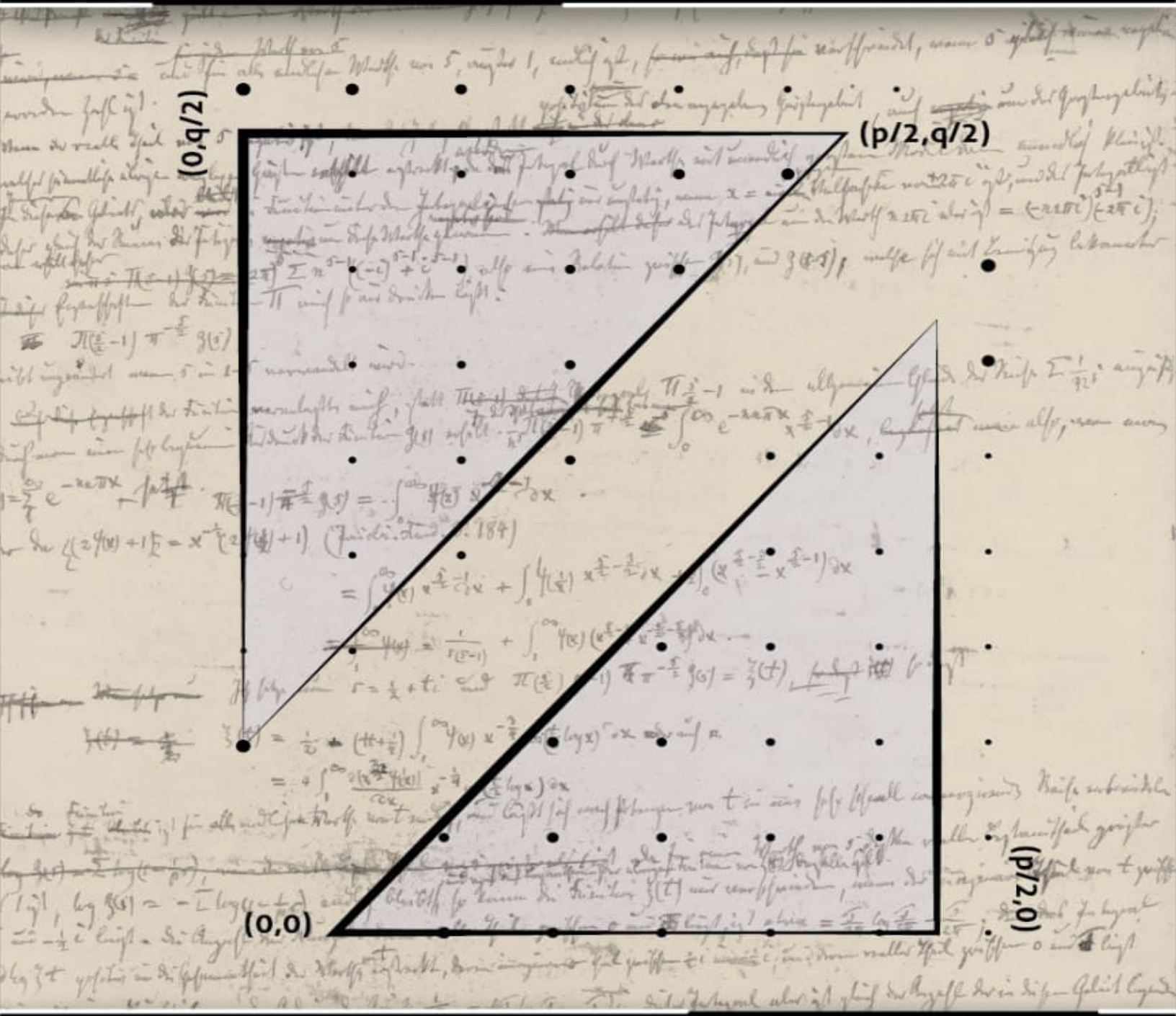
Topics in Number Theory

an Olympiad-Oriented Approach



Masum Billal

Amir Hossein Parvardi

TOPICS IN NUMBER THEORY

An Olympiad–Oriented Approach

Second Edition

Masum Billal
Amir Parvardi

Dedicated to

Fermat, the father of modern number theory.
Euler, without whom number theory probably wouldn't be so rich today.
Riemann, who made huge contributions to analytic number theory.
Ramanujan, the mathematician of mathematicians.
Paul Erdős, the man who loved only numbers.

Preface to Second Edition

It has been over 3 years since we have written this book. When we read the book now, we sometimes feel kind of silly. In some places, the writing comes off as childish and probably even unprofessional. But we do not regret writing the book that way. There are reasons why we have written it the way we did. We admit that we did not have the enormous amount of patience required to finish the book in a greater style. We were hurried to write a lot of the things back then. Not because we were told to, since this is an independent publication after all. There are a number of factors why we felt hurried to finish the book. For example, the book was already large even though we discarded a lot of the content we had planned for the book. In fact, we discarded most of the content we planned because the book would be so huge not even us would have been interested in reading a book that large. But that messed with our plans a lot since we had to change a lot of things on the fly. The whole reason we wanted to write a book despite there existing a lot of books on number theory is that we wanted our book to contain results or techniques that would not be as common in other Olympiad books. However, even with the minimum amount of content we decided to go with, it still felt like it was getting too large. So we tried to pick up the pace after some chapters. And one of the biggest concerns we had was that if we had not finished the book soon, we might not have been able to finish it at all. Or even worse, we could have forgotten about the whole book altogether (that has happened as well). Anyway, we mention these here not to make any excuses, nor do we feel terrible about it. Because even though the end-product does not look like the best output right now, we believe this book can still help people, at least some new students who are looking to solve number theory problems. Would the book be a lot better if we rewrote it now? Yes, probably at least ten times better. But we have neither the energy nor the time to do so. There are some updates and error fixes in this edition which hopefully improves at least some aspects of the book.

It is possible there are some LaTeX issues in the new edition. If anyone finds any, please do not hesitate to email us.

Masum Billal
Amir Parvardi
August, 2021

Links, Contact

Preface from first edition

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 learn 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 argue our book itself is a collection of a lot of theorems as well. Sadly, that is partially true for multiple reasons 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. 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 content which we thought would ask for even discussion or we just felt lazy about it), we had to increase the pace.

Initially, 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 could hardly finish writing this first volume, and if I wanted to complete the whole series, we would probably have to keep writing my whole life. So, I had to discard a lot of content and make the book concise. This resulted in squeezing in a lot of content in a few hundred pages.

Finally, I would like to thank Amir for joining 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 objections from a reputed publisher like *Springer*.

Masum Billal

In the past three years, we have always been 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 more number theory concepts of higher level, 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!

Many of our friends helped us on the way to finish this book, as mentioned in the acknowledgment, 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 the only one in the hardest days of my life. Professor **Peyman Nasehpour**, whom I knew from the very first semester of my undergraduate studies in electrical engineering at the 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 and a great colleague to me when it comes to teamwork. I'm looking forward to working with him more often. The idea behind the lattices in the cover is a geometric proof of the law of quadratic reciprocity. Our friends found other interpretations such as the 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. 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 the 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 Parvardi,
Vancouver, BC, Canada,
July 2018.

Acknowledgment

Here is a list of all the kind people who helped us review, edit, and improve this book. The list is ordered alphabetically based on the last name.

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

2. Thanks to **AnréC** from TeX.StackExchange who wrote the code for figure (1.4) in base conversion.

3. We are thankful to **Arta Khanalizadeh** for designing the cover of the book.

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

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

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

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

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

9. Professor **Peyman Nasehpour** sent us the beautiful problem (4.6.9) and an amazing solution using Prime Number Theorem. He also gave us pretty useful comments on chapter 1. He also introduced in section (3.2.2) the amicable numbers to us with a brief historical note on it.

