

1. Set $x_0 = 2$ and form the sequence $x_{i+1} \equiv x_i^2 - 1 \pmod n$ for $i = 0, 1, 2, \ldots, n$.
2. Compute $d_k = (x_i - x_{2i}, n)$ for $i = 1, 2, \ldots, n$. If $d_i \neq 1$ and n, stop. Now d_i is a factor of n.
3. If d_i is either 1 or n for all k, the algorithm does not work.

Example. Let us factorize $n = 391$ using Pollard's Rho algorithm. The process is shown in table 4.3. In 10^{th} step, where $(|x_{2i} - x_i|, 391)$ is 23, we find that 23 is a factor of n (and indeed it is: $391 = 23 \times 17$). We just stopped the algorithm after that step because we have factorized 391. However, we have written the value of x_i for 11th step so that you can observe the periodicity of x_i modulo 391. As illustrated in the table, $x_7 \equiv x_{11} \equiv 46 \pmod{391}$. Now, if you look at the computed values of x_k modulo 23, you will see that for $j \geq 7$, $x_j \equiv x_{j+2} \pmod{23}$. In terms of our previous definitions, $T = 2, i_0 = 7$, and $k = 10$. Observe that we cannot choose $k = 8$ because then $x_{2k} - x_k$ is zero, which is divisible by both 23 and 391. Therefore we choose $k = 10$ so that $x_k - x_{2k} \equiv 0 \pmod{23}$ but $x_k - x_{2k} \equiv 69 \not\equiv 0 \pmod{391}$.

The next example, taken from Patrick Stein's website (see [13]), takes a different polynomial $g(x)$ and initial value x_0 in Pollard's rho method.

Example. We will factorize a much larger integer $n = 16843009$. This time, we take $g(x) = 1024x^2 + 32767$ and $x_0 = 1$. Table 4.4 shows the steps. As you see in the table, at 9^{th} step we find 257 to be a factor of n and the factorization is done:

$$16843009 = 257 \cdot 65537.$$

65537 is a prime number and it equals $2^{2^4} + 1$. Primes of the form $2^{2^n} + 1$ are called *Fermat primes*, and the largest known such prime is 65537.

i	x_i	$\lvert x_{2i} - x_i \rvert \pmod{391}$	$(\lvert x_{2i} - x_i \rvert, 391)$
1	3	5	1
2	8	50	1
3	63	30	1
4	58	102	1
5	235	6	1
6	93	67	1
7	**46**	160	1
8	160	0	0
9	184	45	1
10	229	69	**23**
11	**46**	Whatever	Whatever

Table 4.3: Applying Pollard's rho method to factorize 391.

i	x_i	$\lvert x_{2i} - x_i \rvert \pmod{16843009}$	$(\lvert x_{2i} - x_i \rvert, 16843009)$
1	33791	10798549	1
2	10832340	6592485	1
3	12473782	508279	1
4	4239855	893857	1
5	309274	5203404	1
6	11965503	7424857	1
7	15903688	1657047	1
8	3345998	15737239	1
9	2476108	15298182	257

Table 4.4: Applying Pollard's rho method to factorize 16843009.

4.10 Exercises

Problem 4.10.1. Let $n \geq 1$ be an integer. Show that $\psi(2n) > n \ln 2$.

Hint. Use proposition (4.6.8) and the fact that

$$\binom{2n}{n} \leq \prod_{p \leq 2n} p^{\lfloor \ln 2n / \ln p \rfloor}.$$

Problem 4.10.2. Find a formula for the number of square-free numbers less than x for a real number x. Recall that, a natural number n is square-free if n does not have any factor that is perfect square other than 1. Can you represent this formula using *Mőbius function* as well?

Problem 4.10.3. Show that $8081, 31627$, and 65537 are all primes.

Hint. Take $a = 2$ or 3 and use Pocklington's theorem.

Problem 4.10.4.

1. Let m, n, and k be non-negative integers such that $m > 1$. Prove that at least one of the numbers

$$\binom{n}{k}, \binom{n+1}{k}, \ldots, \binom{n+k}{k}$$

is not divisible by m.

2. Let k and m be positive integers such that $m > 1$. Show that there are infinitely many positive integers n such that

$$\binom{n}{k}, \binom{n+1}{k}, \ldots, \binom{n+k-1}{k}$$

are all divisible by m.

Hint. Use Kummer's theorem to construct the solution.

Problem 4.10.5. Let k and n be positive integers such that $0 < k \leq n$ and let p be a prime such that $p \nmid n+1$. Prove that if $p \not| \binom{n}{k}$, then $p \not| \binom{n+1}{k}$.

Problem 4.10.6. Let m and n be positive integers. Suppose that the binary representation of m and n is

$$m = 2^k m_k + 2^{k-1} m_{k-1} + \cdots + 2m_1 + m_0, \text{and}$$
$$n = 2^k n_k + 2^{k-1} n_{k-1} + \cdots + 2n_1 + n_0.$$

Show that if $\binom{m}{n}$ is odd, then

$$\binom{m}{n} \equiv \prod_{i=1}^{k} (-1)^{n_{i-1} m_i + n_i m_{i-1}} \pmod 4.$$

4.11 Open Questions In Primes

Conjecture 4.2 (Twin Prime Conjecture). *There exists infinitely many primes p so that $p+2$ is a prime too.*

Conjecture 4.3 (Goldbach's Conjecture). *For all even number n greater than 4, n is a sum of two primes.*

Conjecture 4.4 (Legendre's conjecture). *There exists a prime between n^2 and $(n+1)^2$.*

Adway Mitra conjectured an improvement over this, which is known as the improved version of Legendre's conjecture.

Conjecture 4.5. *There always exists at least two primes in the interval $[n^2, (n+1)^2]$.*

Another variation was proposed by *Oppermann*.

Conjecture 4.6 (Oppermann's Conjecture). *For all integer $x > 1$, there exists at least one prime between $x(x-1)$ and x^2 and another prime between x^2 and $x(x+1)$.*

An improved version was conjectured by Brocard.

Conjecture 4.7 (Brocard's conjecture). *There exists at least 4 primes between p_n^2 and p_{n+1}^2 where p_n is the nth prime number.*

Andrica's inequality is worthy of mentioning while we are on the subject.

Conjecture 4.8 (Andrica's Inequality). *For all $n \geq 1$,*

$$\sqrt{p_{n+1}} - \sqrt{p_n} < 1.$$

Conjecture 4.9 (n^2+1 Problem). *Does there exist infinitely primes of the form n^2+1?*

Conjecture 4.10 (Polignac Conjecture). *For every even integer $2n$ are there infinitely many pairs of consecutive primes which differ by $2n$.*

Conjecture 4.11 (Sophie Germain Primes). *A prime is called a Sophie Germain prime if $2p+1$ is a prime too. Does there exist infinitely many Sophie Germain primes?*

Conjecture 4.12 (Mersenne Prime Problem). *Is the number of Mersenne primes infinite?*

Conjecture 4.13 (Rassias Conjecture). *For a prime $p > 2$, there exists two primes p_1, p_2 such that,*

$$p = \frac{p_1 + p_2 + 1}{p_1}.$$

Bibliography

[1] D. Goldfeld, *The Elementary Proof of the Prime Number Theorem: An Historical Perspective*, Number Theory (New York Seminar) (Springer, 2004), pp. 179˘192.

[2] H. Bohr, *Address of Professor Harold Bohr*, Proc. Internat. Congr. Math. (Cambridge, 1950) vol 1, Amer. Math. Soc., Providence, R.I., 1952, 127˘134.

[3] Srinavasa Ramanujan, (1919). *A proof of Bertrand's postulate*. Journal of the Indian Mathematical Society 11 : 181˘182.

[4] Paul Erdős, Beweis eines Satzes von Tschebyschef, Acta Sci. Math. (Szeged) 5 (1930˘1932), 194˘198.

[5] Nils A. Baas and Christian F. Skau., *The Lord of Numbers: Alte Selberg On His Life and Mathematics*, Bulletin of The American Mathematical Society, Volume 45, Number 4, October 2008, Pages 617˘649.

[6] A. E. Ingham, *On the difference between consecutive primes*, Quart. J. Math. Oxford Ser. vol. 8(1937) pp. 255 – 266.

[7] W. H. Mills, *A prime-representing function*, Bull. Amer. Math. Soc. vol. 53(1947) p. 604.

[8] I. Niven, *Functions Which Represent Prime Numbers*, Amer. Math. Soc., November 1950.

[9] Lawrence E. Greenfield, Stephen J. Greenfield, *Some Problems of Combinatorial Number Theory Related to Bertrand's Postulate*, Journal of Integer Sequences, Vol. 1 (1998), Article 98.1.2.

[10] Apostol T. M., *Introduction to Analytic Number Theory*, 2nd Ed, Springer, 1976.

[11] Koblitz N., *A Course in Number Theory and Cryptography*, 2nd Ed, Springer, 1994.

[12] J. C. Lagarias, V. S. Miller, and A. M. Odlyzko, *Computing $\pi(x)$: The Meissel-Lehmer method*, Math. Comp. 44(1985), 537 – 560. MR 86h : 11111

[13] Stein P., *Pollard's Rho Method*, Stein Patrick's personal website at http://www.csh.rit.edu/~pat/math/quickies/rho/.

[14] Archibald C. R., *Mersenne's Numbers*, The Prime Pages at https://primes.utm.edu/mersenne/LukeMirror/lit/lit_008s.htm.

[15] Ribenboim P., *The Little Book of Bigger Primes*, Springer Science & Business Media, 2004.

[16] Bruce J. W., *A Really Trivial Proof of the Lucas-Lehmer Primality Test*, The American Mathematical Monthly 100.4 (1993), pp. 370-371.

[17] Srinivasha Ramanujan, *A proof of Bertrand's postulate*, Journal of the Indian Mathematical Society, XI, 1919, $181-182$.

[18] Jitusoru Nagura, *On the interval containing at least one prime number*, Proc. Japan Acad. Volume 28, Number 4 (1952), $177-181$.

[19] M. El Bachraoui, *Primes in the Interval* $[2n, 3n]$, Int. J. Contemp. Math. Sci., Vol. 1, 2006, no. 13, $617-621$.

[20] Andy Loo, *Primes in the Interval* $[3n, 4n]$, Int. J. Contemp. Math. Sciences, Vol. 6, 2011, no. 38, $1871-1882$.

[21] S. Sambasivarao, *Primes in the Interval* $[kn, (k+1)n]$.

[22] Andreescu, Titu, and Dorin Andrica. Number Theory: Structures, Examples, and Problems. Springer Science & Business Media, 2009.

[23] Dustin G. Mixon, *Another Simple Proof that the Sum of the Reciprocals of the Primes Diverges*, The American Mathematical Monthly Vol. 120, No. 11, p. 831.

[24] Hardy, Godfrey Harold, and Edward Maitland Wright. An introduction to the theory of numbers. Oxford university press, 1979.

[25] Nasehpour, Peyman. "A Simple Criterion for Irrationality of Some Real Numbers." arXiv preprint arXiv:1806.07560 (2018).

Chapter 5

Special Topics

Contents

> `When you have a hammer in your hand, it's hard refraining yourself from treating everything as a nail.`

The objective of this chapter is to provide with some very powerful tools and some special topics, which are incredibly helpful. Some topics may not be very useful for solving problems, but they are quite good for making someone think and thus they encourage us to study more on them. Let's start with a really nice lemma.

5.1 Thue's Lemma

Thue's Lemma is a wonderful theorem in modular arithmetic. It should have been quite popular, but unfortunately, it is not as well-known as it should be. Here we will see what a powerful tool it is.

Theorem 5.1.1 (Thue's Lemma). *Let $n > 1$ be an integer and a be an integer coprime to n. Then, there are integers x and y so that*

$$\begin{aligned} &0 < |x|, |y| \leq \sqrt{n}, \quad \textit{and} \\ &x \equiv ay \pmod{n}. \end{aligned}$$

We call such a solution (x, y) to the above congruence equation a small solution.

Proof. Let $r = \lfloor \sqrt{n} \rfloor$. That means r is the unique integer for which $r^2 \leq n < (r+1)^2$. The number of pairs (x, y) of integers for which $0 \leq x, y \leq r$, is $(r+1)^2$. This number is greater than n. Therefore, by pigeonhole principle, there must be two different pairs (x_1, y_1) and (x_2, y_2) among these $(r+1)^2$ pairs so that

$$\begin{aligned} x_1 - ay_1 &\equiv x_2 - ay_2 \pmod{n} \\ \implies x_1 - x_2 &\equiv a(y_1 - y_2) \pmod{n}. \end{aligned}$$

Let $x = x_1 - x_2$ and $y = y_1 - y_2$, so we get $x \equiv ay \pmod{n}$. We only need to show that x and y are non-zero (it is obvious that $|x|$ and $|y|$ are both less than or equal to $\sqrt{n}$). Certainly, if one of x or y is zero, the other is zero as well. If both x and y are zero, that would mean that two pairs (x_1, y_1) and (x_2, y_2) are actually the same. That is not the case because we first assumed that they are different pairs of integers. Therefore, none of x or y is zero and we are done. □

Note. The condition $0 < x, y < \sqrt{n}$ is important. Because of this condition, we can rule out trivial cases and bound the small solutions as the problems require.

Corollary 5.1.2. *For a prime p and an integer a coprime to p, there exist integers x and y with $0 < |x|, |y| < \sqrt{p}$ such that*

$$a \equiv xy \pmod{p}.$$

This lemma can be generalized even more with the same proof.

Theorem 5.1.3 (Generalization of Thue's Lemma). *Let p be a prime number and let α and β be two real numbers so that $\alpha\beta \geq p$. Then, for an integer x coprime to p, there are integers a and b with $0 < |a| < \alpha$ and $0 < |b| < \beta$ so that*

$$a \equiv xb \pmod{p}.$$

We can also generalize the latter theorem to a two-dimensional theorem.

Theorem 5.1.4 (Two-dimensional Thue's Lemma). *Let $n \geq 2$ be an integer and define $r = \sqrt{n}$. For arbitrary integers a, b, c, and d, there exist integers w, x, y, and z with at least one of y or z non-zero such that*

$$\begin{aligned} 0 \leq |w|, |x|, |y|, |z| &\leq r, \\ w &\equiv ay + bz \pmod{n}, \quad \textit{and} \\ x &\equiv cy + dz \pmod{n}. \end{aligned}$$

Now we demonstrate some applications of the lemma. First, we show an elegant proof of Fermat's $4n + 1$ theorem, restated in theorem (5.1.5).

Theorem 5.1.5 (Fermat's Theorem on Sum of Two Squares). *Any prime of the form $4n + 1$ can be represented as sum of two squares.*

Proof. We already know from theorem (2.8.9) that for $p \equiv 1 \pmod 4$, there is an x so that

$$x^2 \equiv -1 \pmod{p}.$$

From Thue's lemma, for such an x, there are integers a and b with $0 < |a|, |b| < \sqrt{p}$ so that

$$\begin{aligned} a \equiv xb \pmod{p} &\implies a^2 \equiv x^2 b^2 \equiv -b^2 \pmod{p} \\ &\implies a^2 + b^2 \equiv 0 \pmod{p}. \end{aligned}$$

The last congruence means that $p | a^2 + b^2$, so

$$\begin{aligned} p \leq a^2 + b^2, \text{ but} \\ a^2 + b^2 < p + p = 2p. \end{aligned}$$

Therefore, $a^2 + b^2 = p$ must occur. □

Remark. We can prove a stronger result than that of Theorem 5.1.5 using Fibonacci-Brahmagupta Identity (see Identity A.6 in Appendix 5). This identity states that

$$\begin{aligned} (a^2 + nb^2)(c^2 + nd^2) &= (ac - nbd)^2 + n(ad + bc)^2 \\ &= (ac + nbd)^2 + n(ad - bc)^2. \end{aligned}$$

Since we know that the product of any two numbers of the form $4k + 1$ is again of the form $4k+1$ (see the proof of Theorem 1.4.14), the special case when $n = 1$ of the above identity along with Theorem 5.1.5 shows that all numbers which are comprised only of prime divisors of the form $4k + 1$ are representable as the sum of two squares.

In fact, we can use the same technique for generalizing theorem (5.1.5).

Theorem 5.1.6. *Let $n \in \{-1, -2, -3\}$. If n is a quadratic residue modulo a prime p, then there are integers a and b so that $a^2 - nb^2 = p$.*

Proof. We have already proven the case $n = -1$. If n is a quadratic residue modulo p,

$$x^2 \equiv n \pmod{p}$$

has a solution. Fix the integer x and take a and b as in Thue's lemma so that

$$\begin{aligned} a \equiv xb \pmod{p} &\implies a^2 \equiv x^2b^2 \equiv nb^2 \pmod{p} \\ &\implies p|a^2 - nb^2. \end{aligned}$$

1. If $n = -2$, then $p \leq a^2 + 2b^2 < p + 2p = 3p$. This means either $a^2 + 2b^2 = p$ or $a^2 + 2b^2 = 2p$ occurs. If the first equation holds, we are done. If $a^2 + 2b^2 = 2p$, we see that a must be even. Replace $a = 2a'$ in the latter equation to get $p = b^2 + 2a'^2$, as desired.

2. If $n = -3$, we find $p \leq a^2 + 3b^2 < p + 3p = 4p$. If $a^2 + 3b^2 = 2p$, then a and b are both odd or both even. If both are even, then $2p$ is divisible by 4, a contradiction since p is odd. Otherwise, a and b are both odd:

$$\begin{aligned} a^2 + 3b^2 &\equiv 1 + 3 \cdot 1 \pmod{4} \\ \implies 2p &\equiv 0 \pmod{4}. \end{aligned}$$

   This is, again, a contradiction. We are left with the case $a^2 + 3b^2 = 3p$. This shows a is divisible by 3. If we take $a = 3a'$, we easily observe that $p = b^2 + 3a'^2$.

□

Question 5.1.7. Can you prove a similar result to that of the remark after Theorem 5.1.5, but for the above theorem? Try using Fibonacci-Brahmagupta's identity before reading the next corollary.

Corollary 5.1.8. *For a prime p and an integer n with $p \nmid n$ the following two statements are equivalent:*

- *There exist coprime integers x and y so that p divides $x^2 + ny^2$.*
- *$-n$ is a quadratic residue modulo p.*

Proof. First, assume that $p|x^2 + ny^2$. Then, y must be coprime to p. Therefore, y has an inverse modulo p, say a. So, $ay \equiv 1 \pmod{p}$. Then, $a^2y^2 \equiv 1 \pmod{p}$, and

$$\begin{aligned} p|x^2 + ny^2 &\implies p|a^2x^2 + na^2y^2 \\ &\implies p|a^2x^2 + n \\ &\implies (ax)^2 \equiv -n \pmod{p}. \end{aligned}$$

Now, suppose that $-n$ is a quadratic residue modulo p. Let $k^2 \equiv -n \pmod{p}$. Clearly, $(k, p) = 1$, otherwise p will divide n. From Thue's lemma, there are integers x and y such that

$$\begin{aligned} x \equiv ky \pmod{p} &\implies x^2 \equiv k^2y^2 \equiv -ny^2 \pmod{p} \\ &\implies p|x^2 + ny^2. \end{aligned}$$

□

We can use these results to imply the following theorem.

Theorem 5.1.9. *For $D \in \{1, 2, 3\}$, if $n = x^2 + Dy^2$ for some coprime integers x and y, then every divisor d of n is of the same form as n.*

Proof. According to the Fibonacci-Brahmagupta Identity (identity (A.6) in appendix (A)),

$$\begin{aligned}(a^2 + Db^2)(c^2 + Dd^2) &= (ac - Dbd)^2 + D(ad + bc)^2 \\ &= (ac + Dbd)^2 + D(ad - bc)^2.\end{aligned}$$

This means that the product of two numbers of the form $x^2 + Dy^2$ is of the same form. From theorems above, if p is a divisor of $x^2 + Dy^2$, then $p = a^2 + Db^2$ for some integers a and b. The identity clearly says that if $m = a^2 + Db^2$, then any power of m, say, m^k, is of this form again. Let's assume that the prime factorization of n is

$$n = p_1^{e_1} \cdots p_k^{e_k} = \prod_{i=1}^{k} p_i^{e_i}.$$

Then, since d is a factor of n, the factorization of d is

$$d = \prod_{i=1}^{k} p_i^{f_i} \text{ where } 0 \leq f_i \leq e_i.$$

For any $1 \leq i \leq k$, p_i divides $n = x^2 + Dy^2$. Therefore, according to corollary (5.1.8), $-D$ is a quadratic residue modulo p_i. Now, by theorem (5.1.6), each p_i is of the form $x^2 + Dy^2$. From our previous discussion, we find that $p_i^{f_i}$ is of the same form for all i. As a consequence, the product $p_1^{f_1} \cdots p_k^{f_k} = d$ is of the same form and we are done. □

Now we prove another theorem that demonstrates the power of Thue's lemma. We will use a theorems which we proved in section (2.8). For convenience, we state the theorem here again.