10. We appreciate **Kenji Nakagawa**'s comments on chapters 4 and 5. He was one of the first people who read and reviewed these two chapters when we put them on the website of the book.

11. We are thankful towards **Mohammadamin Nejatbakhshesfahani**, Iran National Olympiad gold medalist (2010) and winner of gold medals at IMS and IMC, who honored us to read and review the whole book and gave us really instructive comments.

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

13. We are honored to thank Professor **Greg Martin**, a faculty member at the Mathematics Department of the 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.

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

15. 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 on our website.

16. **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.

17. Thanks to **Amin Soofiani**, who is a Master's student of mathematics at the 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.

18. 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

$\binom{n}{k}$ n choose k, the binomial coefficient of the $k+1$-th term in the expansion of $(1+x)^n$.

$\lambda(n)$ Liouville function of n, $\lambda(n) = (-1)^{\Omega(n)}$ if n is square-free, otherwise $\lambda(n) = 0$. It is also used for Carmichael's universal function.

$a \perp b$ $\gcd(a,b) = 1$ or a and b are relatively prime.

$\alpha * \beta$ Dirichlet convolution of two arithmetic functions α and β.

$\lfloor x \rfloor$ and $\lceil x \rceil$ The largest integer not greater than x and the smallest integer integer not less than x respectively.

$\gcd(a,b)$ (for brevity, (a,b)) and $\operatorname{lcm}(a,b)$ (for brevity, $[a,b]$) are greatest common divisor and least common multiple of a and b respectively.

$\alpha \circ \beta$ General convolution of two arithmetic functions α and β.

$\left(\frac{a}{n}\right)$ The Jacobi symbol for an integer a and a positive integer n.

$\left(\frac{a}{p}\right)$ The Legendre symbol for an integer a and prime p.

$\Lambda(n)$ Von Mangoldt Function of n. $\Lambda(n) = \log p$ if $n = p^e$ for some positive integer e, otherwise $\Lambda(n) = 0$.

$\mu(n)$ Möbius function of n, $\mu(n) = (-1)^{\omega(n)}$ if n is square-free, otherwise $\mu(n) = 0$.

$d(n)$ Number of divisors of n.

$\pi(x)$ The number of primes not exceeding x.

$\Omega(n)$ Number of total prime divisors of n

$\omega(n)$ Number of distinct prime divisors of n

$\psi(x)$ Tchebycheff function of the second kind.

$\operatorname{rad}(n)$ Product of distinct prime divisors of n, $\operatorname{rad}(n) = \prod_{p|n} p$.

$\mathbb{N}, \mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{P}$, and $\mathbb{C}$ Sets of positive integers, non-negative integers, integers, rational numbers, real numbers, primes and complex numbers respectively.

$\sigma(n)$ Sum of divisors of n.

$\vartheta(x)$ Tchebycheff function of the first kind.

$\varphi(n)$ The number of positive integers not exceeding n which are relatively prime to n.

$\zeta(s)$ Zeta function of the complex number s.

Part I

Fundamentals

§§1 Divisibility

§§1.1 Definitions and Propositions

Let us start from the very basics. Whenever you encounter a definition, try to make sense of it with a few examples. As we move on to next sections, you will get used to the divisibility terms and notation. The following definitions are designed to teach a beginner student the basics of divisibility, so please do not bore yourself with them.

Definition. When an integer b is divided by another (non-zero) integer a, we can write $b = aq + r$ for some integers q and r. In this most general case, we call r the *remainder* of the division.

However, if we choose q such that $0 \leq r < |a|$, then we say r is the *minimum remainder* of the division[1].

At times, it is convenient to carry out the division (i.e., choose q) so that b is as close as possible to an integral multiple of a. Then we can write $b = aq + r$, with $|r| \leq |a/2|$ for some integer q. In this case, we call r the *minimum absolute remainder*.

Note (1). We will prove later that the minimum remainder is unique. That is, there exists exactly one value for r such that $b = aq + r$ and $0 \leq r < a$. Because of its uniqueness and non-negativity, remainder in this book will mean minimum remainder unless otherwise stated.

Note (2). When we talk about the the minimum absolute remainder in the division $b = aq + r$, note that if a is odd, we will have a unique r. That is, there exist only one possible value for r such that $|r| \leq |a/2|$. However, if a and b both are even, there can be two possible values for r. For example, if $a = 20$ and $b = 8$, the division can be done as both $20 = 8 \cdot 2 + 4$ and $20 = 3 \cdot 8 - 4$ and we would have two values for r: 4 and -4. To force r to be unique in this case, we will take the positive value of r as the minimum absolute remainder. Therefore, in our example, $20 = 2 \cdot 8 + 4$ would be accepted as the division equation and $r = 4$ is the minimum absolute remainder.

[1] $|x|$ is the absolute value of x.

Definition. If $b = aq + r$ is the proper division of b by a (that is, a division in which r is the minimum remainder), b is the *dividend*, a is the *divisor*, and q is the *quotient*.

Example. Let $b = 23$ and $a = 5$. The division of b by a can be done in many ways. Take $23 = 5 \cdot 2 + 13$, so we can say 13 is a remainder of 23 upon division by 5, but not a minimum remainder. If we write the division as $23 = 5 \cdot 4 + 3$, then 3 is the minimum remainder. And if we write it as $23 = 5 \cdot 5 + (-2)$, then -2 is the minimum absolute remainder.

If we divide 4 by 2, we get a zero remainder. In this case, we say that 4 is *divisible* by 2 and write it as $2 \mid 4$.

Definition. Let a and b be two integers. If b leaves a zero remainder upon division by a, or equivalently, if there is an integer k for which $b = ak$, we write $a \mid b$ and say that

- b is *divisible* by a,
- a *divides* b,
- a is a *divisor* (or a *factor*) of b, or
- b is a *multiple* of a.

Likewise, $a \nmid b$ denotes that b is not divisible by a.

Remark. Some (Eastern) authors use the notation $b : a$ instead of $a \mid b$, but it is not as common.

Definition. If a divides b and $|a| < |b|$, the number a is called a *proper divisor* of b. Here, $|a|$ denotes the absolute value of a. For example, $|-5| = 5$ and $|5| = 5$.

Example. $4 \mid 20$ and $5 \mid 20$ but $11 \nmid 20$.

Example. 1 is a divisor of all integers.

You can also try to make sense of division in this way: 8 divides 40 because 40 has every factor that 8 has in it. In other words, if 8 had a factor which was not a factor of 40, then 40 would not be divisible by 8. For example, 42 does not have the factor 4, which is a factor of 8, therefore $8 \nmid 42$.

Prime and Composite Numbers. An integer $n > 1$ is called *prime* if it has exactly two distinct (positive) divisors, namely 1 and n itself. A number greater than 1 which is not a prime is *composite*. In other words, an integer n is composite if it has a proper divisor other than 1. We do not wish to discuss primality for negative integers.

Note. When we say a is a divisor of b, unless otherwise stated, we usually mean a is a *positive* divisor of b. This is distinguished because negative divisors exist as well.

Question 1.1.1. Is 1 a prime number? If so, why? If not, how is it a composite number? You may be already familiar with prime numbers and in that case, the definition you know may seem a little different. Try to understand why we chose to stick with the above definition of primes rather than the following: *a positive integer n that is not divisible by any positive integer other than* 1 *and n is a prime.*

Parity. Parity is the property of an integer being *even* or *odd*. An even number is one which is divisible by 2. Odd numbers, on the other hand, leave a remainder of 1 when divided by 2.

Example. 2 and 4 have the same parity; they are both even. 5 and 10 are of different parity; 5 is odd and 10 is even.

Example. 11 is a prime because no positive integer greater than 1 and less than 11 divides it. Similarly 2, 3, and 29 are primes, but 169 (divisible by 13) and 1001 (why?) are composites. If a number is divisible by 2, it is composite. Thus, the only even prime is 2.

If we add or subtract two numbers of the same parity, the answer will be even. Conversely, the result of addition or subtraction of two numbers with different parities is always an odd number. Using these two facts, you can easily find many properties of integers related to parity. For instance, we can say that if we add or subtract an even number to or from a positive integer n, the parity does not change; i.e., parity remains *invariant* in this case. Moreover, any odd multiple of n has the same parity as n.

We usually deal only with positive integers in divisibility relations. However, sometimes negative integers or zero also come into play.

Proposition 1.1.2 (Basic Properties of Divisibility). *For any three integers a, b, and c, the following statements are true.*

1. $a \mid 0$.
2. $a \mid a$.
3. $1 \mid a$ *and* $-1 \mid a$.
4. *If a is non-zero, then* $0 \nmid a$.[2]
5. *If $a \mid b$, then $a \mid -b$, $-a \mid b$, and $-a \mid -b$.*
6. *If $a \mid b$, then $a \mid bk$ for all integers k.*
7. *If $a \mid b$, then $ak \mid bk$ for all integers k.*
8. *If $ak \mid bk$ for some non-zero integer k, then $a \mid b$.*
9. *If $a \mid b$ and $b \mid c$, then $a \mid c$.* [3]
10. *If $a \mid b$ and $b \neq 0$, then $|b| \geq |a|$. Consequently, if $a \mid b$ and $|a| > |b|$, then $b = 0$.*
11. *If $a \mid b$, then $a^n \mid b^n$ for all non-negative integers n.*
12. *If $a^n \mid b^n$ for some positive integer n, then $a \mid b$.*

[2] Does zero divide zero? That depends on the context. In arithmetic, we can write $0 = 0 \cdot 0 + 0$, so technically $0 \mid 0$ in number theory. However, when studying real analysis, division is defined as multiplying by the multiplicative inverse, which means that $0/0$ is undefined and therefore, $0 \nmid 0$ with that logic.

[3] *Keith Conrad* states this as a mantra: "A factor of a factor is a factor."

Proof. Most of the parts are trivial and we prove only the important ones. A general approach to solve this kind of problems is simply transforming them into equations. That is, when $x \mid y$, write $y = kx$ for some integer k.

4. Assume that $0 \mid a$ for some integer a. This means that $a = 0k$ for some integer k. Therefore, $a = 0$ is the only integer that is divisible by zero (in number theory).

6. $a \mid b$ means that $b = aq$ for some q. Multiply both sides of this equation by k to get $bk = akq = aq'$. Therefore $a \mid bk$.

9. $a \mid b$ and $b \mid c$, so $b = aq_1$ and $c = bq_2$ for some integers q_1 and q_2. Combine these two equations to get $c = aq_1q_2 = aq$, thus $a \mid c$.

10. $a \mid b$, so $b = ak$ for some integer k. Rewrite this equation in absolute value terms: $|b| = |ak| = |a| \cdot |k|$. Since k is a non-zero integer, the smallest value for $|k|$ is 1, so $|b| = |a| \cdot |k| \geq |a|$.

□

Note. You may think that it is straightforward to prove statement (12) in the above Proposition. However, it is not so simple. The reason is we need to prove that if

$$\frac{b^n}{a^n} = \left(\frac{b}{a}\right)^n$$

is an integer, then so is $\frac{b}{a}$. This is not obvious (try to make sense why).

Proposition 1.1.3. *If $a \mid b$ and $b \mid a$, then $|a| = |b|$. In other words, $a = \pm b$.*

Proof. The proof is quite simple using part 10 of the previous proposition. In fact, we get $|b| \geq |a|$ and $|a| \geq |b|$, which means $|a| = |b|$ or $a = \pm b$. □

The above proposition often comes handy when you want to prove that two expressions are equal. If you can show that each expressions divides the other one and that they have the same sign (both positive or both negative), you can imply that their values are equal.

Proposition 1.1.4. *For fixed positive integers a and b, there are unique integers q and r so that $b = aq + r$ with $0 \leq r < a$. In other words, the quotient and the minimum remainder of the division are unique.*

Proof. We can easily rule out the case $r = 0$. Just notice that $a \mid b$.

We can now assume that $a \nmid b$. Then, b must have a nonzero remainder upon division by a, say r. One can rewrite the equation $b = aq + r$ as $aq = b - r$ or $q = (b - r)/a$. This simply means that uniqueness of r implies the uniqueness of q. Therefore, we only need to prove that r is unique. Assume that there exist integers q' and r' so that

$$\begin{aligned} b &= aq + r \\ &= aq' + r' \end{aligned}$$

This implies $a(q-q') = r'-r$, which shows that $r'-r$ is divisible by a. Is it possible? The answer is clearly no. Since r' and r are both less than a, we have $|r'-r| < a$. By part 10 of proposition (1.1.2), we must have $|r'-r| = 0$, which gives $r' = r$. This means two remainders are the same and the minimum remainder is unique. The proof is complete. □

Question 1.1.5. We know that $4 \mid 20$ and $4 \mid 16$. Do they imply $4 \mid 20+16$? Again, this is not too obvious. Try to prove it first.

Proposition 1.1.6. *If $a \mid b$ and $a \mid c$, then $a \mid bx+cy$ for any arbitrary integers x and y. In particular, we have $a \mid b \pm ak$, $a \mid b+c$, and $a \mid b-c$.*

Proof. Since $a \mid b$, there is an integer k so that $b = ak$. Similarly, there is an integer ℓ so that $c = a\ell$. Therefore,

$$\begin{aligned} bx+cy &= akx + a\ell y \\ &= a(kx+\ell y) \end{aligned}$$

which is certainly divisible by a since it has a factor a in it. □

Note. Here, x and y can be negative integers as well. This shows how negative numbers may come into play even when we start off with positive integers.

Question 1.1.7. Let a, b, and n be positive integers such that $a \mid n$ and $b \mid n$. Do we have $ab \mid n$?

This is a very common mistake among new problem solvers. Consider an integer that is divisible by both 6 and 4. Is that integer divisible by $4 \cdot 6 = 24$? If you think the answer is yes, think again! How about 12?

In general, the answer is a big NO. Try to find a few more counterexamples and then find the condition when we can be certain that $ab \mid n$ if $a \mid n$ and $b \mid n$. We will now focus on prime divisors.

Proposition 1.1.8. *Any integer n greater than 1 has a prime divisor.*

Proof. If n itself is a prime, we are done. So, assume n is composite. By definition, n has a proper divisor, i.e., there is an integer greater than 1 and less than n which divides n. Call this divisor d. Now, if d is not a prime, then d has a divisor too. We can continue like this until we reach a point where d does not have a proper divisor greater than 1. We know by definition that only a prime number does not have a proper divisor other than 1. Therefore, that divisor must be a prime. □

Corollary 1.1.9. *Let n be a positive integer larger than 1. The smallest divisor of n is a prime.*

You should be able to prove the following proposition by yourself. Even if you can not prove it formally, at least make sense of why this is true. We will not prove it here. Try not to skip it and move on. Can you use induction[4] to prove it? How about using the facts you already know?

[4]The traditional induction process. Prove the claim for a base case, say n_0. Assume the claim is true for $n = m$, then prove it for $n = m+1$.