Theorem 5.1.10. *-3 is a quadratic residue modulo p if and only if p is of the form $3k + 1$.*

Using this theorem, we will prove the following.

Theorem 5.1.11. *If p is a prime of the form $3k + 1$, there are integers a and b such that $p = a^2 + ab + b^2$.*

Proof. Since p is of the form $3k + 1$, -3 is a quadratic residue of p. Take y to be an odd integer for which $p | y^2 + 3$ or,

$$y^2 \equiv -3 \pmod{p}.$$

Such an y exists since p is odd. Then, the congruence equation $y \equiv 2x+1 \pmod{p}$ has an integer solution for x. For that x, we get

$$\begin{aligned}(2x+1)^2 &\equiv -3 \pmod{p}\\ 4x^2+4x+1 &\equiv -3 \pmod{p}\\ 4(x^2+x+1) &\equiv 0 \pmod{p}\\ x^2+x+1 &\equiv 0 \pmod{p}.\end{aligned}$$

The latter congruence equation holds because p is odd. From Thue's lemma, there are integers a and b with $0 < |a|, |b| < \sqrt{p}$ such that

$$a \equiv xb \pmod{p}.$$

Then,

$$\begin{aligned}a^2+ab+b^2 &\equiv (xb)^2+(xb)\cdot b+b^2\\ &\equiv b^2(x^2+x+1)\\ &\equiv 0 \pmod{p}.\end{aligned}$$

Since $p|a^2+ab+b^2$, we have $p \leq a^2+ab+b^2$. On the other hand,

$$\begin{aligned}p &\leq a^2+ab+b^2\\ &< p+p+p\\ &= 3p.\end{aligned}$$

Consequently, either $a^2+ab+b^2 = p$ or $a^2+ab+b^2 = 2p$ happens. We can easily check that $a^2+ab+b^2 = 2p$ can not happen (try it yourself). Thus, $a^2+ab+b^2 = p$, which is what we wanted. □

You have probably figured out by now that **our focus should be on the small solutions** so that we can bound the necessary expressions like the problem asks for. Let's see more examples on this.

Theorem 5.1.12. *Let $p > 5$ be a prime which divides k^2+5 for some integer k. Show that there are integers x and y such that $p^2 = x^2+5y^2$.*

Hint. Try to find x such that $x^2 \equiv -5 \pmod{p^2}$. Then from Thue's lemma, there exist a and b so that $a^2, b^2 < p$ and $a \equiv kb \pmod{p^2}$. This gives $a^2 \equiv k^2b^2 \equiv -5b^2 \pmod{p^2}$. Now, check all the cases like we did before.

Problem 5.1.13. Let p be a prime for which there exists a positive integer a such that p divides $2a^2-1$. Prove that there exist integers b and c so that $p = 2b^2-c^2$.

Solution. Let's look for small solutions again for the bounding purpose! We have $2a^2-1 \equiv 0 \pmod{p}$. Since we want to bound $2b^2-c^2$, it is obvious that we must find b and c so that p divides $2b^2-c^2$ and then bound it. Fix the integer a, which

is clearly coprime to p. Then from Thue's lemma, we there are integers b and c with $0 < |b|, |c| < \sqrt{p}$ so that

$$b \equiv ac \pmod{p}.$$

This gives us what we need. Note that

$$\begin{aligned} 2b^2 - c^2 &\equiv 2(ac)^2 - c^2 \\ &\equiv c^2(2a^2 - 1) \\ &\equiv 0 \pmod{p}. \end{aligned}$$

Thus, p divides $2b^2 - c^2$, and now we get to use the fact that

$$\begin{aligned} p &\leq 2b^2 - c^2 \\ &< 2b^2 \\ &< 2p. \end{aligned}$$

We immediately get that $p = 2b^2 - c^2$.

5.2 Chicken McNugget Theorem

You are probably wondering how come this can be the name of a theorem if you have encountered it for the first time. The name just might be the weirdest of all names a theorem can possibly assume! Here is the reason behind such a name: The story goes that the Chicken McNugget Theorem got its name because in McDonalds, people bought Chicken McNuggets in 9 and 20 piece packages. Somebody wondered what the largest amount you could never buy was, assuming that you did not eat or take away any McNuggets. They found the answer to be 151 McNuggets, thus creating the Chicken McNugget Theorem. Actually it is *Sylvester's Theorem*, now known as the *Chicken McNugget Theorem*. The problem is known as *Frobenius Coin Problem*, which is a generalization of this one. Have you ever wondered about the coin system of your own country? It is designed in a way so that you should never face a situation where you can not exchange a certain amount of money. But have you thought how it is possible? In this section, we will deal with problems like this. First think for yourself on the following two problems:

Problem 5.2.1. You are in a strange country where only two units are available for exchange: 4 and 6. Can you pay any amount you want?

Problem 5.2.2. In another country, you see that only two units are available for exchange: 3 and 10. Can you pay any amount you want?

If you have come to the right conclusions, you will see that you can not pay any amount you want in the first case. But you can pay whatever you want with the second one. Let's say two units available value a and b. So if you use a unit x times and b unit y times, the total amount of money you can pay is $ax + by$. Here, x, y can be negative

or non-negative integers. If $x > 0$, it will mean you are paying, or if $x < 0$ it will mean you are being paid (or getting the exchange). Therefore, if you need to pay exactly n amount, you need integers x and y with

$$ax + by = n.$$

Play with some more values of a and b. You will understand that you can pay n amount with units a and b if and only (a, b) divides n. Here is another intuitive fact: If we can pay just 1, we can pay any amount we want with as many 1s needed. So we should focus on when we can pay 1 by a and b. This tells us, a and b must be co-prime. And from Bézout's Identity, for any co-prime a and b, we will get integers x, y so that

$$ax + by = 1.$$

In the problems above, we can't pay any amount with 4 and 6 because they are not co-prime. But we can pay any amount that is a multiple of $(4, 6) = 2$. But we can pay any amount with 3 and 10 because they are co-prime. This leads us to the following theorem.

Theorem 5.2.3. *Any integer can be written as a linear combination of a and b if and only if $a \perp b$.*

By linear combination, we mean using only a and b as many times as we want. Now we see the same problem from another perspective. Consider the following problem. If n can be written as $ax+by$ for non-negative x, y, we will call n a *good* number. Otherwise, n is *bad*. But to do that, we can't change the values of a and b simultaneously. Therefore, we fix two co-prime integers a and b. Next, let's see why we are only considering $a \perp b$. If $(a, b) = g$ and $g > 1$, then we already know that only multiples of g can be good. But we want as many integers to be good as possible, and not skipping some integers is better.

Problem 5.2.4. A shop sells nuggets in packages of two sizes, 3 nuggets and 10 nuggets. What is the maximum number of nuggets that cannot be expressed as a nonnegative combination of these package sizes?

Definition 5.2.5 (Frobenius Number). For two integers a and b, the largest bad integer is the *Frobenius number*. In fact, it can be generalized for n natural numbers. If $a_1, \ldots, a_n$ are natural numbers so that $(a_1, \ldots, a_n) = 1$, the largest natural number that can not be written as $a_1x_1 + \ldots a_nx_n$ for nonnegative $x_1, \ldots, x_n$ is the Frobenius number. It is denoted as $F_n(a_1, \ldots, a_n)$. Here, we will deal with the case $n = 2$, $F_2(a, b)$.

The following theorem answers this question.

Theorem 5.2.6 (Sylvester's Theorem, 1882). *Let a and b be two co-prime positive integers greater than 1. Then the maximum integer that can not be expressed as $ax+by$ for non-negative integer x, y is $ab - a - b$.*

If we can prove that for all $N > ab-a-b$, there are non-negative integers x, y such that

$$N = ax + by,$$

and that for $N \leq ab - a - b$, there are no such x and y, we are done. First, let's prove the next lemma.

Lemma 5.2.7. *$ab - a - b$ is a bad number.*

Proof. On the contrary, let's assume that

$$ab - a - b = ax + by,$$

for some $x, y \in \mathbb{N}_0$. We can rewrite it as

$$a(x - b + 1) = -b(y + 1).$$

From this equation, $a|b(y+1)$ but $a \perp b$. So, $a|y+1$. Again, $b|a(x-b+1)$ but $b \perp a$ so $b|x-b+1$ or $b|x+1$. We get,

$$\begin{aligned} & x + 1 \geq b, y + 1 \geq a \\ \implies & x \geq b - 1, y \geq a - 1. \end{aligned}$$

Using these inequalities,

$$\begin{aligned} ax + by &\geq a(b-1) + b(a-1) \\ &= ab - a + ab - b \\ \implies ab - a - b &\geq 2ab - a - b, \end{aligned}$$

which is a contradiction. □

Lemma 5.2.8. *If m and n both are good, then so is $m + n$.*

Proof. If m and n are good, then there are nonnegative integers x, y, u and v so that

$$\begin{aligned} m &= ax + by, \text{ and} \\ n &= au + bv. \end{aligned}$$

Therefore, $m + n = a(x + u) + b(y + v)$ is good. □

Lemma 5.2.9. *If $m + n = ab - a - b$, then exactly one of m and n is good.*

Proof. If both m and n are good, then according to the lemma above, $m + n$ is good too. But that would contradict the fact that $ab - a - b$ is bad. So, one of m or n must be bad. □

So, now we know that, any integer below $ab - a - b$ is bad. All that's left to prove is the following lemma.

Lemma 5.2.10. *Any integer $n > ab - a - b$ is good.*

Proof. Since $(a, b) = 1$, by Bézout's identity, there are integers u and v so that

$$\begin{aligned} au + bv = 1 &\implies anu + bnv = n \\ &\implies ax_0 + by_0 = n. \end{aligned} \tag{5.1}$$

We need to show that such $x_0, y_0 \geq 0$ exist. If (x_0, y_0) is a solution of equation (5.1), then so is $(x_0 - bt, y_0 + at)$ for any integer t. Here, one can choose t such that $0 \leq x_0 - bt < b$.

In case you don't understand how we can choose such t, just divide x_0 by b. Then $x_0 = bq + r$, where $0 \leq r < b$. This means that $0 \leq x_0 - bq < b$, so one choice for t is q. So we know that there exists some x_0 such that $0 \leq x_0 < b$. We will show that y_0 is also positive. Note that

$$\begin{aligned} ax_0 + by_0 = n > ab - a - b \\ \implies b(y_0 + 1) > a(b - x_0 - 1). \end{aligned}$$

Since we know that $x_0 < b$, we get $b - x_0 - 1 \geq 0$. This means that $b(y_0 + 1) > 0$, so $y_0 + 1 > 0$, i.e., $y \geq 0$. Therefore, there is a valid solution (x_0, y_0) and the proof is complete. □

Now, the proof is complete. The same proof can be used for generalizing the case where $(a, b) > 1$.

Theorem 5.2.11 (Generalization of Sylvester's Theorem). *Let a, b be positive integers with $(a, b) = g$. Then every integer*

$$n \geq \frac{(a-g)(b-g)}{g}$$

such that $g|n$ is good. Also,

$$F_2(a, b) = \frac{(a-g)(b-g)}{g} - g,$$

i.e., $F_2(a, b)$ is the largest bad integer.

We see some problems related to this theorem. A classical example would be the following problem that appeared at the IMO 1983.

Problem 5.2.12 (IMO 1983). Let $a, b, c \in \mathbb{N}$ with $(a, b) = (b, c) = (c, a) = 1$. Prove that, $2abc - ab - bc - ca$ is the largest integer that can not be expressed as $xbc + yca + zab$ for nonnegative x, y, z.

Solution. Clearly, we need to invoke Sylvester's theorem here. But the expression tells us, it can not be done in one step. Note that

$$xbc + yca + zab = c(bx + ay) + zab.$$

Therefore, we should first focus only on $bx + ay$ first. As we know from the theorem, for k to be good, $bx + ay \geq ab - a - b + 1 + t$ must hold for some $t \geq 0$. Substitute it into the equation to get

$$\begin{aligned} xbc + yca + zab &= c(bx + ay) + zab \\ &= c(ab - a - b + 1 + t) + zab \\ &= abc - bc - ca + c + ct + zab. \end{aligned}$$

This again calls for using the theorem for c and ab. The minimum integer that can be expressed as $ct + abz$ for nonnegative t and z is $abc - ab - c + 1$. So $ct + zab = abc - ab - c + 1 + w$ for some non-negative w. Then

$$\begin{aligned} xbc + yca + zab &= abc - bc - ca + c + ct + zab \\ &= abc - bc - ca + c + abc - ab - c + 1 + w \\ &= 2abc - ab - bc - ca + 1 + w \\ &> 2abc - ab - bc - ca. \end{aligned}$$

So, the problem is solved. As you can see, the theorem is fairly easy to understand and use in problems. There will be some related problems in the problem column. See if you can get how to solve those using this (first you have to understand that this theorem will come to the rescue though).

5.3 Vietta Jumping

By now, *Vietta jumping* has become a standard technique for solving some particular type of olympiad number theory problems. It is also known as *Root Jumping* or *Root Flipping*. Though it involves Diophantine equations and for now, it is out of our scope, many divisibility or congruence problems can be turned into one that can be solved using this tactic. Hence, this section. To understand just how popular it has been, let's just mention that there are at least two IMO problems that have standard solutions using this particular technique. And surely, there are many other olympiad problems that fall into the same category. Now, let's see what it is and what it actually does.

Consider the following quadratic equation

$$ax^2 + bx + c = 0.$$

According to Vietta's formula, if two of its roots are x_1 and x_2, then

$$\begin{aligned} x_1 + x_2 &= -\frac{b}{a}, \text{ and} \\ x_1 x_2 &= \frac{c}{a}. \end{aligned}$$

Vietta jumping relies on these two equations. It is in fact, a *descent* method in which we usually prefer using one of the following two methods:

(i) **Standard Descent:** It is usually used to show that the equation doesn't have any solution or some sort of contradiction to prove a claim, like we do in *Infinite Descent*. For a solution (x, y) of the equation, we define a function dependent on x, y ($x + y$ is such a common function, as we will see later). Then we consider the solution that minimizes that function over all solutions possible. If there are multiple solutions that can achieve this, we are free to choose any one depending on the problem. But then, using Vietta's formulas, we try to find another solution that makes the function's value smaller, which gives us the necessary contradiction. So, this is a modified version of infinite descent.

(ii) **Constant Descending:** Sometimes, we take some constants, for example, an integer k and fix it for the whole problem. For a solution (a, b), we fix b and k. Then using those formulas, we find a solution x so that $0 < x < b$ so that it produces a solution (b, x) smaller than (a, b). Note that, here, we have to take $b < a$ so that the new solution is guaranteed to be smaller. Repeating this, we will reach a base case and those constants (k, for example) will remain constant through the whole process. Thus, we will show what's required.

(iii) Sometimes, there can be even geometric interpretations. For example, *Arthur Engel* showed one in his book *Problem Solving Strategies* chapter 6, problem 15.

We will now demonstrate this using some example problems. Let's start with the classical problem from IMO 1988. Here is what Engel said about this problem in his book:

> *Nobody of the six members of the Australian problem committee could solve it. Two of the members were George Szekeres and his wife Esther Klein, both famous problem solvers and problem creators. Since it was a number theoretic problem it was sent to the four most renowned Australian number theorists. They were asked to work on it for six hours. None of them could solve it in this time. The problem committee submitted it to the jury of the XXIX IMO marked with a double asterisk, which meant a superhard problem, possibly too hard to pose. After a long discussion, the jury finally had the courage to choose it as the last problem of the competition. Eleven students gave perfect solutions.*

Problem 5.3.1 (IMO 1988, Problem 6). Let a and b be two positive integers such that $ab + 1$ divides $a^2 + b^2$. Show that $\dfrac{a^2 + b^2}{ab + 1}$ is a perfect square.

Solution. Let k be an integer so that

$$\begin{aligned} &\frac{a^2 + b^2}{ab + 1} = k \\ \implies &a^2 + b^2 = kab + k \\ \implies &a^2 - kab + b^2 - k = 0. \end{aligned}$$

As we said in the process, we will fix k and consider all pairs of integers (a, b) that gives us k as the quotient. And take a solution (a, b) in nonnegative integers so that the sum $a + b$ is minimum (and if there are multiple such (a, b), we take an arbitrary one). Without loss of generality, we can assume $a \geq b > 0$. Now, fix b and set $a = x$ which will be the variable. We get an equation which is quadratic in x with a root a:

$$x^2 - kbx + b^2 - k = 0.$$

Using Vietta, we get that $x + a = kb$ or $x = kb - a$. From this, we infer x is integer. Note that, we can write it in another way:

$$x = \frac{b^2 - k}{a}.$$

This equation will do the talking now! Firstly, if $x = 0$, we are done since that would give us $b^2 - k = 0$ or $k = b^2$, a perfect square. So, we can assume that $x \neq 0$. To descend the solution, we will need $x > 0$. For the sake of contradiction, take $x = -z$ where $z > 0$. But that would give us

$$\begin{aligned} x^2 - kbx + b^2 - k &= z^2 + kbz + b^2 - k \\ &\geq z^2 + k + b^2 - k \\ &= z^2 + b^2 > 0. \end{aligned}$$

This is impossible. Thus, $x > 0$ and now, if we can prove that $0 < x < a$, then we will have a solution (x, b) smaller than (a, b). We actually have this already because

$$\begin{aligned} x &= \frac{b^2 - k}{a} \\ &< \frac{b^2}{a} \text{ since } k \text{ is a positive integer} \\ &\leq \frac{a^2}{a} = a. \end{aligned}$$

Therefore, we must have a solution $(0, b)$ for the equation which gives us $k = b^2$.

Problem 5.3.2. Let a and b be positive integers such that ab divides $a^2 + b^2 + 1$. Prove that $a^2 + b^2 + 1 = 3ab$.

Solution. Again, let $k = \frac{a^2+b^2+1}{ab}$ and among all the solutions of the equation, consider the solution that minimizes the sum $a + b$. We can also assume that, $a \geq b$. Now for applying Vietta, we rewrite it as

$$a^2 - kab + b^2 + 1 = 0.$$

Just like before, let's fix b and make it quadratic in x, which already has a solution a:

$$x^2 - kbx + b^2 + 1 = 0.$$

For the other solution, we have

$$x = \frac{b^2 + 1}{a} \tag{5.2}$$

$$= kb - a. \tag{5.3}$$

Equation (5.2) implies that x is positive and equation (5.3) implies that x is an integer. Now, if $a = b$, we already get that $k = \dfrac{1^2 + 1^2 + 1}{1 \cdot 1} = 3$. So we are left with $a > b$. But then,

$$x = \frac{b^2 + 1}{a} < \frac{b^2 + 2b + 1}{a} = \frac{(b+1)^2}{a} \leq \frac{a^2}{a} = a,$$

which again produces a smaller sum $x + b < a + b$. This is a contradiction, so $a = b$ must happen.

Problem 5.3.3 (Romanian TST 2004). Find all integer values the expression $\frac{a^2+b^2+1}{ab-1}$ can assume for $ab \neq 1$ where a and b are positive integers.