Proposition 1.1.10 (Euclid's Lemma). *Let a and b be two integers. If p is a prime and $p \mid ab$, then either $p \mid a$ or $p \mid b$.*

Corollary 1.1.11. *If a prime divides the product of some integers, it divides at least one of them.*

Proposition 1.1.12. *Every composite n has a prime factor less than or equal to $\sqrt{n}$.*

Proof. Since n is composite, it has at least one proper prime divisor. *Consider the smallest prime factor p of n* and write $n = pk$ for some integer k. Of course $p \leq k$, because otherwise according to Corollary (1.1.9), the smallest prime factor would be k or one of its divisors. Therefore,

$$n = pk \geq p^2$$

which in turn implies $p \leq \sqrt{n}$. □

This proposition is quite useful to test the primality of a number. It implies that it suffices to check if n is divisible by any of the primes less than or equal to $\sqrt{n}$. If it is, then n is not a prime. Check this with some simulations by hand, say for $11, 25$, and 479. However, the test can be quite lengthy and tedious if n is too large and its smallest prime factor is not small. If you are curious how lengthy this test can be, take the number 357 879 581 and try finding its smallest prime divisor.

Prime Factorization. Prime factorization is the process of finding all the prime factors of a positive integer.

The fact that every positive integer greater than 1 has a prime factorization gives birth to the *Fundamental Theorem of Arithmetic*.

Theorem 1.1.13 (Fundamental Theorem of Arithmetic). *Every positive integer n larger than 1 can be written as a product of primes in a unique way. We write this factorization as*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \tag{1.1}$$

where $p_1, p_2, \cdots p_k$ are different primes and $e_1, e_2, \cdots e_k$ are positive integers. Using product notation, we can write equation (1.1) as

$$\begin{aligned} n &= \prod_{i=1}^{k} p_i^{e_i} \\ &= \prod_{p \mid n} p^e \end{aligned}$$

In the second product notation above, p runs through all primes dividing n and e is the maximum power of p that divides n.[5]

[5] Make sure you understand the notations $\sum$ and $\prod$.

Proof. We first prove by induction that the factorization indeed exists. Suppose that all numbers k such that $1 < k < n$ have a factorization. If n is a prime, its factorization is obvious. Otherwise, there exist positive integers a and b both less than n such that $ab = n$. By induction hypothesis, a and b both have factorizations. Let $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ and $b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l}$ be the prime factorizations of a and b. Then,

$$\begin{aligned} n &= ab \\ &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l} \end{aligned}$$

This is a prime factorization for n and the induction is complete.

Now, let us prove that the prime factorization of n is unique. Suppose that there are two factorizations for n. That is,

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t} \tag{1.2}$$

are two factorization of n, where p_i and q_j are primes and α_i and β_j are positive integers ($1 \le i \le s, 1 \le j \le t$). The above equation implies that p_1 divides $q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t}$. By generalization of Euclid's lemma (Corollary (1.1.11)), p_1 must divide at least one of $q_1^{\beta_1}, q_2^{\beta_2}, \ldots,$ or $q_t^{\beta_t}$. Without loss of generality, suppose that $p_1 \mid q_1^{\beta_1}$. Since q_1 is a prime, the only prime divisor of $q_1^{\beta_1}$ is q_1. This means that $p_1 = q_1$ and $\alpha_1 = \beta_1$. Divide both sides of equation (1.2) by p_1 to obtain

$$p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_s^{\alpha_s} = q_2^{\beta_2} q_3^{\beta_3} \cdots q_t^{\beta_t}$$

With similar reasoning, we can deduce that $p_2^{\alpha_2}$ is equal to some other $q_j^{\beta_j}$, say $q_2^{\beta_2}$. Continuing this process, one soon realizes that $t = s$ and all prime powers in the left side of equation (1.2) appear in the right side, but maybe in a different order. In other words, the two factorizations of n are the same and the uniqueness of factorization is implied. □

Example. Try to understand the following examples and match them with the factorization formula:

- $12 = 2^2 \cdot 3$. Here, $p_1 = 2, e_1 = 2, p_2 = 3, e_2 = 1$
- $180 = 2^2 \cdot 3^2 \cdot 5$. So, $p_1 = 2, e_1 = 2, p_2 = 3, e_2 = 2, p_3 = 5, e_3 = 1$

The factorization of n is unique no matter in what order you factor out the primes. Also, note that all the powers are positive. We could bring primes with power zero but that does not make any sense (because any number to the power of zero yields 1 and the product would not be changed).

Note. In the product $n = \prod_{i=1}^{k} p_i^{e_i}$, k is the number of distinct prime factors of n. For example, if $n = 12$, then $k = 2$ since 12 has only two distinct prime factors: 2 and 3. If $n = 180$, then $k = 3$ because 2, 3, and 5 are the only prime factors of n.

As explained above, one way to factorize a number n is to divide it by all primes less than $\sqrt{n}$. Dividing a number by another would be pretty boring for large numbers. In order to simplify the process, next section provides some rules for divisibility by some specific numbers like 3, 5, 7, 11, etc.

§§§1.1 Divisibility by Certain Numbers

As soon as one is introduced to the concept of natural numbers, one can make sense of odd and even numbers. We all know that an even number, namely a number that is divisible by 2, must have an even rightmost digit (ones digit). We also know the *rules of divisibility* for 5: a number is divisible by 5 if and only if its ones digit is. Let us make our knowledge concrete and write a proof for these two simple facts.

Proposition 1.1.14 (Divisibility by 2). *A number is divisible by* 2 *if and only if its last digit is even (one of* $0, 2, 4, 6, 8$*).*

Proof. Suppose that one has the number $x = \overline{x_{k-1}x_{k-2}\dots x_0}$, where x_i $(0 \leq i \leq k-1)$ are its digits (so the number has k digits). One can write

$$\begin{aligned} x &= \overline{x_{k-1}x_{k-2}\dots x_1 0} + x_0 \\ &= 10 \cdot \overline{x_{k-1}x_{k-2}\dots x_1} + x_0 \end{aligned}$$

It is now clear that the first term in the right-hand side of the latest equation is divisible by 2 (because $2 \mid 10$). So, x is divisible by 2 if and only if x_0 is even. □

The proof of the rule of divisibility by 5 is very similar and left as an exercise for the reader.

Proposition 1.1.15 (Divisibility by 5). *A number is divisible by* 5 *if and only if it has* 0 *or* 5 *as last digit.*

So far, we discovered and proved the rules of divisibility by 2 and 5. Is it always possible to find a divisibility rule for division by a given arbitrary number n? Maybe the question is somehow unclear at the moment. We need to define a *divisibility rule* first:

Definition. Let $n > 1$ be any integer. A divisibility rule for n is defined to be a process which leads to determining whether a given natural number is divisible by n.

Let's think about the question again. Can we find a divisibility rule for any $n > 1$? The answer is obviously yes. With our definition of a divisibility rule, you can consider division by n as a divisibility rule. One can always divide a natural number by n and find the remainder of the division. The number is divisible by n if and only if this remainder is equal to zero.

Well, of course, that is not what we had in mind. We are looking for divisibility rules that make our life simpler, not the ones which ask you to do it by brute force. So, it would be wise to refine our definition:

Definition. Let $n > 1$ be any integer. A *proper* divisibility rule for n is a divisibility rule which uses a recursive algorithm. From now on, by a divisibility rule, we mean a proper one.

As an example, recall the rule of divisibility by 3. To find out the remainder of a number upon division by 3, we add up all the digits to create a smaller number. This is

the *recursive* step: we are doing a simple process (adding the digits) to transform our initial given number (which we suppose is large) into a new number which is smaller in size. Then, we find the remainder of the new smaller number by 3. We know from high school (or elementary school) that the remainder of the new number when divided by 3 is the same as that of the original number.

In general, we are looking for divisibility rules which explain a method for creating a smaller number from an initially large given number. This new number has one thing in common property with the initial number: its remainder when dived by n. We can repeat this algorithm as many times as we wish until we reach numbers small enough for us to do the division by hand. We know that our iterative algorithm will terminate at some point because you cannot go smaller than 1.