Solution. Take

$$k = \frac{a^2+ab+b^2}{ab-1},$$

or $a^2 - a(kb-b) + k + b^2 = 0$ and fix b, when we consider the smallest sum $a+b$ for a solution (a,b) where $a \geq b$. Consider it as a quadratic in x again which has a solution a:

$$\begin{aligned} & x^2 - x(kb-b) + b^2 + k = 0 \\ \implies & x + a = kb - b \implies x = kb - a - b, \text{ and} \\ & xa = b^2 + k \implies x = \frac{b^2+k}{a}. \end{aligned}$$

We have that x is a positive integer. Since $a+b$ is minimal, we have $x \geq a$. So

$$\begin{aligned} & \frac{b^2+k}{a} \geq a \\ \implies & k \geq a^2 - b^2. \end{aligned}$$

But $k = \frac{a^2+ab+b^2}{ab-1}$, so

$$\begin{aligned} & \frac{a^2+ab+b^2}{ab-1} \geq a^2 - b^2 \\ \implies & a^2+ab+b^2 \geq (a^2-b^2)(ab-1) = ab(a+b)(a-b) - a^2 + b^2 \\ \implies & a(a+b) \geq ab(a+b)(a-b) - a^2 \\ \implies & a \geq (a+b)(ab-b^2-1). \end{aligned} \tag{5.4}$$

If $a = b$, then $k = \frac{3a^2}{a^2-1}$. Since $a^2 \perp a^2 - 1$, we have $a^2 - 1$ divides 3 or $a = 2$. In that case, $k = 4$. If $b = 1$, then $k = \frac{a^2+a+1}{a-1}$ so $a-1$ divides a^2+a+1.

$$\begin{aligned} & a-1 | a^2 - 1 \\ \implies & a-1 | a^2 + a + 1 - (a^2-1) = a+2 \\ \implies & a-1 | (a+2) - (a-1) = 3. \end{aligned}$$

We get that $a = 2$ or $a = 4$. If $a = 2$ or $a = 4$, then $k = 7$. If $a > b > 1$, then, $a \geq b+1$ and we have

$$(a+b)(ab-b^2-1) > a,$$

which is in contradiction with equation (5.4). Therefore, we have $k = 4$ or $k = 7$.

Problem 5.3.4 (Mathlinks Contest). Let a, b, c, d be four distinct positive integers in arithmetic progression. Prove that $abcd$ is not a perfect square.

5.4 Exponent gcd Lemma

For brevity assume

$$f(x,y,n)=\frac{x^n-y^n}{x-y}.$$

Remember from definition (3.2.12) that $v_p(n)=\alpha$ means α is the greatest positive integer so that $p^\alpha|n$. Alternatively, we can denote this by $p^\alpha\|n$.

Theorem 5.4.1 (Exponent gcd Lemma). *If $x\perp y$, then*

$$g=\big(x-y,f(x,y,n)\big)\big|n.$$

Proof. Re-call the identity

$$x^n-y^n=(x-y)\left(x^{n-1}+x^{n-2}y+\cdots+xy^{n-2}+y^{n-1}\right).$$

This yields to

$$f(x,y,n)=x^{n-1}+x^{n-2}y+\ldots+xy^{n-2}+y^{n-1}$$

We know that for polynomials P and Q, if

$$P(x)=(x-a)\cdot Q(x)+r,$$

then $r=P(a)$ (the reason is simple, just plug in a into P). So, in this case,

$$f(x,y,n)=(x-y)\cdot Q(x,y,n)+r.$$

Hence, $r=f(y,y,n)$ which equals

$$f(y,y,n)=y^{n-1}+y^{n-2}\cdot y+\ldots+y^{n-1}=ny^{n-1}.$$

From Euclidean algorithm, we can infer

$$\big(x-y,f(x,y,n)\big)=\big(x-y,f(y,y,n)\big)=\big(x-y,ny^{n-1}\big).$$

Earlier we assumed $x\perp y$, and so $x-y\perp y^{n-1}$ because $(x-y,y)=(x,y)=1$. Thus

$$g=\big(x-y,f(x,y,n)\big)=\big(x-y,n\big),$$

which results in $g|n$. □

Corollary 5.4.2. *The following result is true for any odd positive integer n:*

$$\left(x+y,\frac{x^n+y^n}{x+y}\right)\Big|n.$$

Corollary 5.4.3. *For a prime p,*

$$(x-y,f(x,y,p))=1 \text{ or } p.$$

Let's see how we can use this lemma to solve problems.

Problem 5.4.4 (Hungary 2000). Find all positive primes p for which there exist positive integers n, x, and y such that

$$x^3 + y^3 = p^n.$$

Solution. For $p = 2$, $x = y = 1$ works. Assume p is greater than 2, and hence odd.

If $(x, y) = d$, then we have $d|p^n$. So, d is a power of p. But in that case, we can divide the whole equation by d and still it remains an equation of the same form. Let's therefore, consider $(x, y) = 1$. Factorizing,

$$(x + y)(x^2 - xy + y^2) = p^n.$$

According to the lemma,

$$g = (x + y, f(x, y, 3)) \,\big|\, (x + y, 3)$$

This means $g|3$. If $g = 3$, then we have $3|p$ or $p = 3$. On the other hand, $g = 1$ shall mean that $x + y = 1$ or $x^2 - xy + y^2 = 1$. Neither of them is true because $x, y > 0, x + y > 1$ and $(x - y)^2 + xy > 1$.

Problem 5.4.5. Find all primes p and positive integer x such that

$$p^x - 1 \;=\; (p - 1)!.$$

Solution. We know that if $n \geq 6$ is a composite integer, then n divides $(n - 1)!$. Now, $\dfrac{p^x - 1}{p - 1} = (p - 2)!$. Assume $p > 5$, then $p \geq 7$ so $p - 1|(p - 2)!$. Thus, $p - 1 \Big| \dfrac{p^x - 1}{p - 1}$ and so from the lemma, $p - 1|x$ or $x \geq p - 1$. So

$$(p - 1)! = p^x - 1 \geq p^{p-1} - 1,$$

which is not true since

$$n! < (n + 1)^n - 1,$$

for $n > 1$. So we need to check for only $p \in \{2, 3, 5\}$. If $p = 2$, then $2^x - 1 = 1$, so $x = 1$. If $p = 3$, then $3^x - 1 = 2$ so $x = 1$. If $p = 5$, $5^x - 1 = 24$ so $x = 2$.

5.5 A Congruence Lemma Involving gcd

In this section, we discuss yet another lemma, which involves gcd like the previous one. The first author of this book finds it really useful for solving some types of problems. The lemma was proved in Theorem (2.4.15) of chapter (2).

Lemma 5.5.1. *Let a, b, and n be three positive integers such that $(a, n) = (b, n) = 1$ and*

$$\begin{aligned} a^x &\equiv b^x \pmod{n}, \\ a^y &\equiv b^y \pmod{n}, \end{aligned}$$

then

$$a^{(x,y)} \equiv b^{(x,y)} \pmod{n}.$$

Corollary 5.5.2. *Let p be a prime and let a and b be integers not divisible by p so that*

$$a^k \equiv b^k \pmod{p}.$$

Then

$$a^{(k,p-1)} \equiv b^{(k,p-1)} \pmod{n}.$$

The following corollary also proves theorem (2.12.2) easily.

Corollary 5.5.3. *Let a, b, and n be three positive integers such that $(a, n) = (b, n) = 1$. If h is the smallest integer such that*

$$a^h \equiv b^h \pmod{n},$$

and k is an integer such that

$$a^k \equiv b^k \pmod{n},$$

then $h|k$.

Proof. From the lemma, we have $a^{(h,k)} \equiv b^{(h,k)} \pmod{n}$. We have $(h, k) \leq h$ and $(h, k)|k$. Now, if $(h, k) < h$ then (h, k) is smaller than h which satisfies the condition. So we must have $(h, k) = h$, or $h|k$. □

Corollary 5.5.4. *Let p be a prime and let a be a positive integer. If $\mathrm{ord}_p(a) = d$ and $a^k \equiv 1 \pmod{p}$, then $d|(p - 1, k)$.*

Proof. From Fermat's little theorem, $a^{p-1} \equiv 1 \pmod{p}$. From the theorem, $a^{(k,p-1)} \equiv 1 \pmod{p}$ and from corollary above, $d|(k, p - 1)$. □

You should see that if a problem can be solved using the dividing property of order, then we can solve it using this lemma as well. Let's see some problems that this lemma is useful with. Sometimes, we have to couple this lemma with some other techniques such as the **smallest prime factor trick**.

Problem 5.5.5. Find all $n \in \mathbb{N}$ such that $2^n - 1$ is divisible by n.

A standard problem with a very nice idea. There are many ways to start working on such problems. A common one is to find the prime factors of n first. That way, we have some idea about n at first, from which we can understand the nature of the problem. **Sometimes we have to find special prime factors first**. The special prime factors can provide some extra information necessary.

Solution. Here, we consider the **smallest prime divisor** of n. Let's call this prime p. Since n divides $2^n - 1$, p divides it too. Because $2^n - 1$ is odd, both n and p must be odd. So

$$2^n \equiv 1 \pmod{p}.$$

This equation alone does not say a lot, so we need more information. Remember Fermat's little theorem! This is another reason to find primes first. Only for primes we can get the power a^{p-1}, otherwise from Euler's Totient theorem, it would be $a^{\varphi(n)}$ which would bring troubles in this case. We have

$$2^{p-1} \equiv 1 \pmod{p}$$

Whenever you get two congruences like this, be sure to use theorem (2.4.15). Using this,

$$2^{(n,p-1)} \equiv 1 \pmod{p}$$

Now you will see why we specifically chose the smallest prime divisor instead of an arbitrary prime divisor. Since p is the smallest prime divisor of n, if a prime q divides $p-1$, it can not divide n. Because if $q|n$, then $q \leq p-1 < p$, which is a smaller prime divisor than the smallest prime divisor of n, a contradiction! We must have $(n, p-1) = 1$. But then $2^1 \equiv 1 \pmod{p}$ or $p|2-1=1$. Another contradiction. This means for no prime p, n is divisible by p. So n can not have any primes i.e. $n = 1$.

Note. Not just smallest prime divisor, depending on the problem we occasionally take the greatest prime divisor or something that makes our job easier to do. See the following problems for better understanding.

Problem 5.5.6. Determine all pairs of primes (p, q) such that $pq|p^p + q^q + 1$.

Solution. If (p, q) is a solution, so is (q, p). Without loss of generality, assume that $p < q$ since $p = q$ implies $p|1$. Now, $pq|p^p + q^q + 1$ gives us two things: $p|q^q + 1$ and $q|p^p + 1$.. Consider $p = 2$, then $q|p^p + 1 = 5$, so $q = 5$. Now, p is odd and so $q > p + 1$. We can alternatively write them as $q^{2q} \equiv 1 \pmod{p}$ and $p^{2p} \equiv 1 \pmod{q}$. From Fermat's theorem, we also have $q^{p-1} \equiv 1 \pmod{p}$ and $p^{q-1} \equiv 1 \pmod{q}$. Thus, $q^{\gcd(2q,p-1)} \equiv 1 \pmod{p}$ and $p^{\gcd(2p,q-1)} \equiv 1 \pmod{q}$. Since q is odd and greater than $p-1$, $\gcd(q, p-1) = 1$. We have $q^2 \equiv 1 \pmod{p}$ or p divides $(q+1)(q-1)$. If p divides $q-1$, then p also divides $q^q - 1$. But that would force the contradiction $p|q^q + 1 - (q^q - 1) = 2$. So, p must divide $q+1$. On the other hand, since p can't divide $q-1$, we get $\gcd(2p, q-1) = 2$. This gives $p^2 \equiv 1 \pmod{q}$ or $q|(p+1)(p-1)$. This is impossible since q divides none of $p \pm 1$. So no other solutions.

Problem 5.5.7. Find all primes p, q such that $pq|(5^p - 2^p)(5^q - 2^q)$.

Solution. If $p|5^p - 2^p$, from FLT (Fermat's little theorem) we get

$$5^p - 2^p \equiv 5 - 2 \equiv 3 \pmod{p}.$$

So, p must be 3. Then if $p = q$, $q = 3$. Otherwise, $q|5^p - 2^p = 5^3 - 2^3 = 117 = 3^2 \cdot 13$ so $q = 13$. Now, we can assume $p|5^q - 2^q$ and $q|5^p - 2^p$. It is obvious, none of p or q can be 2 or 5. From the lemma,

$$5^{(p,q-1)} \equiv 2^{(p,q-1)} \pmod{q}.$$

Here, $p > q - 1$, so $p \perp q - 1$. Therefore, $5^1 \equiv 2 \pmod{q}$ or $q = 3$.

5.6 Lifting the Exponent Lemma

Lifting The Exponent Lemma is a powerful method for solving exponential Diophantine equations. It is pretty well-known in the literature though its origins are hard to trace. Mathematically, it is a close relative of *Hensel's lemma* in number theory (in both the statement and the idea of the proof). This is a technique that has been used a lot in recent olympiad problems.

One can use the Lifting The Exponent Lemma (this is a long name, let's call it **LTE**!) in problems involving exponential equations, especially when there are some prime numbers (and actually in some cases overkills the problems). This lemma shows how to find the greatest power of a prime p – which is often ≥ 3 – that divides $a^n \pm b^n$ for some positive integers a and b. The advantage of this lemma is that, it is quite simple to understand and if in some contest, it is refrained from being used, the proof is not hard as well.

In section (3.2.2) of chapter (3), we defined $v_p(n)$. Recall that $v_p(n)$ is the highest power of a prime p which divides a positive integer n. Here, we will make use of this function to solve Diophantine equations.

Here is a problem which will explain the main idea behind LTE.

Problem 5.6.1. Show that there exist no positive integers x and y such that

$$2^{6x+1} + 1 = 3^{2y}.$$

Solution. The idea is that the largest power of 3 which divides the right side of the given equation, should be the same as that of the left side. Clearly, $v_3(3^{2y}) = 2y$. Let's find $v_3\left(2^{6x+1} + 1\right)$. Since $6x + 1 = 2 \cdot x + 1$ is odd, we can write

$$2^{6x+1} + 1 = (2 + 1)\left(2^{6x} - 2^{6x-1} + 2^{6x-2} - \cdots - 2 + 1\right).$$

$(2^{6x} - 2^{6x-1} + 2^{6x-2} - \cdots - 2 + 1)$ is not divisible by 3 (try to figure out why, using induction on x). Therefore

$$\begin{aligned} v_3\left(2^{6x+1} + 1\right) &= v_3\left(2 + 1\right) + v_3\left(2^{6x} - 2^{6x-1} + 2^{6x-2} - \cdots - 2 + 1\right) \\ &= 1 + 0 \\ &= 1. \end{aligned}$$

This means that $2y = 1$, which is impossible since y is an integer.

5.6.1 Two Important and Useful Lemmas

Lemma 5.6.2. *Let x and y be (not necessarily positive) integers and let n be a positive integer. Given an arbitrary prime p (in particular, we can have $p = 2$) such that $\gcd(n, p) = 1$, $p \mid x - y$ and neither x, nor y is divisible by p (i.e., $p \nmid x$ and $p \nmid y$). We have*

$$v_p\big(x^n - y^n\big) = v_p(x - y).$$

Proof. We use the fact that

$$x^n - y^n = (x - y)\big(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + y^{n-1}\big).$$

Now if we show that $p \nmid x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + y^{n-1}$, then we are done. In order to show this, we use the assumption $p \mid x - y$. So we have $x - y \equiv 0 \pmod{p}$, or $x \equiv y \pmod{p}$. Thus

$$\begin{aligned} x^{n-1}+x^{n-2}y + x^{n-3}y^2 + \cdots + y^{n-1} &\equiv x^{n-1} + x^{n-2} \cdot x + x^{n-3} \cdot x^2 + \cdots + x \cdot x^{n-2} + x^{n-1} \\ &\equiv nx^{n-1} \\ &\not\equiv 0 \pmod{p}. \end{aligned}$$

This completes the proof. □

Lemma 5.6.3. *Let x and y be (not necessarily positive) integers and let n be an odd positive integer. Given an arbitrary prime p (in particular, we can have $p = 2$) such that $\gcd(n, p) = 1$, $p \mid x + y$ and neither x, nor y is divisible by p, we have*

$$v_p\big(x^n + y^n\big) = v_p(x + y).$$

Proof. Since x and y can be negative in lemma (5.6.2) we only need to put $(-y)^n$ instead of y^n in the formula to obtain

$$v_p\big(x^n - (-y)^n\big) = v_p(x - (-y)) \implies v_p\big(x^n + y^n\big) = v_p(x + y).$$

Note that since n is an odd positive integer we can replace $(-y)^n$ with $-y^n$. □

5.6.2 Main Result

Theorem 5.6.4 (First Form of LTE). *Let x and y be (not necessarily positive) integers, let n be a positive integer, and let p be an odd prime such that $p \mid x - y$ and none of x and y is divisible by p (i.e., $p \nmid x$ and $p \nmid y$). We have*

$$v_p(x^n - y^n) = v_p(x - y) + v_p(n).$$

Proof. We may use induction on $v_p(n)$. First, let us prove the following statement:

$$v_p(x^p - y^p) = v_p(x - y) + 1. \tag{5.5}$$

In order to prove this, we will show that

$$p \mid x^{p-1} + x^{p-2}y + \cdots + xy^{p-2} + y^{p-1} \tag{5.6}$$

and

$$p^2 \nmid x^{p-1} + x^{p-2}y + \cdots + xy^{p-2} + y^{p-1}. \tag{5.7}$$

For (5.6), we note that

$$x^{p-1} + x^{p-2}y + \cdots + xy^{p-2} + y^{p-1} \equiv px^{p-1} \equiv 0 \pmod{p}.$$

Now, let $y = x + kp$, where k is an integer. For an integer $1 \leq t < p$ we have

$$\begin{aligned} y^t x^{p-1-t} &\equiv (x + kp)^t x^{p-1-t} \\ &\equiv x^{p-1-t}\left(x^t + t(kp)(x^{t-1}) + \frac{t(t-1)}{2}(kp)^2(x^{t-2}) + \cdots\right) \\ &\equiv x^{p-1-t}\left(x^t + t(kp)(x^{t-1})\right) \\ &\equiv x^{p-1} + tkpx^{p-2} \pmod{p^2}. \end{aligned}$$

This means

$$y^t x^{p-1-t} \equiv x^{p-1} + tkpx^{p-2} \pmod{p^2}, \quad t = 1, 2, \ldots, p-1.$$

Using this fact, we have

$$\begin{aligned} &x^{p-1} + x^{p-2}y + \cdots + xy^{p-2} + y^{p-1} \\ &\quad\equiv x^{p-1} + \left(x^{p-1} + kpx^{p-2}\right) + \left(x^{p-1} + 2kpx^{p-2}\right) + \cdots + \left(x^{p-1} + (p-1)kpx^{p-2}\right) \\ &\quad\equiv px^{p-1} + \left(1 + 2 + \cdots + p - 1\right)kpx^{p-2} \\ &\quad\equiv px^{p-1} + \left(\frac{p(p-1)}{2}\right)kpx^{p-2} \\ &\quad\equiv px^{p-1} + \left(\frac{p-1}{2}\right)kp^2x^{p-1} \\ &\quad\equiv px^{p-1} \not\equiv 0 \pmod{p^2}. \end{aligned}$$

So we proved the relation (5.7) and the proof of equation (5.5) is complete. Now let us return to our problem. We want to show that

$$v_p\left(x^n - y^n\right) = v_p(x - y) + v_p(n).$$

Suppose that $n = p^\alpha b$ where $\gcd(p, b) = 1$. Then

$$\begin{aligned} v_p(x^n - y^n) &= v_p\big((x^{p^\alpha})^b - (y^{p^\alpha})^b\big) \\ &= v_p\big(x^{p^\alpha} - y^{p^\alpha}\big) = v_p\big((x^{p^{\alpha-1}})^p - (y^{p^{\alpha-1}})^p\big) \\ &= v_p\big(x^{p^{\alpha-1}} - y^{p^{\alpha-1}}\big) + 1 = v_p\big((x^{p^{\alpha-2}})^p - (y^{p^{\alpha-2}})^p\big) + 1 \\ &= v_p\big(x^{p^{\alpha-2}} - y^{p^{\alpha-2}}\big) + 2 \\ &\vdots \\ &= v_p\big((x^{p^1})^1 - (y^{p^1})^1\big) + \alpha - 1 = v_p\big(x - y\big) + \alpha \\ &= v_p\big(x - y\big) + v_p\big(n\big). \end{aligned}$$

Note that we used the fact that if $p \mid x - y$, then we have $p \mid x^k - y^k$, because we have $x - y \mid x^k - y^k$ for all positive integers k. The proof is complete. □

Theorem 5.6.5 (Second Form of LTE). *Let x, y be two integers, n be an odd positive integer, and p be an odd prime such that $p \mid x + y$ and none of x and y is divisible by p. We have*

$$v_p(x^n + y^n) = v_p(x + y) + v_p(n).$$

Proof. This is obvious using theorem (5.6.4). See the trick we used in proof of lemma (5.6.3). □

The following theorem is a special case of Zsigmondy's theorem (discussed later in (5.7.2)), which can be proved using LTE and EGL (theorem (5.4.1)). And probably it is the most important case of Zsigmondy's theorem we use in problems. In case someone considers the original theorem to be a sledgehammer, in that case this theorem should work fine. We leave the proof as an exercise.

Theorem 5.6.6. *For a prime $p > 3$ and coprime integers x, y, $x^{p^k} - y^{p^k}$ has a prime factor q such that $q | x^{p^k} - y^{p^k}$ but $q \nmid x^{p^i} - y^{p^i}$ for $0 \leq i < k$.*

5.6.3 The Case $p = 2$

Question 5.6.7. Why did we assume that p is an odd prime, i.e., $p \neq 2$? Why can't we assume that $p = 2$ in our proofs?

Hint. Note that $\frac{p-1}{2}$ is an integer only for $p > 2$.

Theorem 5.6.8 (LTE for $p = 2$). *Let x and y be two odd integers such that $4 \mid x - y$. Then*

$$v_2\big(x^n - y^n\big) = v_2(x - y) + v_2(n).$$

Proof. We showed that for any prime p such that $\gcd(p, n) = 1, p \mid x - y$ and none of x and y is divisible by p, we have

$$v_p(x^n - y^n) = v_p(x - y)$$

So it suffices to show that

$$v_2(x^{2^n} - y^{2^n}) = v_2(x - y) + n.$$

Factorization gives

$$x^{2^n} - y^{2^n} = (x^{2^{n-1}} + y^{2^{n-1}})(x^{2^{n-2}} + y^{2^{n-2}}) \cdots (x^2 + y^2)(x + y)(x - y)$$

Now since $x \equiv y \equiv \pm 1 \pmod 4$ then we have $x^{2^k} \equiv y^{2^k} \equiv 1 \pmod 4$ for all positive integers k and so $x^{2^k} + y^{2^k} \equiv 2 \pmod 4, k = 1, 2, 3, \ldots$. Also, since x and y are odd and $4 \mid x - y$, we have $x + y \equiv 2 \pmod 4$. This means the power of 2 in all of the factors in the above product (except $x - y$) is one. We are done. □

Theorem 5.6.9. *Let x and y be two odd integers and let n be an even positive integer. Then*

$$v_2\big(x^n - y^n\big) = v_2(x - y) + v_2(x + y) + v_2(n) - 1.$$

Proof. We know that the square of an odd integer is of the form $4k + 1$. So for odd x and y we have $4 \mid x^2 - y^2$. Now let m be an odd integer and k be a positive integer such that $n = m \cdot 2^k$. Then

$$\begin{aligned} v_2\big(x^n - y^n\big) &= v_2\big(x^{m \cdot 2^k} - y^{m \cdot 2^k}\big) \\ &= v_2\big((x^2)^{2^{k-1}} - (y^2)^{2^{k-1}}\big) \\ &\vdots \\ &= v_2\big(x^2 - y^2\big) + k - 1 \\ &= v_2(x - y) + v_2(x + y) + v_2(n) - 1. \end{aligned}$$

□

5.6.4 Summary

Let p be a prime number and let x and y be two (not necessarily positive) integers that are not divisible by p. Then:

(a) For a positive integer n

- if $p \neq 2$ and $p \mid x - y$, then
$$v_p\big(x^n - y^n\big) = v_p(x - y) + v_p(n).$$
- if $p = 2$ and $4 \mid x - y$, then
$$v_2\big(x^n - y^n\big) = v_2(x - y) + v_2(n).$$
- if $p = 2$, n is even, and $2 \mid x - y$, then
$$v_2\big(x^n - y^n\big) = v_2(x - y) + v_2(x + y) + v_2(n) - 1.$$

(b) For an odd positive integer n, if $p \mid x+y$, then

$$v_p\big(x^n+y^n\big) = v_p(x+y) + v_p(n).$$

(c) For a positive integer n with $\gcd(p,n)=1$, if $p \mid x-y$, we have

$$v_p\big(x^n-y^n\big) = v_p(x-y).$$

If n is odd, $\gcd(p,n)=1$, and $p \mid x+y$, then we have

$$v_p\big(x^n+y^n\big) = v_p(x+y).$$

Note. The most common mistake in using LTE is when you do not check the $p \mid x \pm y$ condition, so always remember to check it. Otherwise your solution will be completely wrong.

5.6.5 Solved Problems

Problem 5.6.10 (Russia 1996). Find all positive integers n for which there exist positive integers x, y and k such that $\gcd(x,y)=1, k>1$ and $3^n = x^k + y^k$.

Solution. k should be an odd integer (otherwise, if k is even, then x^k and y^k are perfect squares, and it is well known that for integers a, b we have $3 \mid a^2+b^2$ if and only if $3 \mid a$ and $3 \mid b$, which is in contradiction with $\gcd(x,y)=1$.). Suppose that there exists a prime p such that $p \mid x+y$. This prime should be odd. So $v_p(3^n) = v_p(x^k+y^k)$, and using (5.6.5) we have

$$v_p(3^n) = v_p(x^k+y^k) = v_p(k) + v_p(x+y).$$

But $p \mid x+y$ means that $v_p(x+y) \geq 1 > 0$ and so $v_p(3^n) = v_p(k) + v_p(x+y) > 0$ and so $p \mid 3^n$. Thus $p=3$. This means $x+y = 3^m$ for some positive integer m. Note that $n = v_3(k) + m$. There are two cases:

1. $m > 1$. We can prove by induction that $3^a \geq a+2$ for all integers $a \geq 1$, and so we have $v_3(k) \leq k-2$ (why?). Let $M = \max(x,y)$. Since $x+y = 3^m \geq 9$, we have $M \geq 5$. Then

$$\begin{aligned} x^k + y^k \geq M^k &= \underbrace{M}_{\geq \frac{x+y}{2} = \frac{1}{2}\cdot 3^m} \cdot \underbrace{M^{k-1}}_{\geq 5^{k-1}} \\ &> \frac{1}{2} 3^m \cdot 5^{k-1} \\ &> 3^m \cdot 5^{k-2} \\ &\geq 3^{m+k-2} \\ &\geq 3^{m+v_3(k)} \\ &= 3^n, \end{aligned}$$

which is a contradiction.

2. $m = 1$. Then $x + y = 3$, so $x = 1, y = 2$ (or $x = 2, y = 1$). Thus $3^{1+v_3(k)} = 1 + 2^k$. But note that $3^{v_3(k)} \mid k$ so $3^{v_3(k)} \leq k$. Thus

$$1 + 2^k = 3^{v_3(k)+1} = 3 \cdot \underbrace{3^{v_3(k)}}_{\leq k} \leq 3k \implies 2^k + 1 \leq 3k.$$

And one can check that the only odd value of $k > 1$ that satisfies the above inequality is $k = 3$. So $(x, y, n, k) = (1, 2, 2, 3), (2, 1, 2, 3)$ in this case.

Thus, the final answer is $n = 2$.

Problem 5.6.11 (Balkan 1993). Let p be a prime number and $m > 1$ be a positive integer. Show that if for some positive integers $x > 1, y > 1$ we have

$$\frac{x^p + y^p}{2} = \left(\frac{x + y}{2}\right)^m,$$

then $m = p$.

Solution. One can prove by induction on p that

$$\frac{x^p + y^p}{2} \geq \left(\frac{x + y}{2}\right)^p$$

for all positive integers p. Now since

$$\frac{x^p + y^p}{2} = \left(\frac{x + y}{2}\right)^m,$$

we should have $m \geq p$. Let $d = \gcd(x, y)$, so there exist positive integers x_1 and y_1 with $\gcd(x_1, y_1) = 1$ such that $x = dx_1$, $y = dy_1$, and

$$2^{m-1}(x_1^p + y_1^p) = d^{m-p}(x_1 + y_1)^m.$$

There are two cases:

1. Assume that p is odd. Take any prime divisor q of $x_1 + y_1$ and let $v = v_q(x_1 + y_1)$. If q is odd, we see that

$$v_q(x_1^p + y_1^p) = v + v_q(p) \text{ and } v_q(d^{m-p}(x_1 + y_1)^m) \geq mv$$

(because q may also be a factor of d). Thus $m \leq 2$ and $p \leq 2$, giving an immediate contradiction. If $q = 2$, then $m - 1 + v \geq mv$, so $v \leq 1$ and $x_1 + y_1 = 2$, i.e., $x = y$, which immediately implies $m = p$.

2. Assume that $p = 2$. We notice that for $x + y \geq 4$ we have

$$\frac{x^2 + y^2}{2} < 2\left(\frac{x + y}{2}\right)^2 \leq \left(\frac{x + y}{2}\right)^3,$$

so $m = 2$. It remains to check that the remaining cases $(x, y) = (1, 2), (2, 1)$ are impossible.

Problem 5.6.12. Find all positive integers a, b that are greater than 1 and satisfy

$$b^a | a^b - 1.$$

Solution. Let p be the least prime divisor of b. Let m be the least positive integer for which $p|a^m - 1$. Then $m|b$ and $m \mid p-1$, so any prime divisor of m divides b and is less than p. Thus, not to run into a contradiction, we must have $m = 1$. Now, if p is odd, we have $av_p(b) \leq v_p(a-1) + v_p(b)$, so

$$a - 1 \leq (a-1)v_p(b) \leq v_p(a-1),$$

which is impossible. Thus $p = 2$, b is even, a is odd, and

$$av_2(b) \leq v_2(a-1) + v_2(a+1) + v_2(b) - 1$$

whence

$$a \leq (a-1)v_2(b) + 1 \leq v_2(a-1) + v_2(a+1)$$

which is possible only if $a = 3$ and $v_2(b) = 1$. Put $b = 2B$ with odd B and rewrite the condition as $2^3B^3 \mid 3^{2B} - 1$. Let q be the least prime divisor of B (now, surely, odd). Let n be the least positive integer such that $q \mid 3^n - 1$. Then $n \mid 2B$ and $n \mid q-1$ whence n must be 1 or 2 (or B has a smaller prime divisor), so $q \mid 3 - 1 = 2$ or $q \mid 3^2 - 1 = 8$, which is impossible. Thus $B = 1$ and $b = 2$.

Problem 5.6.13. Find all positive integer solutions of the equation $x^{2009} + y^{2009} = 7^z$

Solution. Factor 2009. We have $2009 = 7^2 \cdot 41$. Since $x+y \mid x^{2009}+y^{2009}$ and $x+y > 1$, we must have $7 \mid x + y$. Removing the highest possible power of 7 from x, y, we get

$$v_7(x^{2009} + y^{2009}) = v_7(x + y) + v_7(2009) = v_7(x + y) + 2,$$

so $x^{2009}+y^{2009} = 49 \cdot k \cdot (x+y)$ where $7 \nmid k$. But we have $x^{2009}+y^{2009} = 7^z$, which means the only prime factor of $x^{2009}+y^{2009}$ is 7, so $k = 1$. Thus $x^{2009}+y^{2009} = 49(x+y)$. But in this equation the left hand side is much larger than the right hand one if $\max(x, y) > 1$, and, clearly, $(x, y) = (1, 1)$ is not a solution. Thus the given equation does not have any solutions in the set of positive integers.

5.7 Zsigmondy's Theorem

Zsigmondy's theorem is one of the tactics that can easily tackle a good number of *hard problems* in recent years. This is indeed a mighty theorem to be used in an olympiad. But it seems everyone has accepted it as a tool for solving problems because the proof of its theorem is quite elementary[1] (still hard). At the IMO, often some problems appear that can be solved very easily using some heavy theorems. But those theorems are usually not accepted by everyone for not being as elementary as needed. But in this

[1] according to the first author, there may be a difference in opinion

case, everyone seems to like this theorem. The first author was really keen to provide the proof of this theorem along with some other similar theorems[2]. But that really is beyond the scope of our book. Since it is a well established theorem, for now, we will just assume it is true. Rather we focus on how to implement this theorem in solving problems.

Definition 5.7.1 (Primitive Divisor). For a sequence of integers $a_1, a_2, \ldots, a_n, \ldots$ a prime number p is a *primitive* divisor of a_n if p divides a_n but p doesn't divide a_k for any $k < n$. *R. D. Carmichael* called such a prime an *intrinsic* divisor.

Example. Consider the sequence $a_k = 2^k - 1$. $a_1 = 1, a_2 = 3, a_3 = 7, a_4 = 15$. Note that, a_3 has primitive divisor 7 and a_4 has the primitive divisor 5.

Theorem 5.7.2 (Zsigmondy's Theorem, 1882**).** *Let a, b be co-prime integers and $n \geq 1$ be an integer.*

- *$a^n - b^n$ has a primitive divisor except when:*
  - *(a) $a - b = 1$, $n = 1$.*
  - *(b) $a = 2, b = 1$ and $n = 6$.*
  - *(c) $a + b$ is a power of 2 and $n = 2$.*
- *$a^n + b^n$ has a primitive divisor for $n \geq 2$ except for the case $2^3 + 1^3$.*

This theorem can be extended even further.

Theorem 5.7.3 (First Extension). *Let p be a primitive divisor of $a^n + b^n$. Then p does not divide $a^k + b^k$ for $n + 1 \leq k \leq 2n$.*

Proof. Since $n + 1 \leq k \leq 2n$, for $k = n + l$, we get $1 \leq l \leq n$. p does not divide any of a or b. For the sake of contradiction, let's assume, p divides $a^k + b^k$.

$$p|a^l(a^n + b^n) = a^k + a^l b^n, \text{ and}$$
$$p|b^l(a^n + b^n) = a^n b^l + b^k.$$

Therefore

$$p|a^k + a^l b^n + a^n b^l + b^k.$$

We already know $p|a^k + b^k$, so if $n = l + m$ (since $l \leq n$), then

$$p|a^l b^n + a^n b^l = a^l b^l(a^m + b^m).$$

Since $p \perp ab$, we have $p \perp a^l b^l$. So $p|a^m + b^m$ where $m < n$, which is a contradiction. □

In a similar fashion, we can prove the following theorem.

[2]such as Carmichael Theorem

Theorem 5.7.4 (Second Extension). *Let p be a primitive divisor of $a^n + b^n$. Then p does not divide $a^k - b^k$ for $1 \leq k < \frac{n}{2}$.*

In this section, we will see some demonstration of its power in solving problems and then develop a theorem that generalizes a problem of IMO shortlist. The main idea is to find some contradictions using the fact that $a^n - b^n$ will have a prime factor that won't divide something else.

Problem 5.7.5 (Japanese Math Olympiad, 2011). Find all $5-$tuples (a, n, x, y, z) of positive integers so that

$$a^n - 1 = (a^x - 1)(a^y - 1)(a^z - 1).$$

Solution. If $a, n \geq 3$ and $n > x, y, z$, we already know from the theorem that $a^n - 1$ has a prime divisor that none of $a^x - 1, a^y - 1$ or $a^z - 1$ has. Therefore, two sides can never be equal. We are left with cases $n \leq 3$. Note that, $n \notin \{x, y, z\}$. But $a^x - 1$ divides $a^n - 1$, so x divides n. Thus, $n > x, y, z$ and hence $a, n \leq 3$, like we said before.

Now, either $a < 3$ or $n < 3$. If $a < 3$, then $a = 2$ and

$$2^n - 1 = (2^x - 1)(2^y - 1)(2^z - 1).$$

Here, the only exception is $n = 6$ and $2^6 - 1 = 63 = 3 \cdot 3 \cdot 7 = (2^2 - 1)(2^2 - 1)(2^3 - 1)$. So, $\{x, y, z\} = \{2, 2, 3\}$. Only $n < 3$ is left to deal with and it is easy to check that there are no solutions in this case.

Problem 5.7.6 (Polish Math Olympiad). If p and q are distinct odd primes, show that $2^{pq} - 1$ has at least three distinct prime divisors.

Solution. Without loss of generality, consider that $2 < q < p < pq$. Then $2^q - 1$ has at least one prime factor, $2^p - 1$ has a prime factor that is not in $2^q - 1$ and $2^{pq} - 1$ has a prime factor that is not in any of $2^p - 1$ or $2^q - 1$. Since $2^p - 1 | 2^{pq} - 1$ and $2^q - 1 | 2^{pq} - 1$, we have three distinct prime factors.

Problem 5.7.7 (Hungary 2000, Problem 1). Find all $4-$tuples (a, b, p, n) of positive integers with p a prime number such that

$$a^3 + b^3 = p^n.$$

Solution. To apply the theorem, first we need to make a and b co-prime. If q is a prime divisor of $(a, b) = g$, then $q|p$. Therefore, $g = p^r$ for some r. Let, $a = p^r x, b = p^r y$ with $x \perp y$. Then,

$$x^3 + y^3 = p^{n-3r}.$$

Assume that $m = n - 3r$. Since the power is three, we need to consider the exceptional case first. The case $x = 2$ and $y = 1$ when $p = 3$ and $n - 3r = 2$ produces infinitely many solutions. Otherwise, $x^3 + y^3$ has a prime divisor that does not divide $x + y$. Obviously $x + y$ is divisible by p since $x + y > 1$. This is a contradiction. Therefore, the only families of solutions are

$$(a, b, p, n) = (2 \cdot 3^r, 3^r, 3, 3r + 2) \text{ and } (3^r, 2 \cdot 3^r, 3, 3r + 2),$$

for any positive integer r.

The next problem is from IMO Shortlist.

Problem 5.7.8 (IMO Shortlist 2002, Problem 4). If $p_1, p_2, \ldots, p_n$ are distinct primes greater than 3, prove that, $2^{p_1 p_2 \cdots p_n} + 1$ has at least 4^n divisors.

Here, we will prove a much more generalization. And you can certainly see just how much the problem can be improved with this theorem.

Theorem 5.7.9. *If $p_1, p_2, \ldots, p_n$ are all primes greater than 3, then $2^{p_1 p_2 \cdots p_n} + 1$ has at least 2^{2^n} divisors.*

In order to prove this theorem, let's first prove the following lemma.

Lemma 5.7.10. *Let $N = 2^{p_1 \cdots p_n} + 1$ where $p_i > 3$ is a prime. Then N has at least 2^n distinct prime divisors.*

Proof. The number $M = p_1 p_2 \ldots p_n$ has $\underbrace{(1+1)(1+1)\ldots(1+1)}_{n \text{ times}} = 2^n$ divisors. Say the divisors are

$$1 = d_1 < d_2 < \ldots < d_{2^n} = p_1 \cdots p_n.$$

Then first $2^{d_1} + 1$ has the prime divisor 3. $2^{d_2} + 1$ has a divisor that is not 3. Generally, each $d_i > d_{i-1}$ gives us a new primitive divisor that was not in $2^{d_{i-1}} + 1$. Therefore, we have at least 2^n distinct prime divisors. □

Now we prove the theorem.

Proof. Let's assume that these 2^n primes are $q_1, q_2, \ldots, q_{2^n}$. Then,

$$N = q_1 q_2 \ldots q_{2^n} K,$$

for some integer $K \geq 1$. Thus, every divisor of $D = q_1 q_2 \ldots q_{2^n}$ is a divisor of N and so, N has at least 2^{2^n} divisors. □

This theorem can be generalized even more.