It is quite easy to see that the algorithm for checking divisibility by 3 is indeed very fast and terminates quickly. That is, the algorithm is *time-efficient*. Suppose that you have a 100 digit number and you want to check its divisibility by 3. Dividing the number by 3 to find the remainder is the worst thing to do because there is probably no calculator which can do this task for you and you would need to do the division by hand. Now, if you use the algorithm provided above, you would need to sum up all the digits of the number, which would be at most $100 \times 9 = 900$ (in case where all the digits are the largest, 9), and then find the remainder of this sum upon division by 3. If you are reading this text right now, you must be able to divide any three digit number by 3 without using a calculator. So, this algorithm terminates after one iteration in this case because you will find the remainder right after finding the sum of the digits. Considering we started with a 100 digit number, that is assumed to be a pretty fast algorithm.

Let's see the mathematical idea behind the divisibility rule for 3.

Proposition 1.1.16 (Divisibility by 3). *A number is divisible by* 3 *if and only if the sum of digits of the number is divisible by* 3.

Example. Take the number 951 which has a sum of digits $9+5+1=15$, divisible by 3. According to our claim, 951 should be divisible by 3 and indeed it is: $951 = 3 \cdot 317$.

Proof. The secret lies behind the fact that $10 = 3 \cdot 3 + 1$. Write your initial number $x = \overline{x_{k-1}x_{k-2}\cdots x_0}$ as

$$\begin{aligned} x &= 10^{k-1}x_{k-1} + 10^{k-2}x_{k-2} + \cdots + 10x_1 + x_0 \\ &= (3\cdot 3+1)^{k-1}x_{k-1} + (3\cdot 3+1)^{k-2}x_{k-2} + \cdots + (3\cdot 3+1)x_1 + x_0 \end{aligned}$$

Try to show as an exercise that the remainder of division of $(3\cdot 3+1)^i$ (for $1 \le i \le k-1$) is always equal to 1 (hint: you might want to use theorem PBinomial Theorem). In other words, there exist integers q_i (for $1 \le i \le k-1$) such that $(3\cdot 3+1)^i = 3q_i+1$. Therefore,

$$\begin{aligned} x &= (3\cdot 3+1)^{k-1}x_{k-1} + (3\cdot 3+1)^{k-2}x_{k-2} + \cdots + (3\cdot 3+1)x_1 + x_0 \\ &= (3q_{k-1}+1)x_{k-1} + (3q_{k-2}+1)x_{k-2} + \cdots + (3q_1+1)x_1 + x_0 \\ &= 3(q_{k-1}+q_{k-2}+\cdots+q_1) + x_{k-1} + x_{k-2} + \cdots + x_1 + x_0 \end{aligned}$$

It is now clear that $3(q_{k-1}+q_{k-2}+\cdots+q_1)$ is always divisible by 3. This means that the remainder of x upon division by 3 is the same as that of $x_{k-1}+x_{k-2}+\cdots+x_1+x_0$, which is the sum of digits of x. It remains to verify the other direction, but all we did can be reversed and so the other direction also follows. The proof is complete. □

You might be curious if we can find such simple proper divisibility rules for other numbers. Unfortunately, the recursive algorithms we find for (most of) other numbers are not always time-efficient like that of 3 and it is possible that we need to wait for several iterations for the algorithm to terminate.

Another issue that we need to discuss is the following: for which numbers n do we really need a divisibility rule? For instance, now that we know the divisibility rules for 2 and 3, do we really need another rule for divisibility by 6? No! We know that a number is divisible by 6 if and only if it is divisible by both 2 and 3. If the previous sentence is not clear for you, think about it for a few minutes and investigate some examples to see why it is true. You don't need to know a rigorous proof of this fact; just convince yourself that it is true.

Proposition 1.1.17 (Divisibility by 6). *A number is divisible by* 6 *if and only if it is even and divisible by* 3.

We got that there is no need for us to define a divisibility rule for 6 because we already know rules for 2 and 3. There is nothing special about $6 = 2 \cdot 3$. In general, we do not need a divisibility rule for pq, where p and q are distinct primes, if we already have rules for p and q.

Proposition 1.1.18 (Divisibility by pq). *Let p and q be distinct primes. A number is divisible by pq if and only if it is divisible by both p and q.*

Proof. The only if part is pretty obvious: if n is divisible by pq, then it is divisible by both p and q. To prove the if part, assume that a positive integer n is divisible by both p and q. From divisibility by p, we can write $n = pk$ for some integer k. Since p and q are different, p is not divisible by q. Since $n = pk$ is divisible by q, we must have that q divides k. This means that $k = ql$ for an integer l. Finally, $n = pql$, which implies that n is divisible by pq. □

You have probably figured out where this is going: we only need divisibility rules for n when n is either a prime or a power of a prime. The other cases would follow from the next corollary of proposition (1.1.18) (can you explain why?).

Corollary 1.1.19. *Let m and n be two positive integers (not necessarily primes) which do not share any common divisors. Then, a number is divisible by mn if and only if it is divisible by both m and n.*

We said that in order to find divisibility rules for all natural numbers, we need a divisibility rule for primes as well as their powers. Finding divisibility rules for powers of primes other than 2, 3, and 5 would not be something of interest for our book. We will discuss only divisibility rules for powers of 2. Let's see the most basic case, $4 = 2^2$.

Proposition 1.1.20 (Divisibility by 4). *A number is divisible by* 4 *if and only if the number formed by its last two digits is divisible by* 4.

Example. 202 390 2348 has the last two digits 4 and 8 which make the number formed by its last two digits 48. Since 48 is divisible by 4, the number 202 390 2348 is divisible by 4.

What about $2^3 = 8$?

Proposition 1.1.21 (Divisibility by 8). *A number is divisible by* 8 *if and only if the number formed by its last three digits is divisible by* 8.

If you have a curious mind, you should already notice a pattern in the divisibility rules for 2, 4, and 8. For 2, we only check the last digit. For 4, we check the last two digits and for 8, the last three digits. Do you see the pattern now? $2 = 2^1, 4 = 2^2$ and $8 = 2^3$. You can easily check that the same is true if we take $16 = 2^4$. To check divisibility by 16, it suffices to test the number formed by the last 4 digits. We can generalize this result for 2^k.

Theorem 1.1.22 (Divisibility by 2^k). *Let k be a positive integer. A number x is divisible by 2^k if and only if the number formed by the last k digits of x is divisible by 2^k.*

Proof. To prove this one, suppose that you have an n digit number x, represented as

$$x = \overline{x_{n-1}\cdots x_k x_{k-1}\cdots x_1 x_0}.$$

Then, note that

$$\begin{aligned} x &= \overline{x_{n-1}\cdots x_{k+1}\underbrace{000\cdots 0}_{k \text{ times}}} + \overline{x_k x_{k-1}\cdots x_1 x_0} \\ &= 10^k \cdot \overline{x_{n-1}\cdots x_{k+1}} + \overline{x_k x_{k-1}\cdots x_1 x_0} \end{aligned}$$

Since $10^k = 2^k \cdot 5^k$ is divisible by 2^k, we get the conclusion. □

Let's find a divisibility rule for 7.

Proposition 1.1.23 (Divisibility by 7). *A number is divisible by* 7 *if and only if the difference of the number formed by the last three digits and the rest of digits is divisible by* 7.

Proof. Notice that if $x = \overline{x_{n-1}\cdots x_1 x_0}$, then

$$\begin{aligned} x &= \overline{x_{n-1}\cdots x_1 x_0} \\ &= \overline{x_{n-1}\cdots x_3 000} + \overline{x_2 x_1 x_0} \\ &= 10^3 \cdot \overline{x_{n-1}\cdots x_3} + \overline{x_2 x_1 x_0} \end{aligned}$$

The remainder of division of 1000 by 7 is 6. So, there exists a positive integer q such that $1000 = 7q - 1$ (why is that? find q). Hence,

$$\begin{aligned} x &= (7q-1)\cdot \overline{x_{n-1}\cdots x_3} + \overline{x_2 x_1 x_0} \\ &= 7q \cdot \overline{x_{n-1}\cdots x_3} + (\overline{x_2 x_1 x_0} - \overline{x_{n-1}\cdots x_3}) \end{aligned}$$

Now, if x is divisible by 7, then so must be $\overline{x_2 x_1 x_0} - \overline{x_{n-1}\cdots x_3}$ and vice versa. The proof is complete. □

Example. Take the number 13 111. To see if it is divisible by 7 or not, first separate the number into two parts: Form a number with last three digits and another with the other part. In this case, we have 111 and 13. Their difference is 98, which is divisible by 7. According to the rule of divisibility by 7, this number is divisible by 7.