Theorem 5.7.11. *Let a, b, n be positive integers with $a \perp b$.*

i. If $3 \nmid n$, $a^n + b^n$ has at least $2^{\tau(n)}$ divisors. That is,

$$\tau(a^n + b^n) \geq 2^{\tau(n)}.$$

ii. If n is odd and $a - b > 1$, $a^n - b^n$ has at least $2^{\tau(n)}$ divisors. That is,

$$\tau(a^n - b^n) \geq 2^{\tau(n)}.$$

Problem 5.7.12 (Romanian TST 1994). Prove that the sequence $a_n = 3^n - 2^n$ contains no three numbers in geometric progression.

Solution. Assume to the contrary, $a_n^2 = a_m a_k$, since they are in geometric progression. So

$$(3^n - 2^n)^2 = (3^k - 2^k)(3^m - 2^m).$$

Since k, m, n are distinct, we must have $k < n < m$. If not, we can not have $n < k < m$ or $n > m > k$ because that would make one side larger. But due to the fact $m > n$, we get that, $3^m - 2^m$ has a prime divisor that does not divide $3^n - 2^n$.

The next problem is taken from the IMO Shortlist.

Problem 5.7.13 (IMO Shortlist 2000). Find all positive integers a, m, and n such that

$$a^m + 1 | (a+1)^n.$$

Solution. Note that $(a, m, n) = (1, m, n)$ is a solution for all m, n. $(a, m, n) = (2, 3, n)$ is a solution for $n > 1$. If $m \neq 3$ and $a, m \geq 2$, then $a^m + 1$ has a prime factor that is not a prime factor of $a + 1$. Therefore, in such cases there are no solutions.

5.8 How to Use Matrices?

Matrices come to the rescue as a useful tool in many problems (for example, in Diophantine equations or representation problems), and contribute a much better and more elegant solution. But since we are not doing a linear algebra course, we will define and discuss only what's required here.

Definition 5.8.1 (Matrix). A *matrix* is a rectangular array which can consist of numbers, variables, or anything. Like a grid, it can have m horizontal *rows* and n vertical *columns*. So, there are mn *cells* in a matrix. Then the matrix is of the size $m \times n$. There are some common notations for denoting matrix. But we will use the usual one:

$$A_{m\times n} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

Here, a_{ij} are the *entries* of the $m \times n$ matrix A. Notice how the index of each entry is written. The entry a_{ij} belongs to the i^{th} row and j^{th} column of the matrix.

Example. Consider the matrices

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \\ 7 & 8 \end{pmatrix}, \qquad C = \begin{pmatrix} -1 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

A is 3×3, B is 4×2, and C is 2×4.

Definition 5.8.2 (Square Matrix). A matrix is *square* if the number of rows is equal to the number of columns, i.e., $m = n$ if the size is $m \times n$. The example above is a square matrix as well.

Definition 5.8.3 (Matrix Diagonals). Let $A_{m\times n}$ be a matrix with entries a_{ij}. The *main diagonal* of A is the collection of entries a_{ij} where $i = j$.

Definition 5.8.4 (Identity Matrix). An square matrix $A_{n\times n}$ is called *identity matrix* and denoted by I_n if entries of its main diagonal equal to one, and all other entries are zero.

Example. Matrix A in the previous example is a square matrix however B and C are not. Moreover, I is an identity matrix of dimension 3, that is, $A = I_3$. The main diagonal of matrix B is formed by the entries $b_{11} = 1$ and $b_{22} = 4$.

Matrices might seem a bit confusing. You might wonder why someone would create matrices, what's wrong with normal numbers? Before giving you an application of where matrices are used, you should know how to do some basic matrix operations.

Definition 5.8.5 (Matrix Addition). The matrix addition is the operation of adding two matrices by adding the corresponding entries together. If A and B are $m \times n$ matrices, then

$$A_{m\times n} + B_{m\times n} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \dots & b_{mn} \end{pmatrix}$$

$$= \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \dots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \dots & a_{2n} + b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \dots & a_{mn} + b_{mn} \end{pmatrix}.$$

Definition 5.8.6 (Matrix Multiplication). Let A be an $m \times n$ matrix and let B be an $n \times P$. The multiplication of A and B is an $m \times p$ matrix C, such that

$$A_{m\times n} \times B_{n\times p} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1p} \\ b_{21} & b_{22} & \dots & b_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{np} \end{pmatrix}$$

$$= \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1p} \\ c_{21} & c_{22} & \dots & c_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \dots & c_{mp} \end{pmatrix},$$

where $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$. We denote this by $AB = C$.

Note. The product AB is defined only if the number of columns in A equals the number of rows in B.

Addition of matrices is easily done by adding corresponding entries. However, the product of two matrices may seem difficult to understand. We will clarify it with an example.

Example. Let

$$A = \begin{pmatrix} 1 & 1 & 5 \\ 2 & 3 & 1 \\ 4 & 6 & 1 \\ 2 & 1 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 3 & 1 & 0 & 2 \\ 5 & 1 & 0 & 1 \\ 4 & 0 & 1 & 1 \end{pmatrix}.$$

A is 4×3 and B is 3×4, so we can multiply them together and the result is a 4×4 matrix. Let's start calculating the product of A and B. Let $AB = C$. We start by finding c_{11}. Note that

$$\begin{pmatrix} \boxed{1 & 1 & 5} \\ 2 & 3 & 1 \\ 4 & 6 & 1 \\ 2 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} \boxed{3} & 1 & 0 & 2 \\ \boxed{5} & 1 & 0 & 1 \\ \boxed{4} & 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} \boxed{c_{11}} & c_{12} & c_{13} & c_{14} \\ c_{21} & c_{22} & c_{23} & c_{24} \\ c_{31} & c_{32} & c_{33} & c_{34} \\ c_{41} & c_{42} & c_{43} & c_{44} \end{pmatrix}.$$

From the definition, the entry c_{11} of C is calculated by multiplying the corresponding entries of first row of A and first column of B (and you can now see why number of columns of A must be equal to the number of rows of B). That is,

$$c_{11} = 1 \cdot 3 + 1 \times 5 + 5 \times 4 = 28.$$

In general, the entry c_{ij} is calculated by multiplying the corresponding entries of i^{th} row of A and j^{th} column of B. Do the product yourself and check the result with the following:

$$C = \begin{pmatrix} 28 & 2 & 5 & 8 \\ 25 & 5 & 1 & 8 \\ 46 & 10 & 1 & 15 \\ 23 & 3 & 3 & 8 \end{pmatrix}.$$

Note. Let A and B be square matrices of the same dimension. Then both AB and BA are defined. However, they are not necessarily equal, i.e., matrix multiplication is not *commutative*.

Definition 5.8.7 (Matrix Powers). For a square matrix $A_{n\times n}$, we define A^2 as the multiplication of A by itself. The definition of all higher powers of A is followed. In fact, $A^k = A \cdot A^{k-1}$, for any positive integer k. We also assume that $A^0 = I_n$, where I_n is the $n-$dimensional identity matrix.

Definition 5.8.8 (Matrix Determinant). A determinant is a real number associated with every square matrix. For a square matrix A, its determinant is denoted by $\det(A)$ or $|A|$.

For the simplest case when A is 1×1 (a single number), the determinant of A equals A, which is sensible (what else would it be?). The definition above is not the exact definition of matrix determinant. We will first explain how to calculate determinant of a 2×2 matrix and then move to the precise definition of determinants.

Definition 5.8.9. Determinant of a 2×2 matrix is the product of entries on its main diagonal minus the product of two other entries. That is, if

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

then $\det(A) = ad - bc$. This is also shown by

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

Example. $\begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} = 4 - 6 = -2.$

We will now generalize the definition of determinant to $n \times n$ matrices. In order for this, you need to know what are cofactors and minors first.

Definition 5.8.10 (Minor). Let A be an $n \times n$ matrix. The *minor* for entry a_{ij} is denoted by M_{ij} and is the determinant that results when the i^{th} row and the j^{th} column of A are deleted.

Example. Let's find M_{21} for the matrix

$$A = \begin{pmatrix} \boxed{1} & 1 & 5 \\ \boxed{2} & \boxed{3} & \boxed{1} \\ \boxed{4} & 6 & 1 \end{pmatrix}.$$

The corresponding row and column (which should be deleted in order to calculate the minor) are shown in the matrix. Therefore, $M_{21} = \begin{vmatrix} 1 & 5 \\ 6 & 1 \end{vmatrix} = 1 - 30 = -29.$

Definition 5.8.11 (Matrix of Minors). Let A be an $n \times n$ matrix. The matrix of minors is an $n \times n$ matrix in which each element is the minor for the corresponding entry of A.

Example. The matrix of minors for matrix A in the previous example is

$$M = \begin{pmatrix} 3-6 & 2-4 & 12-12 \\ 1-30 & 1-20 & 6-4 \\ 1-15 & 1-10 & 3-2 \end{pmatrix} = \begin{pmatrix} -3 & -2 & 0 \\ -29 & -19 & 2 \\ -14 & -9 & 1 \end{pmatrix}.$$

Definition 5.8.12 (Cofactor). The *cofactor* for any entry of a matrix is either the minor or the opposite of the minor, depending on where the element is placed in the original determinant. If the row and column of the entry add up to be an even number, then the cofactor is the same as the minor. If the row and column of the entry add up to be an odd number, then the cofactor is the opposite of the minor.

In other words, if we denote C_{ij} to be the cofactor of the corresponding entry a_i, then $C_{ij} = (-1)^{i+j}M_{ij}$.

Example. You should now be able to make sense of definition of *matrix of cofactors*. The matrix of cofactors of matrix A in previous examples is

$$M = \begin{pmatrix} (-1)^2(3-6) & (-1)^3(2-4) & (-1)^4(12-12) \\ (-1)^3(1-30) & (-1)^4(1-20) & (-1)^5(6-4) \\ (-1)^4(1-15) & (-1)^5(1-10) & (-1)^6(3-2) \end{pmatrix} = \begin{pmatrix} -3 & 2 & 0 \\ 29 & -19 & -2 \\ -14 & 9 & 1 \end{pmatrix}.$$

See the difference between matrix of minors and matrix of cofactors of A.

Now you are ready to see a formula for determinant. Our method is computing larger determinants in terms of smaller ones.

Definition 5.8.13. Given the $n \times n$ matrix A with entries a_{ij}, the determinant of A can be written as the sum of the cofactors of any row or column of A multiplied by the entries that generated them. In other words, the cofactor expansion along the j^{th} column gives

$$\det(A) = a_{1j}C_{1j} + a_{2j}C_{2j} + a_{3j}C_{3j} + \cdots + a_{nj}C_{nj} = \sum_{i=1}^{n} a_{ij}C_{ij}.$$

The cofactor expansion along the i^{th} row gives:

$$\det(A) = a_{i1}C_{i1} + a_{i2}C_{i2} + a_{i3}C_{i3} + \cdots + a_{in}C_{in} = \sum_{j=1}^{n} a_{ij}C_{ij}.$$

Example. Consider the matrix A in the previous examples. If we use the cofactor expansion along the second column, we get

$$\det(A) = a_{12}C_{12} + a_{22}C_{22} + a_{32}C_{32} = 1 \cdot 2 + 3 \cdot (-19) + 6 \cdot 9 = -1.$$

Also, if we use the cofactor expansion along the third row, we get

$$\det(A) = a_{31}C_{31} + a_{32}C_{32} + a_{33}C_{33} = 4 \cdot (-14) + 6 \cdot 9 + 1 \cdot 1 = -1.$$

Note that we used the matrix of cofactors found above for C_{ij}. As you see, the result of both calculations is the same.

If you carefully track what we explained until now, you see that we used the determinant of 2×2 matrices when calculating the matrix of cofactors of A. Then, in order to calculate $\det(A)$, we used some entries of the matrix of cofactors of A. All in all, we have used the determinant of 2×2 matrices when calculating determinant of the 3×3

matrix A. This process is the same for larger matrices. For example, in order to find determinant of a 4×4 matrix, you need to calculate four 3×3 matrices determinants.

Finding the determinant of large matrices (larger than 4×4) is a really boring job and we do not want you to calculate such determinants. You know the basic and you can find determinant of any $n \times n$ matrix. It's just the matter of time it takes to find it.

The definition of determinant may seem useless to you, but it actually is impossible to find the *inverse* of a matrix without knowing its determinant. However, we are not going to introduce inverse matrices. We want to use determinants in a number theorical approach. We will only use the formula for determinant of 2×2 matrices, however we included the definition of determinant so that you can find 3×3 (or even larger) determinants easily.

We state two theorems without proof. If you are interested in seeing a proof, you can read any *linear algebra* book.

Theorem 5.8.14. *Let A and B be $n \times n$ matrices. The product of the determinant of A and B equals the determinant of their product, i.e.,*

$$\det(A \cdot B) = \det(A) \det(B).$$

Theorem 5.8.15. *If $\mathcal{A}$ is a square matrix, then*

$$\mathcal{A}^{m+n} = \mathcal{A}^m \cdot \mathcal{A}^n.$$

Now let's see some of its applications.

Problem 5.8.16 (Fibonacci-Brahmagupta Identity). The sum of two squares is called a *bi-square*. Prove that product of two bi-squares is also a bi-square.

Problem 5.8.17. Let x and y be two integers. Prove that the product of two number of the form $x^2 + dy^2$ is of the same form for a certain d.

Solution. We want to solve this problem using matrices. We already know that

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc, .$$

so we try to represent $x^2 + dy^2$ in the form $ad - bc$, which is determinant of some matrix. This is pretty simple. Assume the matrices

$$\mathcal{M} = \begin{pmatrix} x & yd \\ -y & x \end{pmatrix}, \text{ and } \mathcal{N} = \begin{pmatrix} u & vd \\ -v & u \end{pmatrix}.$$

So $\det(\mathcal{M}) = x^2 + yd^2$ and $\det(\mathcal{N}) = u^2 + dv^2$. Now, we multiply them as explained in Definition (5.8.6) to get

$$\mathcal{M} \cdot \mathcal{N} = \begin{pmatrix} xu - dvy & dvx + duy \\ -(vx + uy) & xu - dvy \end{pmatrix}.$$

Thus, $\det(\mathcal{M} \cdot \mathcal{N}) = (xu - dvy)^2 + d(vx + uy)^2$. Therefore,

$$(x^2 + dy^2)(u^2 + dv^2) = (xu - dvy)^2 + d(vx + uy)^2,$$

which is of the same form.

Problem 5.8.18. Prove that the product of two numbers of the form $x^2 - dy^2$ is again of the same form.

Solution. This is the same as previous one. The only difference is that the matrix would be

$$\mathcal{M} = \begin{pmatrix} x & yd \\ y & x \end{pmatrix}.$$

Problem 5.8.19. Prove that the following equation has infinitely many solutions for integers a, b, c, d, e, and f:

$$(a^2 + ab + b^2)(c^2 + cd + d^2) = (e^2 + ef + f^2).$$

Solution. The following identity gives an infinite family of solutions:

$$(x^2 + x + 1)(x^2 - x + 1) = x^4 + x^2 + 1.$$

But we present a different solution using matrices. In fact, we can prove that for any quartet (a, b, c, d) there are integers e and f such that

$$(a^2 + ab + b^2)(c^2 + cd + d^2) = (e^2 + ef + f^2).$$

Again, we need to choose a suitable matrix to prove our claim. We choose

$$\mathcal{A} = \begin{pmatrix} a & b \\ -b & a+b \end{pmatrix}, \text{ and } \mathcal{B} = \begin{pmatrix} c & d \\ -d & c+d \end{pmatrix}.$$

Afterward process is the same as previous problems.

Note. We could factorize a^2+ab+b^2 as $(a+\zeta b)(a+\zeta^2 b)$, where $\zeta^3 = 1$ is the third root of unity (don't worry if this is unfamiliar for you, it needs some knowledge in complex numbers).

5.8.1 Proving Fibonacci Number Identities

The original Fibonacci sequence F_n is defined by $F_0 = 0$, $F_1 = 1$, and $F_{n+1} = F_n + F_{n-1}$ for $n > 1$. You are familiar with this sequence as it's used in so many cases:

$$0, 1, 1, 2, 3, 5, 8, 13, \ldots$$

We define general Fibonacci numbers G_n by

$$G_0 = a, G_1 = b, \text{ and } G_n = pG_{n-1} + qG_{n-2} \text{ for } n > 1.$$

The matrix representation for this sequence is

$$\begin{pmatrix} p & q \\ 1 & 0 \end{pmatrix} \begin{pmatrix} G_n & G_{n-1} \\ G_{n-1} & G_{n-2} \end{pmatrix} = \begin{pmatrix} G_{n+1} & G_n \\ G_n & G_{n-1} \end{pmatrix}.$$

Special cases are:

1. *Fibonacci* sequence: $a = 0$, and $b = p = q = 1$. The n^{th} term is denoted by F_n.
2. *Lucas* sequence: $a = 2$, and $b = p = q = 1$. The n^{th} term is denoted by L_n.

Theorem 5.8.20.

$$\begin{pmatrix} p & q \\ 1 & 0 \end{pmatrix}^{n-1} \begin{pmatrix} G_2 & G_1 \\ G_1 & G_0 \end{pmatrix} = \begin{pmatrix} G_{n+1} & G_n \\ G_n & G_{n-1} \end{pmatrix}. \tag{5.8}$$

Corollary 5.8.21.

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n} = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}.$$

Proof. We can use induction. It's rather straight-forward. □

Theorem 5.8.22.

$$G_{n+1}G_{n-1} - G_n^2 = (-1)^{n-1}q^{n-1}\left(a^2p + abq - b^2\right).$$

Proof. Take determinant of both sides of equation (5.8). □

Applying the above theorem for Fibonacci and Lucas sequences, we find the following corollaries.

Corollary 5.8.23.

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n.$$

Corollary 5.8.24.

$$L_{n+1}L_{n-1} - L_n^2 = 5 \cdot (-1)^{n-1}.$$

Problem 5.8.25. Prove that

$$F_{m+n+1} = F_{m+1}F_{n+1} + F_mF_n. \tag{5.9}$$

Solution. Consider $I = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Then, $I^{m+n} = I^mI^n$. Note that

$$I^m = \begin{pmatrix} F_{m+1} & F_m \\ F_m & F_{m-1} \end{pmatrix}, I^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}, \text{ and } I^{m+n} = \begin{pmatrix} F_{m+n+1} & F_{m+n} \\ F_{m+n} & F_{m+n-1} \end{pmatrix}.$$

Thus

$$\begin{pmatrix} F_{m+1} & F_m \\ F_m & F_{m-1} \end{pmatrix} \cdot \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} = \begin{pmatrix} F_{m+1}F_{n+1} + F_mF_n & F_{m+1}F_n + F_mF_{n-1} \\ F_mF_{n+1} + F_{m-1}F_n & F_mF_n + F_{m-1}F_{n-1} \end{pmatrix}.$$

We finally find that

$$\begin{pmatrix} F_{m+1}F_{n+1} + F_mF_n & F_{m+1}F_n + F_mF_{n-1} \\ F_mF_{n+1} + F_{m-1}F_n & F_mF_n + F_{m-1}F_{n-1} \end{pmatrix} = \begin{pmatrix} F_{m+n+1} & F_{m+n} \\ F_{m+n} & F_{m+n-1} \end{pmatrix}.$$

Equating the cells of these two matrices, we get

$$F_{m+n+1} = F_{m+1}F_{n+1} + F_mF_n.$$

The following corollaries are immediately concluded.

Corollary 5.8.26.

$$F_{mk+n} = F_{mk+1}F_n + F_{mk}F_{n-1}.$$

Corollary 5.8.27. *Setting $m = n$, we have*

$$F_{2n+1} = F_n^2 + F_{n+1}^2.$$

We end the discussion here, but hopefully you have a better idea of how useful matrix can actually be.

5.9 A Proof for Law of Quadratic Reciprocity

Law of quadratic reciprocity (theorem (2.8.18)) states that for any two different odd primes p and q, we have

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

Mathematicians have provided many proofs for the law of quadratic reciprocity. Gauss himself proved this theorem as well. However, we will be showing arguably the most amazing proof of this theorem, which is due to *Eisenstein*[3]. Before explaining the proof, we should prove two lemmas.

Lemma 5.9.1. *Let p be a prime and let a be an integer co-prime to p. When the numbers $a, 2a, \ldots \frac{p-1}{2}a$ are reduced modulo p into the range from $-\frac{p-1}{2}$ to $\frac{p-1}{2}$, the reduced values are $\pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}$ in some order, with each number appearing once with either a plus sign or a minus sign.*

Proof. We should prove that for any $k, t \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$, the numbers ka and ta are different members of the set $\left\{\pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}\right\}$ when reduced modulo p into the range $-\frac{p-1}{2}$ to $\frac{p-1}{2}$. Assume that $ka \equiv ta \pmod{p}$. Then $a(k-t) \equiv 0 \pmod{p}$ and since $a \perp p$, we get $k - t \equiv 0 \pmod{p}$. But since k and t are both at most $\frac{p-1}{2}$, we should have $k - t = 0$ or $k = t$. On the other hand, if $ak \equiv -at \pmod{p}$, then $k + t \equiv 0 \pmod{p}$. But

$$k + t \leq \frac{p-1}{2} + \frac{p-1}{2} = p - 1,$$

so it's impossible to have $k + t \equiv 0$. This finishes the proof. □

The second lemma uses the definition of $\mu(a, p)$ which we defined in Gauss's Criterion (theorem (2.8.16)).

[3]Do not confuse it with Einstein.

Lemma 5.9.2. *Let p be a prime and let a be an odd integer co-prime to p. Then*

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor \equiv \mu(a,p) \pmod 2.$$

Proof. For each $k \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$, we can write ka as

$$ka = pq_k + r_k, \quad -\frac{p-1}{2} < r_k < \frac{p-1}{2}.$$

Notice that this is different from the normal division (try to see why we can write ka like that). Now divide both sides by p to get

$$\left\lfloor \frac{ka}{p} \right\rfloor = q_k + \left\lfloor \frac{r_k}{p} \right\rfloor, \quad -\frac{1}{2} < \frac{r_k}{p} < \frac{1}{2}.$$

This means that $\left\lfloor \frac{ka}{p} \right\rfloor$ is either q_k (when $r_k > 0$) or $q_k - 1$ (when $r_k < 0$). Adding all the values of $\left\lfloor \frac{ka}{p} \right\rfloor$, we see that

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor = \sum_{k=1}^{\frac{p-1}{2}} q_k - X,$$

where x is the number of negative r_ks. If you look more closely, you see that $X = \mu(a,p)$ (why?), and so

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor = \sum_{k=1}^{\frac{p-1}{2}} q_k - \mu(a,p).$$

We just need to show that $\sum_{k=1}^{\frac{p-1}{2}} q_k$ is an even integer, because then

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor \equiv \sum_{k=1}^{\frac{p-1}{2}} q_k - \mu(a,p) \equiv 0 - \mu(a,p) \equiv \mu(a,p) \pmod 2,$$

which is just what we want. The trick is to write the equation $ka = pq_k + r_k$ modulo 2. Since both a and p are odd, $ka \equiv k \pmod 2$ and $pq_k \equiv q_k \pmod 2$, and so

$$k \equiv q_k + r_k \pmod 2.$$

Summing over k, we see that

$$\sum_{k=1}^{\frac{p-1}{2}} k \equiv \sum_{k=1}^{\frac{p-1}{2}} q_k + \sum_{k=1}^{\frac{p-1}{2}} r_k \pmod 2.$$

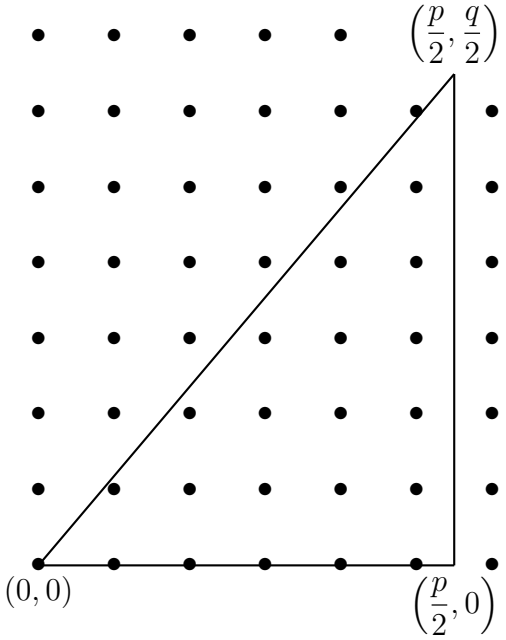
From lemma (5.9.1), we see that the numbers $r_1, r_2, \ldots, r_{\frac{p-1}{2}}$ are equal to the numbers $\pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}$ in some order, with each number appearing once with either a plus sign or a minus sign. We also know that $x \equiv -x \pmod 2$ for any integer x. So, we can say that

$$\sum_{k=1}^{\frac{p-1}{2}} r_k \equiv \sum_{k=1}^{\frac{p-1}{2}} k \pmod 2 \implies \sum_{k=1}^{\frac{p-1}{2}} q_k \equiv 0 \pmod 2.$$

The proof is complete. □

We are now ready to provide a proof for the law of quadratic reciprocity.

Proof of law of quadratic reciprocity. This proof is based on geometry, and that's interesting. Consider a triangle in the xy-plane with vertices on $(0,0), (p/2, 0)$, and $(p/2, q/2)$.

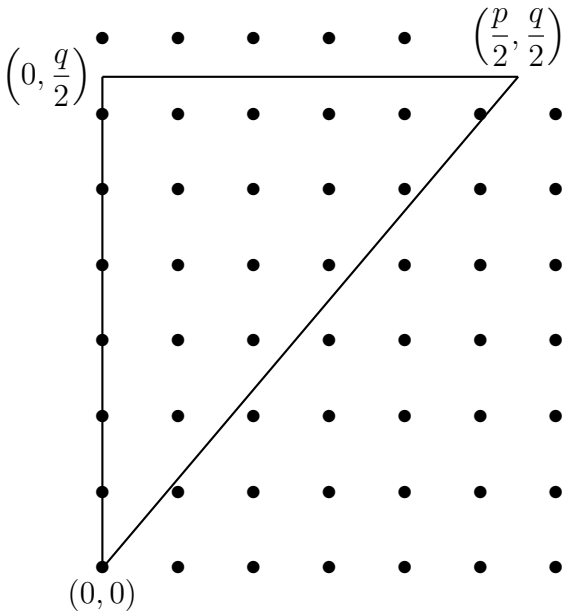


The number of points with integer coordinates inside this triangle equals

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor.$$

You can easily verify this by using the fact that the hypotenuse of triangle lies on the line $y = \frac{q}{p}x$, and so the number of points with $x = k$ (where $1 \leq k \leq \frac{p-1}{2}$) inside the triangle equals $\left\lfloor \frac{kq}{p} \right\rfloor$ (actually, we are counting the points vertically).

Now consider the triangle with vertices on $(0,0), (0, q/2)$, and $(p/2, q/2)$.



We can find the number of points with integer coordinates inside this triangle in a similar way to the previous one. This time, count the points horizontally and sum up the number of points with $y = 1, y = 2, \ldots$, and $y = \frac{p-1}{2}$. The result is

$$\sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor.$$

Now put these two triangles together to form a rectangle with vertices on $(0, 0)$, $(0, q/2)$, $(p/2, 0)$, and $(p/2, q/2)$.

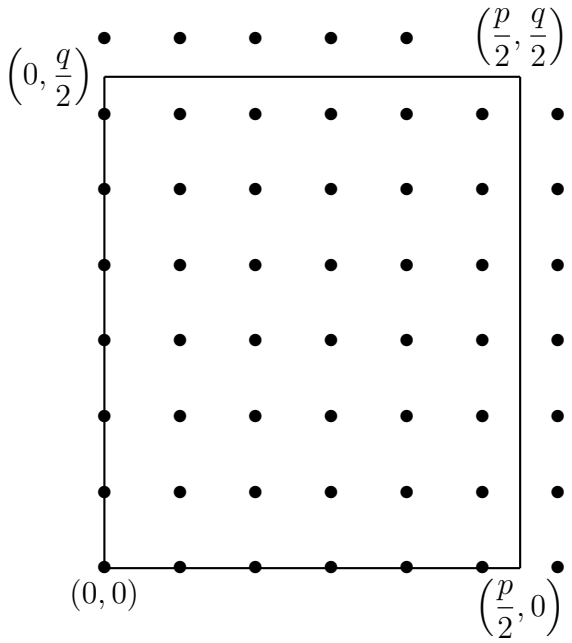
Let x be number of the points with integer coordinates inside this rectangle. Obviously, x is equal to the sum of such points in triangles (notice that since p and q are different, there is no point with integer coordinates on the hypotenuse of triangles). So

$$x = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor.$$

According to lemma (5.9), it follows that

$$x \equiv \mu(q, p) + \mu(p, q) \pmod 2. \tag{5.10}$$

Let's count x in another way.



Clearly, number of points with integer coordinates inside this rectangle is

$$x = \left\lfloor \frac{p}{2} \right\rfloor \cdot \left\lfloor \frac{q}{2} \right\rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2}. \tag{5.11}$$

Combining equations (5.10) and (5.11),

$$\mu(q,p) + \mu(p,q) \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} \pmod 2.$$

Now apply Gauss's criterion to finish the proof:

$$\begin{aligned} \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^{\mu(p,q)} \cdot (-1)^{\mu(q,p)} \\ &= (-1)^{\mu(p,q)+\mu(q,p)} \\ &= (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}. \end{aligned}$$

□

5.10 Darij-Wolstenholme Theorem

The following theorem is a generalization of Wolstenholme's theorem. It was proposed and proved by Darij Grinberg on the *Art of Problem Solving* website. Before stating the theorem, we need to define $v_p(x)$ for a rational number x.

Recall section (3.2.2) where we defined $v_p(x)$ for x being an *integer* as the greatest power of p which divides x. Now, since we are working with fractions, we need to generalize this concept to include rational numbers.

Definition 5.10.1. Let p be a prime and let $x = \frac{a}{b} \neq 0$ be a rational number reduced to lowest terms. Define the *p-adic evaluation of* x as $v_p(x) = v_p(a) - v_p(b)$, where $v_p(n)$ is the notation defined in definition (3.2.12).

Example. $v_3\left(\frac{9}{16}\right) = 2$, and $v_5\left(\frac{34}{25}\right) = -2$.

Note. We can easily check the sign of $v_p(x)$ for any rational number $x = \frac{a}{b}$. If $p|a$, then $v_p(x) > 0$. If p divides none of a and b, then $v_p(x) = 0$. And if $p|b$, then $v_p(x) < 0$. Also, $v_p(xy) = v_p(x) + v_p(y)$ and $v_p(x+y) \geq \min(v_p(x), v_p(y))$ for all rationals x and y.

We can now generalize the concept of congruency to include rational numbers.

Definition 5.10.2. If x and y are two rational numbers such that $v_p(x) \geq 0$ and $v_p(y) \geq 0$, then we say that $x \equiv y \pmod{p}$ if and only if $v_p(x-y) > 0$.

The following problem gives you a good sight of the above notation.

Problem 5.10.3. Let $p \geq 3$ be a prime. Prove that $p|2^{p-2} + 3^{p-2} + 6^{p-2} - 1$.

Solution. Let $a \perp p$ be an integer. We can write $a^{p-2} \equiv \frac{1}{a} \pmod{p}$ because

$$v_p\left(a^p - \frac{1}{a}\right) = v_p\left(\frac{a^{p-1}-1}{a}\right) > 0$$

by Fermat's little theorem. Now

$$2^{p-2} + 3^{p-2} + 6^{p-2} - 1 \equiv \frac{1}{2} + \frac{1}{3} + \frac{1}{6} - 1 \equiv 0 \pmod{p}.$$

Theorem 5.10.4 (Darij-Wolstenholme Theorem). *Let $p > 3$ be a prime and let u be a non-negative and odd integer such that $p \geq u + 3$. Then*

$$v_p\left(\sum_{k=1}^{p-1} \frac{1}{k^u}\right) \geq 2.$$

The idea of the proof is similar to the proof of Wolstenholme's theorem. We need to prove a lemma first.

Lemma 5.10.5. *Let p be a prime and let n be an integer such that $1 \leq n \leq p-2$. Then*

$$\sum_{k=1}^{p-1} k^n \equiv 0 \pmod{p}.$$

Proof. There exists an integer a co-prime to p such that $p \nmid a^n - 1$. The set $A = \{0, 1^n, 2^n, \ldots, (p-1)^n\}$ forms a compete residue system modulo p (why?). Proposition (2.3.4) says that the set $B = \{0, a^n, (2a)^n, \ldots, ((p-1)a)^n\}$ also forms a complete residue system modulo p. Therefore, the sum of elements of both sets are equivalent modulo p. So

$$\sum_{k=1}^{p-1} k^n \equiv \sum_{k=1}^{p-1} (a \cdot k)^n \equiv a^n \sum_{k=1}^{p-1} k^n \pmod{p}.$$

This means that

$$\left(a^k-1\right)\sum_{k=1}^{p-1}k^n\equiv 0 \pmod p,$$

and since $p\nmid a^n-1$, we should have

$$\sum_{k=1}^{p-1}k^n\equiv 0 \pmod p.$$

If the proof seemed confusing to you, here is a potentially better version. Consider a primitive root g of p (we already know there is one from modular arithmetic chapter). Then we also know that $\{1,2,\ldots,p-1\}$ can be generated by g (the set $\{1,g,g^2,\ldots,g^{p-2}\}$). So,

$$\begin{aligned}1^n+2^n+\cdots+(p-1)^n &= 1^n+g^n+g^{2n}+\cdots+\left(g^{p-2}\right)^n\\ &= \frac{(g^n)^{p-1}-1}{g^n-1}\\ &= \frac{g^{(p-1)n}-1}{g^n-1}\end{aligned}$$

From Fermat's little theorem, $g^{p-1}\equiv 1 \pmod p$, so the conclusion follows. □

Proof of Darij-Wolstenholme Theorem. The idea is to use the trick explained in lemma (2.9.4). That is, we write the given sum as a sum of terms of the form $\frac{1}{k^u}+\frac{1}{(p-k)^u}$. We have

$$\begin{aligned}2\sum_{k=1}^{p-1}\frac{1}{k^u} &= \sum_{k=1}^{p-1}\frac{1}{k^u}+\sum_{k=1}^{p-1}\frac{1}{(p-k)^u}\\ &= \sum_{k=1}^{p-1}\left(\frac{1}{k^u}+\frac{1}{(p-k)^u}\right)\\ &= \sum_{k=1}^{p-1}\frac{k^u+(p-k)^u}{k^u(p-k)^u}\\ &= \sum_{k=1}^{p-1}\frac{k^u+(p^u-up^{u-1}k+\cdots+upk^{u-1}-k^u)}{k^u(p-k)^u}\\ &= \sum_{k=1}^{p-1}\frac{p^u-up^{u-1}k+\cdots+upk^{u-1}}{k^u(p-k)^u}\\ &= p\cdot\sum_{k=1}^{p-1}\frac{p^{u-1}-up^{u-2}k+\cdots+uk^{u-1}}{k^u(p-k)^u}.\end{aligned}$$

We have used the fact that u is an odd integer to expand $(p-k)^u$ in above lines. Now since $p>3$ is an odd prime, $v_p(2)=0$ and therefore

$$\begin{aligned} v_p\left(2\sum_{k=1}^{p-1}\frac{1}{k^u}\right) &= v_p(2)+v_p\left(\sum_{k=1}^{p-1}\frac{1}{k^u}\right) = v_p\left(\sum_{k=1}^{p-1}\frac{1}{k^u}\right) \\ &= v_p\left(p\cdot\sum_{k=1}^{p-1}\frac{p^{u-1}-up^{u-2}k+\cdots+uk^{u-1}}{k^u(p-k)^u}\right) \\ &= v_p(p)+v_p\left(\sum_{k=1}^{p-1}\frac{p^{u-1}-up^{u-2}k+\cdots+uk^{u-1}}{k^u(p-k)^u}\right) \\ &= 1+v_p\left(\sum_{k=1}^{p-1}\frac{p^{u-1}-up^{u-2}k+\cdots+uk^{u-1}}{k^u(p-k)^u}\right). \end{aligned}$$

So instead of showing $v_p\left(2\sum_{k=1}^{p-1}\frac{1}{k^u}\right)\geq 2$, it is enough to show that

$$v_p\left(\sum_{k=1}^{p-1}\frac{p^{u-1}-up^{u-2}k+\cdots+uk^{u-1}}{k^u(p-k)^u}\right)\geq 1,$$

which is equivalent to showing that

$$\sum_{k=1}^{p-1}\frac{p^{u-1}-up^{u-2}k+\cdots+uk^{u-1}}{k^u(p-k)^u}\equiv 0 \pmod p.$$

Since $p^{u-1}-up^{u-2}k+\cdots+uk^{u-1}\equiv uk^{u-1} \pmod p$ and $k^u(p-k)^u\equiv k^u(-k)^u\equiv(-1)^uk^{2u} \pmod p$, we should prove that

$$\sum_{k=1}^{p-1}\frac{uk^{u-1}}{(-1)^uk^{2u}}\equiv\frac{u}{(-1)^u}\sum_{k=1}^{p-1}k^{-u-1}\equiv 0 \pmod p.$$

From Fermat's little theorem, we have $k^{p-1}\equiv 1 \pmod p$ for every k such that $1\leq k\leq p-1$. So $k^{-u-1}\equiv k^{-u-1}k^{p-1}=k^{p-u-2} \pmod p$ and we must prove that

$$\frac{u}{(-1)^u}\sum_{k=1}^{p-1}k^{p-u-2}\equiv 0 \pmod p,$$

which follows directly from lemma (5.10.5) because $1\leq p-u-2\leq p-2$. The proof is complete. □

Problem 5.10.6. Let $p>3$ be a prime. Prove that

$$\sum_{i=1}^{\lfloor 2p/3\rfloor}\frac{(-1)^{i-1}}{i}\equiv 0 \pmod p.$$

Solution. First, let us prove that

$$p - \lfloor \lfloor 2p/3 \rfloor /2 \rfloor = \lfloor 2p/3 \rfloor + 1, \tag{5.12}$$

where $\lfloor x \rfloor$ is the largest integer not greater than x for any real x. Since $p > 3$, either $p \equiv 1 \pmod 3$ or $p \equiv 2 \pmod 3$. Consider both cases:

- If $p \equiv 1 \pmod 3$, then $\frac{p-1}{3}$ is an integer and

$$2 \cdot \frac{p-1}{3} \leq \frac{2p}{3} < 2 \cdot \frac{p-1}{3} + 1,$$

which means

$$\left\lfloor \frac{2p}{3} \right\rfloor = 2 \cdot \frac{p-1}{3},$$
$$\left\lfloor \left\lfloor \frac{2p}{3} \right\rfloor /2 \right\rfloor = \left\lfloor \left(2 \cdot \frac{p-1}{3} \right) /2 \right\rfloor = \frac{p-1}{3}.$$

Finally,

$$p - \left\lfloor \left\lfloor \frac{2p}{3} \right\rfloor /2 \right\rfloor = p - \frac{p-1}{3} = 2 \cdot \frac{p-1}{3} + 1 = \left\lfloor \frac{2p}{3} \right\rfloor + 1,$$

as desired.