There are other rules for divisibility as well, and we are just suggesting a selected one for each number. You might have seen other divisibility rules for 7 (and other numbers). Another famous divisibility rule for 7 is the following: take the last digit of the number, double it, and then subtract the result from the number formed by the rest of the digits. The resulting number would have the same remainder upon division by 7. For instance, the steps for 13 111 would be

$$\begin{aligned} 13\,111 &\implies 1\,311 - 2 = 1\,309 \\ 1\,309 &\implies 130 - 18 = 112 \\ 112 &\implies 11 - 4 = 7 \end{aligned}$$

and this verifies that 13 111 is divisible by 7. Try to prove this new divisibility rule for 7.

It is very important to bear in mind that each divisibility rule is time-efficient when applied to a number with proper number of digits. For instance, the divisibility rule for 7 given in proposition (1.1.23) works best for numbers with a few digits (say, 6 to 10 digit numbers) and if your number has, say, 100 digits, you would need to wait for a long time for the algorithm to terminate because you are removing three digits from your number at each step and a 97 digit number is not much different from a 100 digit number when it comes to computation: they are both huge! Try to figure out for what range of numbers the other divisibility rule for 7 works best.

Proposition 1.1.24 (Divisibility by 9). *A number is divisible by* 9 *if and only if the sum of its digits is divisible by* 9.

Proposition 1.1.25 (Divisibility by 11). *A number is divisible by* 11 *if and only if the difference of sums of alternating digits is divisible by* 11.

Example. Take 12 047 816. The sum of digits in even places is $2 + 4 + 8 + 6 = 20$ and sum of digits in odd places $1 + 0 + 7 + 1 = 9$. Their difference is $20 - 9 = 11$, which is divisible by 11. You can easily check that

$$12\,047\,816 = 11 \cdot 1\,095\,256$$

which verifies our test.

Proposition 1.1.26 (Divisibility by 13). *A number is divisible by* 13 *if and only if the result of addition of four times the last digit and the the number formed by rest of the digits is divisible by* 13.

Example.

$$\begin{aligned} 8658 &\implies 865 + 4 \cdot 8 = 897 \\ 897 &\implies 89 + 4 \cdot 7 = 117 \\ 117 &\implies 11 + 4 \cdot 7 = 39 \end{aligned}$$

And $39 = 13 \cdot 3$, so 8658 is divisible by 13.

Proposition 1.1.27 (Divisibility by 17). *A number is divisible by* 17 *if and only if the result of subtraction of five times the last digit from the number formed by rest of the digits is divisible by* 17.

Example.

$$\begin{aligned} 11\,322 &\implies 1\,132 - 5 \cdot 2 = 1\,122 \\ 1\,122 &\implies 112 - 5 \cdot 2 = 102 \\ 102 &\implies 10 - 5 \cdot 2 = 0 \end{aligned}$$

So 11 322 is divisible by 17.

Proposition 1.1.28 (Divisibility by 19). *A number is divisible by* 19 *if and only if the result of addition of two times the last digit and the the number formed by rest of the digits is divisible by* 19.

Example.

$$\begin{aligned} 12\,654 &\implies 1\,265 + 2 \cdot 4 = 1\,273 \\ 1\,273 &\implies 127 + 2 \cdot 3 = 133 \\ 133 &\implies 13 + 2 \cdot 3 = 19 \end{aligned}$$

Therefore 12 654 is divisible by 19.

Although the above propositions can be easily proved by modular arithmetic, it would be a great exercise for the reader to prove them with elementary tools we have discussed so far.

Problem 1.1.29. Find a divisibility rule for 37.

Hint. Use the fact that $999 = 1000 - 1$ is divisible by 37.

§§1.2 GCD and LCM

Consider 18 and list all its divisors in your mind. Do the same for 27. What do these two lists have in common? If you have done the calculations correctly, you should come up with 1, 3, and 9. Among these *common divisors* of 18 and 27, 9 is the largest. So, we say that 9 is the *greatest common divisor* of 18 and 27.

Consider 18 and 27 again. This time, list all their integral multiples mentally. The list of multiples of 18 is

$$18, 36, 54, 72, 90, 108, \cdots$$

whereas the list of multiples of 27 is

$$27, 54, 81, 108, \cdots$$

There are infinitely many common numbers shared by these two lists: $54, 108, \cdots$. The smallest number in the latter list is 54, which we call the *least common multiple* of 18 and 27.

You may ask, what makes you think there will even be a common element in both sets? Well, we will have at least 1 common as a divisor since it divides all the integers.

GCD and LCM. For two integers a and b which are not zero at the same time, the greatest common divisor of a and b, denoted by $\gcd(a,b)$, is the greatest positive integer which divides both a and b. For brevity, we denote this by (a,b) in this book.

The least common multiple of a and b, denoted by $\operatorname{lcm}(a,b)$, is the smallest positive integer that is divisible by both a and b. Again, for brevity, we denote this by $[a,b]$ in this book.

The concept of gcd and lcm is the same for more than two integers. The greatest common divisor of $a_1, a_2, \cdots, a_n$ is the largest positive integer which divides them all. We denote this by $(a_1, a_2, \cdots, a_n)$. One can define $[a_1, a_2, \cdots, a_n]$ in a similar way.

Example. $(18, 27) = 9$ and $[18, 27] = 54$. $(18, 27, 36) = 9$ and $[18, 27, 36] = 108$.

Note. The above definition of gcd is equivalent to the following: if (a,b) equals g, then g divides both a and b. Furthermore, if there is a positive integer c for which $c \mid a$ and $c \mid b$, then $g \geq c$. Analogously, if $[a,b]$ equals ℓ, then ℓ is divisible by both a and b. Moreover, if there is a positive integer c for which $a \mid c$ and $b \mid c$, then $c \geq \ell$.

Proposition 1.2.1 (Properties of gcd and lcm). *Let a and b be two positive integers. The following statements are true.*

1. $(a,b) = (b,a) = (a,-b) = (-a,-b)$ *and* $[a,b] = [b,a] = [a,-b] = [-a,-b]$.
2. $(a,0) = a$, $[a,0] = 0$, $(a,1) = 1$ *and* $[a,1] = a$.
3. $(a,a) = [a,a] = a$.
4. $[a,b] \geq (a,b)$.
5. $a \mid b$ *if and only if* $(a,b) = a$. *Similarly,* $a \mid b$ *if and only if* $[a,b] = b$
6. *For any integer* k, $(a, b+ak) = (a,b)$ *and* $(ka,kb) = k(a,b)$. *Furthermore,* $[ka,kb] = k[a,b]$.
7. *For any non-negative integer* n, *we have* $(a^n, b^n) = ((a,b))^n$ *and* $[a^n, b^n] = ([a,b])^n$.
8. *For any two integers* x *and* y, *we have* $(a,b) \mid ax + by$.
9. *If* p *is a prime divisor of* a *or* b, *then* $p \mid [a,b]$.
10. *For any prime divisor* p *of* (a,b), *we have* $p \mid a$ *and* $p \mid b$.
11. *If* p *is a prime, then*

$$(a,p) = \begin{cases} p & \text{if } p \mid a \\ 1 & \text{otherwise} \end{cases}$$

The proofs are pretty obvious and the reader is encouraged to prove them as an exercise. We only provide a hint for part 4: use part 10 of proposition (1.1.2).