- If $p \equiv 2 \pmod 3$, then $\frac{p-2}{3}$ is an integer and

$$2 \cdot \frac{p-2}{3} + 1 \leq \frac{2p}{3} < \left(2 \cdot \frac{p-2}{3} + 1 \right) + 1.$$

This gives

$$\left\lfloor \frac{2p}{3} \right\rfloor = 2 \cdot \frac{p-2}{3} + 1,$$
$$\left\lfloor \left\lfloor \frac{2p}{3} \right\rfloor /2 \right\rfloor = \left\lfloor \left(2 \cdot \frac{p-2}{3} + 1 \right) /2 \right\rfloor = \left\lfloor \frac{p-2}{3} + \frac{1}{2} \right\rfloor = \frac{p-2}{3}.$$

And finally

$$p - \left\lfloor \left\lfloor \frac{2p}{3} \right\rfloor /2 \right\rfloor = p - \frac{p-2}{3} = \left(2 \cdot \frac{p-2}{3} + 1 \right) + 1 = \left\lfloor \frac{2p}{3} \right\rfloor + 1.$$

The proof of equation (5.12) is finished. We will now prove the problem. Obviously,

$$\begin{aligned}
\sum_{i=1}^{\lfloor 2p/3\rfloor}\frac{(-1)^{i-1}}{i} &= \sum_{\substack{1\le i\le\lfloor 2p/3\rfloor;\\ i \text{ is odd}}}\frac{1}{i}+\sum_{\substack{1\le i\le\lfloor 2p/3\rfloor;\\ i \text{ is even}}}\frac{-1}{i}\\
&= \sum_{\substack{1\le i\le\lfloor 2p/3\rfloor;\\ i \text{ is odd}}}\frac{1}{i}-\sum_{\substack{1\le i\le\lfloor 2p/3\rfloor;\\ i \text{ is even}}}\frac{1}{i}\\
&= \left(\sum_{\substack{1\le i\le\lfloor 2p/3\rfloor;\\ i \text{ is odd}}}\frac{1}{i}+\sum_{\substack{1\le i\le\lfloor 2p/3\rfloor;\\ i \text{ is even}}}\frac{1}{i}\right)-2\sum_{\substack{1\le i\le\lfloor 2p/3\rfloor;\\ i \text{ is even}}}\frac{1}{i}\\
&= \sum_{i=1}^{\lfloor 2p/3\rfloor}\frac{1}{i}-2\sum_{\substack{1\le i\le\lfloor 2p/3\rfloor;\\ i \text{ is even}}}\frac{1}{i}\\
&= \sum_{i=1}^{\lfloor 2p/3\rfloor}\frac{1}{i}-2\sum_{j=1}^{\lfloor\lfloor 2p/3\rfloor/2\rfloor}\frac{1}{2j}\\
&= \sum_{i=1}^{\lfloor 2p/3\rfloor}\frac{1}{i}+\sum_{j=1}^{\lfloor\lfloor 2p/3\rfloor/2\rfloor}\frac{1}{-j}\\
&\equiv \sum_{i=1}^{\lfloor 2p/3\rfloor}\frac{1}{i}+\sum_{j=1}^{\lfloor\lfloor 2p/3\rfloor/2\rfloor}\frac{1}{p-j} \pmod p.
\end{aligned}$$

In the second sum in the last line of above equations, we have used the fact that $-j\equiv p-j \pmod p$. Replacing j by $p-i$ in the second sum, we have

$$\sum_{i=1}^{\lfloor 2p/3\rfloor}\frac{(-1)^{i-1}}{i}\equiv\sum_{i=1}^{\lfloor 2p/3\rfloor}\frac{1}{i}+\sum_{i=p-\lfloor\lfloor 2p/3\rfloor/2\rfloor}^{p-1}\frac{1}{i}.$$

Using (5.12), we can write $i=p-\lfloor\lfloor 2p/3\rfloor/2\rfloor=\lfloor 2p/3\rfloor+1$ and so by Wolstenholme's theorem,

$$\begin{aligned}
\sum_{i=1}^{\lfloor 2p/3\rfloor}\frac{(-1)^{i-1}}{i} &\equiv \sum_{i=1}^{\lfloor 2p/3\rfloor}\frac{1}{i}+\sum_{i=\lfloor 2p/3\rfloor+1}^{p-1}\frac{1}{i}\\
&\equiv \sum_{i=1}^{p-1}\frac{1}{i} \pmod p\\
&\equiv 0 \pmod p.
\end{aligned}$$

This finishes the proof of the problem.

5.11 Generalization of Wilson's and Lucas' Theorem

Wilson's theorem says that $(p-1)! \equiv -1 \pmod{p}$ for all primes p. Clearly, for any integer n larger than p, we have $n! \equiv 0 \pmod{p}$. Now, if we remove the multiples of p from $n!$ and then calculate the result modulo p, what would it be? We will state this as a generalization for Wilson's theorem. But first, some definitions and lemmas.

Definition 5.11.1. Let n be a positive integer and p a prime number. The *p-reduced factorial of n* is the product of all positive integers less than or equal to n which are not divisible by p. We denote this by $(n!)_p$.

Example. The 5-reduced factorial of 10, $(10!)_5$, is

$$(10!)_5 = 9 \times 8 \times 7 \times 6 \times 4 \times 3 \times 2 \times 1 = 72,576.$$

Theorem 5.11.2. *Let p be a prime number and let $(n_k n_{k-1} \dots n_1 n_0)_p$ be a positive integer. Then*

$$(n!)_p \equiv (-1)^{\left[\frac{n}{p}\right]} \cdot n_0! \pmod{p}.$$

Proof. The numbers not divisible by p among $1, 2, \dots, n$ are

$$\begin{array}{ccccccc}
1 & 2 & \cdots & n_0 & \cdots & p-1 \\
p+1 & p+2 & \cdots & p+n_0 & \cdots & 2p-1 \\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
(\left[\frac{n}{p}\right]-1)p+1 & (\left[\frac{n}{p}\right]-1)p+2 & \cdots & (\left[\frac{n}{p}\right]p-1)p+n_0 & \cdots & \left[\frac{n}{p}\right]p-1 \\
\left[\frac{n}{p}\right]p+1 & \left[\frac{n}{p}\right]p+2 & \cdots & \left[\frac{n}{p}\right]p+n_0 & &
\end{array}$$

Product of these numbers, $(n!)_p$ is

$$\left(\prod_{k=0}^{\left[\frac{n}{p}\right]-1} \big((kp+1)\cdot(kp+2)\cdots(kp+p-1)\big) \right) \cdot \big(\left[\tfrac{n}{p}\right]p+1\big)\big(\left[\tfrac{n}{p}\right]p+2\big)\dots\big(\left[\tfrac{n}{p}\right]p+n_0\big),$$

which is equal to

$$\begin{aligned}
&= \left(\prod_{k=0}^{\left[\frac{n}{p}\right]-1} \big(1\cdot 2\cdots(p-1)\big) \right) \cdot \big(\left[\tfrac{n}{p}\right]p+1\big)\big(\left[\tfrac{n}{p}\right]p+2\big)\dots\big(\left[\tfrac{n}{p}\right]p+n_0\big) \\
&\equiv \left(\prod_{k=0}^{\left[\frac{n}{p}\right]-1} (-1) \right) \cdot (1\cdot 2\cdots n_0) \\
&\equiv (-1)^{\left[\frac{n}{p}\right]} n_0! \pmod{p}.
\end{aligned}$$

□

Proposition 5.11.3. *Let $p \geq 3$ be a prime and n be a positive integer. Then*

$$(p^n!)_p \equiv -1 \pmod{p^n}.$$

Proof. This is exactly the same as the proof of Wilson's theorem. All numbers in the product $(p^n!)_p$ have a multiplicative inverse modulo p^n. If the inverse of a number a among these numbers is $b \neq a$, then $ab \equiv 1 \pmod{p^n}$ and we can remove a and b from the product $(p^n!)_p$. Our only concern is when the inverse of a equals a itself. But if that's the case, we have

$$a^2 \equiv 1 \pmod{p^n} \implies p^n | (a-1)(a+1).$$

But since $(a-1, a+1) = 2$, we should have $a \equiv \pm 1 \pmod{p^n}$, which means a is either 1 or $p^n - 1$. All in all, we see that the product of all numbers in $(p^n!)_p$ except $p^n - 1$ equals 1 modulo p^n, and if we multiply this number by $p^n - 1$, the result will be -1 modulo p^n. □

Problem 5.11.4. Prove that $(2^n!)_2 \equiv 1 \pmod{2^n}$.

We are ready to prove the following theorem.

Theorem 5.11.5 (Generalization of Wilson's Theorem). *Let p be a prime number and let $(n_k n_{k-1} \dots n_1 n_0)_p$ be the representation of a positive integer n in base p. Then*

$$\frac{n!}{p^{v_p(n!)}} \equiv (-1)^{v_p(n!)} n_0! n_1! \dots n_k! \pmod{p}. \tag{5.13}$$

Proof. According to theorem (5.11.2), one can write

$$\begin{aligned} n! &= (n!)_p \cdot p^{\lfloor n/p \rfloor} \left(\left\lfloor \frac{n}{p} \right\rfloor \right)! \\ &\equiv (-1)^{\lfloor n/p \rfloor} n_0! \cdot p^{\lfloor n/p \rfloor} \left(\left\lfloor \frac{n}{p} \right\rfloor \right)!. \end{aligned}$$

Now write $(\lfloor \frac{n}{p} \rfloor)!$ in the same way and continue this process. The result is concluded. □

Note. If you are interested, you can find a (different) generalization of Wilson's theorem in Problem 2.12.23.

Theorem 5.11.6 (Generalization of Lucas' Theorem). *Let p be a prime number and m, n, and r be non-negative integers such that $r = m - n$ and*

$$\begin{aligned} m &= m_k p^k + m_{k-1} p^{k-1} + \dots + m_1 p + m_0, \\ n &= k_k p^k + n_{k-1} p^{k-1} + \dots + n_1 p + n_0, \\ r &= r_k p^k + r_{k-1} p^{k-1} + \dots + r_1 p + r_0. \end{aligned}$$

Also, let $\ell = v_p\left(\binom{m}{n}\right)$. Then

$$\frac{1}{p^\ell} \binom{m}{n} \equiv (-1)^\ell \left(\frac{m_0!}{n_0! r_0!} \right) \left(\frac{m_1!}{n_1! r_1!} \right) \dots \left(\frac{m_d!}{n_d! r_d!} \right) \pmod{p}.$$

Proof. Note that

$$\begin{aligned}\ell = v_p\left(\binom{m}{n}\right) &= v_p\left(\frac{m!}{n!r!}\right) = v_p(n!) - v_p(n!) - v_p(r!)\\ &= \sum_{i=1}^{k}\left\lfloor\frac{m}{p^i}\right\rfloor - \sum_{i=1}^{k}\left\lfloor\frac{n}{p^i}\right\rfloor - \sum_{i=1}^{k}\left\lfloor\frac{r}{p^i}\right\rfloor\\ &= \sum_{i=1}^{k}\left(\left\lfloor\frac{m}{p^i}\right\rfloor - \left\lfloor\frac{n}{p^i}\right\rfloor - \left\lfloor\frac{r}{p^i}\right\rfloor\right).\end{aligned}$$

Just like the proof of theorem (5.11.5), we can write

$$\binom{m}{n} = \frac{(m!)_p}{(n!)_p(r!)_p}\cdot\frac{p^{\lfloor m/p\rfloor}}{p^{\lfloor n/p\rfloor}\cdot p^{\lfloor r/p\rfloor}}\cdot\frac{\left\lfloor\frac{m}{p}\right\rfloor!}{\left\lfloor\frac{n}{p}\right\rfloor!\cdot\left\lfloor\frac{r}{p}\right\rfloor!}.$$

Use induction and generalization of Wilson's theorem to finish the proof. □

5.12 Inverse of Euler's Totient Function

For a given positive integer n, we can find $\varphi(n)$ after factorizing n. What about the reverse problem? That is, given $\varphi(n)$, can you find n? A more interesting question is whether this solution n is unique or there are other solutions. We can answer the latter question pretty quickly using an example: $\varphi(4) = 2$ and $\varphi(6) = 2$. In other words, φ is not a one to one function. Now, another question normally arises here:

Problem 5.12.1. Is there any $n \in \mathbb{N}$ such that $\varphi(x) = n$ has a unique solution for x?

There are good results on this topic. It has also been studied how to find such x, and the upper or lower bounds of x. Here we will discuss some of the results, which fits into our book.

Definition 5.12.2 (Inverse Phi). Let n be a positive integer. Assume that $\varphi^{-1}(n)$ is the *set* of all possible values of $x \in \mathbb{N}$ such that $\varphi(x) = n$. In other words,

$$\varphi^{-1}(n) = \{x : \varphi(x) = n\}.$$

We call $\varphi^{-1}(n)$ the *inverse of Euler's totient function*, or simply the *inverse of phi function*. Moreover, for ever positive integer x, we define $N(x)$ to be the number of positive integers y such that $\varphi(x) = \varphi(y)$.

Carmichael stated in [2] that the cardinality (number of elements) of $\varphi^{-1}(n)$ is always greater than 1 but due to his proof being inadequate, this is a conjecture now:

Conjecture 5.1 (Carmichael's Totient Conjecture). *For a positive integer n, the number of solutions to $\varphi(x) = n$ is either 0 or at least 2.*

After this statement, quite a lot of number theorists worked on it. There has been no proof of the theorem to our knowledge, though there are some nice results on it. And it is indeed a very interesting topic to work on. Even though it is a conjecture, everything points this to be true. For example, *Klee* pointed out in [4] that if $N(x) = 1$ then x and $\varphi(x)$ are both larger than 10^{400}. Carmichael originally proved that $x > 10^{37}$ must be true. Let's start investigating $N(x)$.

Theorem 5.12.3. *Let x be a positive integer. If $N(x) = 1$, then x is divisible by 4.*

Proof. For $n > 2$, $\varphi(n)$ is always even. If x is odd, then $2 \perp x$ so $\varphi(2x) = \varphi(x)$ so $y = 2x$ is a solution, so contradiction. Again, if $x = 2t$ with t odd then $\varphi(x) = \varphi(t)$ by same argument. Thus, x is divisible by 4. □

The following theorem is due to Carmichael.

Theorem 5.12.4. *Let x be a positive integer and let $p = 2^k + 1$ be a prime divisor of x, where k is some natural number. If $N(x) = 1$, then $p^2|x$.*

Proof. To the contrary, assume that $x = 2^e ps$ for some positive integers e and s with $s \perp 2p$. Then,

$$\begin{aligned}\varphi(x) &= \varphi(2^e)\varphi(p)\varphi(s) \\ &= 2^{e-1}2^k\varphi(s) \\ &= \varphi(2^{k+e})\varphi(s) \\ &= \varphi(2^{k+e}s).\end{aligned}$$

Thus, $y = 2^{k+e}s \neq x$ satisfies the condition, so we must have $p|s$ and hence $p^2|x$. □

Here is a very nice result that provides us with a sufficient condition for $N(x) = 1$ to happen.. The result is due to C. Pomerance [3].

Theorem 5.12.5 (Carl Pomerance). *Let x be a positive integer. Suppose that the following property holds for every prime p:*

$$p - 1|\varphi(x) \text{ implies } p^2|x.$$

Then $N(x) = 1$. That is, if $\varphi(y) = \varphi(x)$ for some positive integer y, then $y = x$.

Proof. For every positive integer n, define $S(n)$ to be the set of prime divisors of n. If the prime factorization of n is $\prod_{i=1}^{r} p_i^{e_i}$, then

$$\varphi(n) = \prod_{i=1}^{r} p_i^{e_i-1}(p_i - 1).$$

According to our assumption, x is a positive integer such that if $p - 1|\varphi(x)$ then $p^2|x$. We are required to prove that under this assumption, if $\varphi(x) = \varphi(y)$ then $x = y$ must hold. If $p \in S(y)$ then $p - 1|\varphi(y) = \varphi(x)$. So, from the assumption, $p^2|x$ for any prime p in $S(y)$. This gives us $S(y) \subseteq S(x)$.

We will investigate the exponent of a prime p in $\varphi(n)$. There are two cases:

1. p divides n. Suppose that $p^e \| n$. Then we have $p^{e-1} | \varphi(n)$. But is this the highest exponent possible? No. Because in the factorization of $\varphi(n)$, there are factors of the form $(q-1)$ for any other prime divisor q of n. If $p|q-1$ for any such q, those will contribute to $v_p(\varphi(n))$ as well. That is,

$$v_p(\varphi(n)) = v_p(n) - 1 + \sum_{q \in S(n)} v_p(q-1).$$

2. p does not divide n. In this case, only factors of the form $(q-1)$ for any prime divisor q of n may contribute to $v_p(\varphi(n))$. In other words,

$$v_p(\varphi(n)) = \sum_{q \in S(n)} v_p(q-1).$$

Combining these two results, we find out that for any prime p and any positive integer n,

$$v_p(\varphi(n)) = \begin{cases} \displaystyle\sum_{q \in S(n)} v_p(q-1), & \text{if } p \nmid n, \\ \displaystyle v_p(n) - 1 + \sum_{q \in S(n)} v_p(q-1), & \text{otherwise.} \end{cases}$$

Let p be a prime factor of x. Since $\varphi(x) = \varphi(y)$, for any prime p, we must have

$$v_p(\varphi(x)) = v_p(\varphi(y)).$$

There are two cases to consider.

1. $p \notin S(y)$ or $p \nmid y$. Then,

$$\begin{aligned} v_p(x) - 1 + \sum_{q \in S(x)} v_p(q-1) &= \sum_{q \in S(y)} v_p(q-1) \\ &\leq \sum_{q \in S(x)} v_p(q-1) \quad \text{since } S(y) \subseteq S(x). \end{aligned}$$

   The latter result implies $v_p(x) \leq 1$. But this is impossible since $v_p(x) \geq 2$ due to the fact that $p^2 | x$.

2. $p \in S(y)$. That is, $p|y$, or $S(x) = S(y)$. In this case we should expect to get $x = y$. One way to prove this is to show that $v_p(x) = v_p(y)$. Notice that

$$\begin{aligned} v_p(x) &= v_p(\varphi(x)) + 1 - \sum_{q \in S(x)} v_p(q-1) \\ &= v_p(\varphi(y)) + 1 - \sum_{q \in S(y)} v_p(q-1) \quad \text{since } \varphi(x) = \varphi(y) \text{ and } S(x) = S(y) \\ &= v_p(y), \end{aligned}$$

which was what we wanted. □

Gupta [5] found upper and lower bounds for $\varphi^{-1}(n)$. For odd n, $\varphi^{-1}(n)$ is empty. Therefore, we only need to consider the case when n is even.

Theorem 5.12.6 (Gupta). *Let m and n be two positive integers such that $n \in \varphi^{-1}(m)$. Then,*

$$m < n \leq m \prod_{p-1|m} \frac{p}{p-1}.$$

Proof. For even n, $m = \varphi(n) < n$ because $\varphi(n) = n$ holds for $n = 1$ only. This proves the lower bound. For the upper bound, we can write

$$\begin{aligned} \frac{n}{\varphi(n)} &= \prod_{p|n} \frac{p}{p-1} \\ &\leq \prod_{p-1|m} \frac{p}{p-1}. \end{aligned}$$

The last line is true because if $p|n$ then $p-1|m$ must hold, but the converse is not true. If $p-1|m$, p may or may not divide n. □

Now we will look at the elements of $\varphi^{-1}(m)$.

Theorem 5.12.7. *Let m be a positive integers and suppose that $\varphi^{-1}(m)$ contains A elements. Then, the number of odd elements of $\varphi^{-1}(m)$ is less than or equal to $A/2$.*

Proof. For a positive integer n, if $\varphi(n) = m$ then $\varphi(2n) = m$ is true as well. Thus, for any odd n, there is an even x which belongs to $\varphi^{-1}(m)$. This proves that the number of odd elements is at most half of the number of elements in $\varphi^{-1}(m)$. □

Theorem 5.12.8. *For a prime p, there exists a positive integer n such that $n \in \varphi^{-1}(2p)$ if and only if $2p+1$ is a prime.*

Proof. The "only if" part is easy to prove. When $q = 2p + 1$ is a prime, $\varphi(q) = 2p$ so $q \in \varphi^{-1}(2p)$.

Now we prove the "if" part. For a positive integer $n \in \varphi^{-1}(m)$, consider that $\varphi(n) = 2p$. In other words, suppose that $n \in \varphi^{-1}(2p)$. If $p = 2$ we see that $n = 5$ works. We need to show it for odd p now.

Suppose that $n = 2^a p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, where $p_1, p_2, \dots, p_k$ are odd primes. Obviously, both a and k cannot be zero at the same time. We have three cases here:

1. If a and k are both non-zero, then

$$\begin{aligned} \varphi(n) &= 2^{a-1} p_1^{e_1-1} p_2^{e_2-1} \dots p_k^{e_k-1} (p_1-1)(p_2-1)\dots(p_k-1) \\ &= 2p. \end{aligned}$$

Notice that $v_2(\varphi(n)) \geq a - 1 + k$ and $v_2(2p) = 1$. Therefore, $a + k - 1 \leq 1$ or $a + k \leq 2$. This gives $a = k = 1$, which means $n = 2p_1$. Then,

$$\begin{aligned} \varphi(n) &= p_1 - 1 \\ &= 2p \\ \implies p_1 &= 2p + 1, \end{aligned}$$

implying $2p + 1$ is a prime.

2. If $a = 0$, then

$$\begin{aligned} \varphi(n) &= p_1^{e_1 - 1} p_2^{e_2 - 1} \dots p_k^{e_k - 1} (p_1 - 1)(p_2 - 1) \dots (p_k - 1) \\ &= 2p. \end{aligned}$$

In this case, $1 = v_2(2p) = v_2(\varphi(n)) \geq k$, and hence $k = 1$ or $n = p_1$. So, $\varphi(n) = p_1 - 1 = 2p$, and $2p + 1$ will be a prime in this case.

3. If $k = 0$, then

$$\begin{aligned} \varphi(n) &= 2^{a-1} \\ &= 2p, \end{aligned}$$

which is not possible.

The proof is complete. □

We leave the following theorems as exercise for the reader.

Theorem 5.12.9. *The number of odd elements in $\varphi^{-1}(2^k)$ is 0 or 1.*

Theorem 5.12.10. *For an odd m, the number of odd elements in $\varphi^{-1}(m)$ is equal to the number of even elements.*

5.13 Exercises

Problem 5.13.1. Let p be a prime number. Prove that there exist integers x and y such that $p = 2x^2 + 3y^2$ if and only if p is congruent to 5 or 11 modulo 24.

Problem 5.13.2 (KöMaL). Prove that the equation $x^3 - x + 9 = 5y^2$ has no solution among the integers.

Problem 5.13.3 (India 1998). If an integer n is such that $7n$ is the form $a^2 + 3b^2$, prove that n is also of that form.

Problem 5.13.4 (USA TST 2017). Prove that there are infinitely many triples (a, b, p) of positive integers with p prime, $a < p$, and $b < p$, such that $(a + b)^p - a^p - b^p$ is a multiple of p^3.

Problem 5.13.5 (Taken from [1]). Let p be a prime other than 7. Prove that the following conditions are equivalent:

1. There exist integers x and y such that $x^2 + 7y^2 = p$.
2. $\left(\frac{-7}{p}\right) = 1$.
3. p is congruent to $1, 2$, or 4 modulo 7.

Problem 5.13.6 (Taken from [1]). Let p be a prime larger than 5. Prove that the following conditions are equivalent:

1. There exist integers x and y such that $x^2 + 6y^2 = p$.
2. p is congruent to 1 or 7 modulo 24.

Problem 5.13.7 (Vietnam TST 1998). Let d be a positive divisor of $5 + 1998^{1998}$. Prove that $d = 2 \cdot x^2 + 2 \cdot x \cdot y + 3 \cdot y^2$, where x, y are integers if and only if d is congruent to 3 or 7 (mod 20).

Problem 5.13.8 (Romania TST 1997). Let A be the set of positive integers of the form $a^2 + 2b^2$, where a and b are integers and $b \neq 0$. Show that if p is a prime number and $p^2 \in A$, then $p \in A$.

Problem 5.13.9 (India TST 2003). On the real number line, paint red all points that correspond to integers of the form $81x + 100y$, where x and y are positive integers. Paint the remaining integer point blue. Find a point P on the line such that, for every integer point T, the reflection of T with respect to P is an integer point of a different color than T.

Problem 5.13.10 (USAMO 2001). Let S be a set of integers (not necessarily positive) such that

1. there exist $a, b \in S$ with $\gcd(a, b) = \gcd(a - 2, b - 2) = 1$;

2. if x and y are elements of S (possibly equal), then $x^2 - y$ also belongs to S.

Prove that S is the set of all integers.

Problem 5.13.11. Let a, b, and n be positive integers such that $n > 2$. Prove that if

$$k = \frac{a^n + b^n}{(ab)^{n-1} + 1}$$

is an integer, then k is a perfect n^{th} power.

Problem 5.13.12 (IZHO 2005). Solve the equation $p^2 - 6pq + (q^2 + 4) = 0$ in prime numbers less than 2005.

Problem 5.13.13. Let a, b, and k be positive integers such that

$$k = \frac{a^2 + b^2}{ab - 1}$$

Prove that $k = 5$.

Problem 5.13.14 (IMO 2007). Let a and b be positive integers. Show that if $4ab - 1$ divides $(4a^2 - 1)^2$, then $a = b$.

Problem 5.13.15 (PEN). If a, b, c are positive integers such that

$$0 < a^2 + b^2 - abc \leq c,$$

show that $a^2 + b^2 - abc$ is a perfect square.

Problem 5.13.16 (IMO ShortList 2003). Determine all pairs of positive integers (a, b) such that

$$\frac{a^2}{2ab^2 - b^3 + 1}$$

is a positive integer.

Problem 5.13.17. Find all triples (x, y, z) of positive integers such that $(x+y+z)^2 = 7xyz$.

Problem 5.13.18. Let a and b be positive integers such that ab divides $a^2 + b^2 + 2$. Prove that $\frac{a^2+b^2+2}{ab} = 4$.

Problem 5.13.19. Find all positive integers x, y, and z such that $x^2 + y^2 + 2 = xyz$.

Problem 5.13.20 (Ireland 2005). Let m, n be integers with the same parity such that $m^2 - n^2 + 1$ divides $n^2 - 1$. Prove that $m^2 - n^2 + 1$ is a perfect square.

Problem 5.13.21 (Mongolia 2000). For which positive integer k there exist positive integers x, y, and z such that $(x + y + z)^2 = kxyz$?

Problem 5.13.22. Prove that the following equation has no positive integer solution (x, y, z)

$$x^2 + y^2 + z^2 = xyz + 1.$$

Problem 5.13.23. Prove that the equation

$$x^2 + y^2 + z^2 = n(xyz + 1)$$

has a solution (x, y, z) in positive integers if and only if n can be represented as sum of two perfect squares.

Problem 5.13.24. Let a and b are positive integers such that

$$\begin{cases} a + 1 \mid b^2 + 1, \\ b + 1 \mid a^2 + 1. \end{cases}$$

Prove that a and b are odd numbers.

Problem 5.13.25. Find all positive integers a and b such that

$$\frac{a^2 + b^2 + a + b + 1}{ab}$$

is an integer

Problem 5.13.26. Let m and n be positive integers such that $mn \neq 1$. Let

$$k = \frac{m^2 + mn + n^2}{mn - 1}.$$

If k is an integer, find all its possible values.

Problem 5.13.27. Find all pairs of integers (m, n) such that

$$\frac{m}{n} + \frac{n}{m}$$

is also an integer.

Problem 5.13.28 (Vietnam 2002). Find all integers n for which there exist infinitely many integer solutions to

$$a + b + c + d = n\sqrt{abcd}.$$

Problem 5.13.29 (Putnam 1933). Prove that for every real number N, the equation

$$a^2 + b^2 + c^2 + d^2 = abc + bcd + cda + dab$$

has a solution in which a, b, c, and d are all integers greater than N.

Problem 5.13.30 (UNESCO Competition 1995). Let a, n be two positive integers and let p be an odd prime number such that

$$a^p \equiv 1 \pmod{p^n}.$$

Prove that

$$a \equiv 1 \pmod{p^{n-1}}.$$

Problem 5.13.31 (Iran Second Round 2008). Show that the only positive integer value of a for which $4(a^n + 1)$ is a perfect cube for all positive integers n, is 1.

Problem 5.13.32. Let $k > 1$ be an integer. Show that there exists infinitely many positive integers n such that

$$n|1^n + 2^n + 3^n + \cdots + k^n.$$

Problem 5.13.33 (Ireland 1996). Let p be a prime number, and a and n positive integers. Prove that if

$$2^p + 3^p = a^n,$$

then $n = 1$.

Problem 5.13.34 (Russia 1996). Let x, y, p, n, k be positive integers such that n is odd and p is an odd prime. Prove that if $x^n + y^n = p^k$, then n is a power of p.

Problem 5.13.35. Find the sum of all the divisors d of $N = 19^{88} - 1$ which are of the form $d = 2^a 3^b$ with $a, b \in \mathbb{N}$.

Problem 5.13.36. Let p be a prime number. Solve the equation $a^p - 1 = p^k$ in the set of positive integers.

Problem 5.13.37. Find all solutions of the equation

$$(n-1)! + 1 = n^m$$

in positive integers.

Problem 5.13.38 (Bulgaria 1997). For some positive integer n, the number $3^n - 2^n$ is a perfect power of a prime. Prove that n is a prime.

Problem 5.13.39. Let m, n, b be three positive integers with $m \neq n$ and $b > 1$. Show that if prime divisors of the numbers $b^n - 1$ and $b^m - 1$ be the same, then $b + 1$ is a perfect power of 2.

Problem 5.13.40 (IMO ShortList 1991). Find the highest degree k of 1991 for which 1991^k divides the number

$$1990^{1991^{1992}} + 1992^{1991^{1990}}.$$

Problem 5.13.41. Prove that the number $a^{a-1} - 1$ is never square-free for all integers $a > 2$.

Problem 5.13.42 (Czech Slovakia 1996). Find all positive integers x, y such that $p^x - y^p = 1$, where p is a prime.

Problem 5.13.43. Let x and y be two positive rational numbers such that for infinitely many positive integers n, the number $x^n - y^n$ is a positive integer. Show that x and y are both positive integers.

Problem 5.13.44 (IMO 2000). Does there exist a positive integer n such that n has exactly 2000 prime divisors and n divides $2^n + 1$?

Problem 5.13.45 (China Western Mathematical Olympiad 2010). Suppose that m and k are non-negative integers, and $p = 2^{2^m} + 1$ is a prime number. Prove that

- $2^{2^{m+1}p^k} \equiv 1 \pmod{p^{k+1}}$;
- $2^{m+1}p^k$ is the smallest positive integer n satisfying the congruence equation $2^n \equiv 1 \pmod{p^{k+1}}$.

Problem 5.13.46. Let $p \geq 5$ be a prime. Find the maximum value of positive integer k such that

$$p^k | (p-2)^{2(p-1)} - (p-4)^{p-1}.$$

Problem 5.13.47. Find all triples (x, y, z) of integers such that $3^x + 11^y = z^2$.

Problem 5.13.48. Find all positive integer solutions to $p^a - 1 = 2^n(p-1)$, where p is prime.

Problem 5.13.49. Prove that there are no positive integers x, y, and z such that $x^7 + y^7 = 1998^z$.

Problem 5.13.50 (Baltic Way 2012). Let $d(n)$ denote the number of positive divisors of n. Find all triples (n, k, p), where n and k are positive integers and p is a prime number, such that

$$n^{d(n)} - 1 = p^k.$$

Problem 5.13.51 (IZHO 2017). For each positive integer k, denote by $C(k)$ the sum of the distinct prime divisors of number k. For example, $C(1) = 0, C(2) = 2, C(45) = 8$. Determine all positive integers n such that $C(2^n + 1) = C(n)$.

Problem 5.13.52 (Hong Kong TST 2016). Find all triples (m, p, q) such that

$$2^m p^2 + 1 = q^7,$$

where p and q are ptimes and m is a positive integer.

Problem 5.13.53 (Brazil 2016). Define the sequence of integers a_n (for $n \geq 0$) such that a_0 is equal to an integer $a > 1$ and

$$a_{n+1} = 2^{a_n} - 1.$$

Let A be a set such that x belongs to A if and only if x is a prime divisor of a_n for some $n \geq 0$. Show that the number of elements of A is infinite.

Problem 5.13.54 (USAMO2017). Prove that there are infinitely many distinct pairs (a, b) of relatively prime integers $a > 1$ and $b > 1$ such that $a^b + b^a$ is divisible by $a + b$.

Problem 5.13.55 (Italy TST 2003). Let a and b be positive integers and p be a prime. Find all solutions to the equation $2^a + p^b = 19^a$.

Problem 5.13.56 (Turkey EGMO TST 2017). Determine all triples (m, k, n) of positive integers satisfying the following equation

$$3^m 5^k = n^3 + 125.$$

Problem 5.13.57 (Balkan 2013). Determine all positive integers x, y, and z such that $x^5 + 4^y = 2013^z$.

Problem 5.13.58. If p_n is the nth prime then prove that the integer $N = p_1 p_2 p_3 \dots p_n +$ 1 can not be a perfect power.

Problem 5.13.59. Find all ordered triplets (a, b, c) of positive integers such that

$$2^a - 5^b \cdot 7^c = 1.$$

Problem 5.13.60 (Vietnam TST 2016). Find all positive integers a and n with $a > 2$ such that each prime divisor of $a^n - 1$ is also prime divisor of $a^{3^{2016}} - 1$.

Problem 5.13.61. Find all positive integers n, for which n and $2^n + 1$ have the same set of prime divisors.

Problem 5.13.62. Find all triplets (x, y, z) of positive integers such that

$$(z + 1)^x - z^y = -1.$$

Bibliography

[1] Clarke, Pete L. *Some Applications of Thue's Lemma.* (2009).

[2] R. D. Carmichael, *Theory of Numbers*, page 36.

[3] C. Pomerance, *On Carmichael Conjecture*, American Mathematical Society, Volume 43, Number 2, April 1974.

[4] V. L. Klee, Jr, *On A Conjecture Of Carmichael*, American Mathematical Society, December, 1947.

[5] Hansraj Gupta, *Euler's Totient Function And Its Inverse*, Indian J. Pure Appl. Math, **12**(1): $22 - 30$, January 1981.

Glossary

Appendix A

Identities and Well-Known Theorems

We suppose that a, b are real numbers in the following results.

Identity A.1.

$$(a+b)^2 + (a-b)^2 = 2(a^2+b^2),$$
$$(a+b)^2 - (a-b)^2 = 4ab.$$

Identity A.2 (Sophie Germain Identity).

$$a^4 + 4b^4 = (a^2 + 2ab + 2b^2)(a^2 - 2ab + 2b^2).$$

Identity A.3.

$$(a+b)^3 - a^3 - b^3 = 3ay(a+b),$$
$$(a+b)^5 - a^5 - b^5 = 5ay(a+b)(a^2+ab+b^2),$$
$$(a+b)^7 - a^7 - b^7 = 7ay(a+b)(a^2+ab+b^2)^2.$$

Theorem A.0.1 (Binomial Theorem). *For any positive integer n,*

$$\begin{aligned}(a+b)^n &= a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{1}ab^{n-1} + b^n \\ &= \sum_{i=0}^{n}\binom{n}{i}a^{n-i}b^i \\ &= \sum_{i=0}^{n}\binom{n}{i}a^i b^{n-i}.\end{aligned}$$

Proof. If we expand the left side, there are n times $(a+b)$ multiplied together. Obviously, each term of this expansion will be of the form $a^i b^{n-i}$. So, we can write it as

$$(a+b)^n = s_n a^n + s_{n-1}a^{n-1}b + \cdots + s_1 ab^{n-1} + s_0 b^n.$$

Here, s_i is the coefficient of $a^i b^{n-i}$. We see that for a term $a^i b^{n-i}$ to appear in the sum, we must choose i of the n times $(a+b)$ to contribute an a to the term, and then each of the other $n-i$ terms of the product must contribute a b. We can take i objects from n objects in $\binom{n}{i}$ ways. Therefore, $s_i = \binom{n}{i}$. □

Theorem A.0.2. *For positive integers n and k such that $k \leq n$,*

1. $\binom{n}{k} = \binom{n}{n-k}$,
2. $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ *(Pascal's recurrence)*,
3. $\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$ *(absorption property)*,
4. $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n$,
5. $\binom{0}{k} + \binom{1}{k} + \cdots + \binom{n-1}{k} + \binom{n}{k} = \binom{n+1}{k+1}$,
6. $\binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n-1}^2 + \binom{n}{n}^2 = \binom{2n}{n}$.

Corollary A.0.3. *If n and k are coprime, then n divides $\binom{n}{k}$ and k divides $\binom{n-1}{k-1}$.*

Proof. Directly implied from part 3 of theorem (A.0.2). □

Identity A.4 (Sum of Powers of Consecutive Integers). *Let n be a positive integer. Then,*

1. $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$,
2. $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$,
3. $\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$,
4. $\sum_{i=1}^{n} i^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$.

Identity A.5 (Sum of Differences). *Let $a_1, a_2, a_3, \ldots$ be an infinite sequence of numbers. Then, for any positive integer n,*

$$a_n = a_1 + \sum_{k=1}^{n-1} (a_{k+1} - a_k).$$

Proof. Expand the sum on the right side to obtain

$$\begin{aligned}\sum_{k=1}^{n-1} (a_{k+1} - a_k) &= (a_n - a_{n-1}) + (a_{n-1} - a_{n-2}) + \cdots + (a_2 - a_1) \\ &= a_n - a_1.\end{aligned}$$

The conclusion follows. □

Identity A.6 (Fibonacci-Brahmagupta Identity). *For any reals a, b, c, d, and any integer n,*

$$\begin{aligned}(a^2+nb^2)(c^2+nd^2) &= (ac-nbd)^2+n(ad+bc)^2\\ &= (ac+nbd)^2+n(ad-bc)^2.\end{aligned}$$

In other words, the product of two numbers of the form a^2+nb^2 is of the same form. Particularly, for $n=1$,

$$\begin{aligned}(a^2+b^2)(c^2+d^2) &= (ac+bd)^2+(ad-bc)^2\\ &= (ad+bc)^2+(ac-bd)^2.\end{aligned}$$

The following identity is a generalization of Fibonacci-Brahmagupta Identity. *Lagrange* used this identity to prove the *Sum of Four Squares Theorem.*

Identity A.7 (Euler's Four Square Identity). *Let $a_1, a_2, \ldots, a_4$ and $b_1, b_2, \ldots, b_4$ be reals. Then,*

$$\begin{aligned}&(a_1^2+a_2^2+a_3^2+a_4^2)(b_1^2+b_2^2+b_3^2+b_4^2)\\ &\quad= (a_1b_1+a_2b_2+a_3b_3+a_4b_4)^2+(a_1b_2-a_2b_1+a_3b_4-a_4b_3)^2\\ &\qquad+(a_1b_3-a_2b_4-a_3b_1+a_4b_2)^2+(a_1b_4+a_2b_3-a_3b_2-a_4b_1)^2.\end{aligned}$$

An interested reader can see *Degen's eight-square identity* [1] or *Pfister's sixteen-square identity* [2], but they do not look pretty at all and we do not include them here.

Identity A.8 (Lebesgue Identity).

$$(a^2+b^2-c^2-d^2)^2+(2ac+2bd)^2+(2ad-2bc)^2=(a^2+b^2+c^2+d^2)^2$$

Identity A.9 (Euler-Aida Ammei Identity). *Let $x_1, x_2, \ldots, x_n$ be reals. Then,*

$$(x_1^2-x_2^2-\cdots-x_n)^2+\sum_{i=2}^{n}(2x_1x_i)^2=(x_1^2+x_2^2+\cdots+x_n^2)^2.$$

Identity A.10 (Bhaskara's Lemma). *Let m, x, y, n and k be integers such that $k\neq 0$. If $y^2-nx^2=k$, then*

$$\left(\frac{mx+ny}{k}\right)^2-n\left(\frac{mx+y}{k}\right)^2=\frac{m^2-n}{k}.$$

This identity is used in *Chakravala method* to find the solutions to *Pell-Fermat equation.*

Bibliography

[1] Piezas III, Titus. "The Degen-Graves-Cayley Eight-Square Identity." Web address accessed 27 August 2016. http://sites.google.com/site/tpiezas/ramanujan/12.TheDegen-Graves-Cayleyeight-squareidentity(July2005).pdf. (2005).

[2] Conrad, Keith. "Pfister's Theorem on Sum of Squares." Web address accessed 27 August 2016. http://www.math.uconn.edu/~kconrad/blurbs/linmultialg/pfister.pdf.