We will now prove part 12 of proposition (1.1.2) as a problem.

Problem 1.2.2. For integers a and b, if $a^n \mid b^n$ for some positive integer n, then $a \mid b$.

Solution. Let $g = (a, b)$. By part 7 of proposition (1.2.1), $g^n = (a^n, b^n)$. On the other hand, $a^n \mid b^n$ implies $(a^n, b^n) = a^n$ by part 5 of the same proposition. Hence, $(a, b)^n = a^n = g^n$. Taking root n, we find $(a, b) = a = g$. Using part 5 again, one obtains $a \mid b$. The proof is complete.

Proposition 1.2.3. *For positive integers a, b, and c, if $c \mid a$ and $c \mid b$, then $c \mid (a, b)$. Analogously, if $a \mid c$ and $b \mid c$ then $[a, b] \mid c$.*

Definition. Two positive integers are *relatively prime* or *relatively prime to each other* if their greatest common divisor is 1. We shall use $a \perp b$ to denote that $(a, b) = 1$, i.e., that a and b are relatively prime.

Example. $3 \perp 4$, but $4 \not\perp 6$ since 2 divides both 4 and 6.

Proposition 1.2.4. *Let a, b, and c be three integers. The following statements hold true.*

1. *If $a \perp b$, $a \mid c$, and $b \mid c$, then $ab \mid c$.*
2. *If $a \perp b$ and $a \mid bc$, then $a \mid c$.*
3. *If $a \perp b$ and $a \perp c$, then $a \perp bc$.*
4. *If $a \perp b$, then $a^m \perp b^n$ for all non-negative integers m, n.*
5. *If $a \perp b$, then $[a, b] = ab$.*
6. *If $a \perp b$, then $(a, bc) = (a, c)$.*
7. *If p and q are distinct primes, then $p \perp q$.*

Note (1). Part 2 is really useful in solving problems. It is actually the general form of proposition (1.1.10). Be careful not to use this part incorrectly. To be precise, one cannot imply from $a \mid bc$ that $a \mid c$ unless $a \perp b$. We state a proof to this part in the solution of problem (2.4.8).

Note (2). If $a \perp b$ and $a \perp c$, it is not necessary that $b \perp c$. Can you think of an example?

Given integers a and b, how can we calculate (a, b)? Chances are you already know how to do this from elementary school. There are two common ways to do that. The first way is to factorize both numbers and find their common factors. Although we use this method a lot, it may not be wise to factorize very large numbers just to find their gcd. In such cases, the second way comes helpful: the Euclidean algorithm.

Theorem 1.2.5 (Euclidean Algorithm). *Let a and b be two positive integers. Divide b by a and write $b = aq + r$, where q is an integer and $0 \leq r < a$. Then $(a, b) = (a, r)$.*

Proof. Let $g = (a, b)$. We already know that $g \mid a$ and $g \mid b$. Since $b = aq + r$, it follows that $g \mid aq + r$. On the other hand, $g \mid a$ implies $g \mid aq$. As established in proposition (1.1.6), we can subtract these two divisibility relations and find $g \mid aq + r - aq$, or $g \mid r$. This means that g divides r too. That is, the greatest common divisor of a and b is a divisor of r too. In order to show that $g = (a, r)$, there is only one thing remained to prove: if there exists some c for which $c \mid a$ and $c \mid r$, then $g \geq c$. We will prove a stronger argument: if such a c exists, then $c \mid g$ (since c and g are both positive, $c \mid g$ implies $g \geq c$). Note that $c \mid a$ gives $c \mid aq$. Adding the latter relation with $c \mid r$ yields $c \mid aq + r = b$. From proposition (1.2.3), we see that $c \mid (a, b) = g$. The proof is complete. □

Euclidean algorithm[6] is pretty useful because it helps us find the gcd only by a series of divisions. Suppose that you have two extremely large numbers a and b such that $b > a$. First, find the remainder r of b upon division by a. The remainder is strictly less than a, and there is a chance that it would be much smaller than b because $b > a > r$. According to Euclidean algorithm, instead of finding gcd of a and b, we can calculate (a, r). In the next step, find the remainder r_1 of a upon division by r. Then $(a, b) = (a, r) = (r, r_1)$. As you might have noticed, the numbers are becoming smaller and smaller. Continuing the divisions, you will reach a point where the numbers are small enough to compute the gcd by hand.

Corollary 1.2.6. *Let $n, a,$ and b be positive integers such that $n \mid a - b$. Then $(n, a) = (n, b)$.*

The proof of this corollary is exactly the same as the previous theorem. If you look closely, you will find that we did not make use of the given inequality $0 \leq r < a$ in the process of proving Euclidean algorithm. In fact, that condition is given only to make the algorithm more efficient.

To make sense of Euclidean algorithm, follow the next example.

Example. Let's find $(112, 20)$. The first division $112 = 20 \cdot 5 + 12$ gives $(112, 20) = (20, 12)$. By performing the second division, $20 = 12 \cdot 1 + 8$, we obtain$(20, 12) = (12, 8)$. The next steps result in $(12, 8) = (8, 4)$ and $(8, 4) = (4, 0)$. The gcd of any number and zero is the number itself. So, $(20, 112) = 4$. If you understood the process correctly, you will know that the algorithm terminates when one of a or b becomes 0.

The other way of finding the greatest common divisor relies on factorization. Before stating the related proposition for this method, we solve the previous example again by factorizing.

Example. First, factorize both 20 and 112:

$$20 = 2^2 \cdot 5$$
$$112 = 2^4 \cdot 7$$

You can easily find that since the prime factor 5 does not appear in the factoring of 112, 5 cannot appear in $(20, 112)$. For the same reason, 7 will not appear in the gcd as well. In other words, we just have to consider the primes that are in both 112 and 20. We are left with the only prime 2. The point is to pay attention to the power of 2 that divides

[6] An algorithm means a set of operations in a certain process to solve a problem or to find something.

the numbers. 112 is divisible by 2^4. However, 20 is divisible by 2^2 but not by any higher power of 2. Therefore, $(20, 112)$ cannot have a power of 2 greater than 2^2 (otherwise it will not divide 20). Since we are looking for the *greatest* common divisor, we will take 2^2 as proper power of 2 in the gcd. Since there is no other prime to take care of, we have $(112, 20) = 2^2$.

This method works for the lcm as well:

Example. Take $180 = 2^2 \cdot 3^2 \cdot 5^1$ and $105 = 3^1 \cdot 5^1 \cdot 7^1$. The lcm of these two numbers is divisible by both of them, so it must contain all their prime factors. That is, $[180, 105] = 2^a 3^b 5^c 7^d$ for some positive integers a, b, c, and d. Since we are looking for the *least* common multiple, we need a, b, c, and d to be as small as possible. The smallest value for a is 2 because otherwise $a = 1$, then the lcm would not be divisible by 4 and consequently not divisible by 180 either. Similarly, the smallest values of b, c, and d are the largest power of $3, 5$, and 7, respectively, which divide 180 and 105. Finally, $b = 2, c = 1, d = 1$, and $[180, 105] = 2^2 \cdot 3^2 \cdot 5^1 \cdot 7^1 = 1260$.

Do the simulation for a few more examples to convince yourself. The following proposition formalizes this method.

Proposition 1.2.7. *Let a and b be two positive integers. If $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ and $b = p_1^{f_1} \cdot p_2^{f_2} \cdots p_k^{f_k}$, where p_i are primes and $e_i, f_i \geq 0$ are integers for $1 \leq i \leq k$, then:* [7]

$$(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \cdots p_k^{\min(e_k, f_k)}$$
$$[a, b] = p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \cdots p_k^{\max(e_k, f_k)}$$

In other words, using the product notation,

$$(a, b) = \prod_{i=1}^{k} p_i^{\min(e_i, f_i)}$$
$$[a, b] = \prod_{i=1}^{k} p_i^{\max(e_i, f_i)}$$

Note. This idea can be generalized for finding gcd or lcm of n integers. Just factorize the numbers and select the proper powers of primes.

Proposition 1.2.8. *For two integers a and b with $g = (a, b)$, there exist integers m and n such that $a = gm$ and $b = gn$. Moreover, m and n are relatively prime.*

Proof. Integers m and n exist because $g \mid a$ and $g \mid b$, but why are m and n relatively prime? This is true because if there were any other common factor between m and n, that would have been included in g too. Otherwise, g could not remain the greatest common divisor since we can make a bigger one multiplying that common factor with g. We can think of m and n as the *uncommon* factors between a and b. □

[7] Try to find out why $e_i \geq 0$ whereas we consider only $e_i \geq 1$ when we first introduced prime factorization.

Example. Consider 18 and 27. $(18, 27) = 9$ and we can write $18 = 9 \cdot 2$ and $27 = 9 \cdot 3$. Now, 9 is the largest common factor. Here, 2 is the uncommon factor from 18 which 27 does not have besides 9, and 3 is the uncommon factor of 27 which 18 does not have apart from 9. Thinking about m and n in this way may make more sense to you.

Proposition 1.2.9. *Let g and ℓ be the greatest common divisor and the least common multiple of positive integers a and b, respectively. If we write $a = gm$ and $b = gn$ with $(m, n) = 1$, then $\ell = gmn$.*

Proposition 1.2.10. *Let $g = (a, b)$ and $\ell = [a, b]$. Then $ab = g\ell$. In words, the product of two positive integers is equal to the product of their* gcd *and* lcm.

First proof. By proposition (1.2.8), there exist relatively prime positive integers m and n such that $a = gm$ and $b = gn$. Therefore $ab = gm \cdot gn = g^2mn$. On the other hand, by proposition (1.2.9), $gl = g \cdot gmn = g^2mn$. □

The following proof uses prime factorization and is somewhat more rigorous. But the previous one makes more sense. Even though it may look uglier, it shows how to invoke prime factorization.

Second Proof (Using Prime Factorization). Assume that we have the prime factorization of a and b (as in proposition (1.2.7)):

$$\begin{aligned} a &= p_1^{e_1} \cdots p_k^{e_k} \\ b &= p_1^{f_1} \cdots p_k^{f_k} \end{aligned}$$

Now, can you understand the simple fact that $\min(x, y) + \max(x, y) = x + y$? If so, then the proof should be clear to you. In fact,

$$ab = p_1^{e_1} \cdots p_k^{e_k} \cdot p_1^{f_1} \cdots p_k^{f_k} = p_1^{e_1+f_1} \cdots p_k^{e_k+f_k}$$

On the other hand, from proposition (1.2.7),

$$\begin{aligned} (a, b) \cdot [a, b] &= p_1^{\min(e_1)} \cdots p_k^{\min(e_k)} \cdot p_1^{\max(e_1 f_1)} \cdots p_k^{\max(e_k f_k)} \\ &= p_1^{\min(e_1 f_1) + \max(e_1 + f_1)} \cdots p_k^{\min(e_k f_k) + \max(e_k f_k)} \\ &= p_1^{e_1+f_1} \cdots p_k^{e_k+f_k} \\ &= ab \end{aligned}$$

□

Question 1.2.11. Let a, b, and c be positive integers. Does the equation

$$abc = (a, b, c) \cdot [a, b, c]$$

hold? If not, why?

§§1.3 Numeral Systems

§§§1.3 Introduction

There is a rumor that Pascal once promised 1000000 dollars to anyone who marries his daughter. Later, when the son-in-law asked for the money, Pascal gave him only 64 dollars. Poor guy! If you got the joke, you are probably good with bases. If not, do not worry, keep reading and you will get the point.

In daily mathematics, meaning the math you face in real life, you unconsciously express numbers in decimal system. That is, when you say you have 15 apples, you are using base 10 without ever realizing it. The question here is that what is this *base* actually? Let us start with a simple example.

Example. Consider the number 573. Have you ever thought why we write digits in this way to denote a number? The reason is that every digit in the number represents the coefficient of a power of ten. That is,

$$573 = 5 \cdot 10^2 + 7 \cdot 10^1 + 3 \cdot 10^0$$

Rigorously talking, each integer has to be written in a *base* for it to make sense. For example, the number 15 has different values when expressed in base 6 and in base 10. Actually, 15 in base 6 is equal to 11 in base 10. Probably it still does not make sense. If so, just keep reading.

All of our calculations in daily life are done in base 10, which is called the *decimal system*. However, this does not mean that we cannot present numbers in any other bases other than 10. There are a limited number of *digits* in each base (to be precise, the number of digits is the same as the value of base). These digits run from 0 to the largest integer smaller than the base. Therefore, in base 10 the digits are $0, 1, \cdots, 9$[8]. Similarly, in base b the digits will be $0, 1, \cdots, b-1$. Observe the base-10 representation of 573 in the above example again. The rightmost digit is multiplied by 1. The middle digit, 7, is multiplied by 10 (hence the name *tenths digit*). Finally, the leftmost digit is multiplied by 100 (the *hundredths digit*). In simpler words, each time we go left, we multiply the multiplier by 10. If it were base b instead of base 10, we would multiply by b each time. So, the multipliers would be $1, b, b^2, \cdots$ and so on. You should understand the formal representation of an integer in base b (for $b > 1$ an integer). Note that it is pointless to take base 1 since we do not have any meaningful digit (recall that 0 is not a meaningful digit). You can think of these multipliers as weights (or contribution) of those digits.

Base b Representation. Let x and b be positive integers such that $b > 1$. In a numeral system[9], the number x and its *base* b are written together as $(x)_b$. If the digits of an

[8] Take a wild guess why we use base 10 and not any other base.

[9] A numeral system (or system of numeration) is a writing system for expressing numbers using digits or symbols.

Base	System Name
2	Binary
3	Ternary
4	Quaternary
8	Octal
10	Decimal
16	Hexadecimal
36	Hexatrigesimal
60	Sexagesimal

Table 1.1: Common numeral systems and their names.

n-digits number x are represented as $\overline{x_{n-1}x_{n-2}\cdots x_0}$ in base b, then

$$\begin{aligned}(x)_b &= (x_{n-1}x_{n-2}\cdots x_1x_0)_b \\ &= b^{n-1}x_{n-1} + b^{n-2}x_{n-2} + \cdots + b^1x_1 + x_0\end{aligned}$$

where $x_0, x_1, \cdots, x_{n-1}$ are non-negative integers less than b.

The base is written in the subscript, while the digits are inside the bracket (or a line is drawn over the digits) to clarify it is not a product. An important note to be mentioned is the fact that x_{n-1} is always non-zero, because if it is zero, then there is no point in keeping it as the leftmost digit. That is, we can remove this digit until we get a nonzero digit as the leftmost digit. The rightmost digit of x is denoted by x_0, and it is called the *least significant digit* of x. Analogously, the leftmost digit, x_n, is called the *most significant digit* of x. You should already be able to guess where these names come from! For instance, in decimal system, observe that the rightmost digit has multiplier 1, and so contributes the least. The largest digit 9 contributes 9 if it is in the rightmost position. On the other hand, if 1 is the leftmost digit (say thousandth), then it has multiplier (you can think of it as a weight in this regard as well) 1000, which is a lot more than 9. So, 1 contributes the most, and naturally it is the most significant digit. Same explanation applies for the least significant digit.

Example. The number $(327)_8$ is calculated as

$$(327)_8 = 3 \cdot 8^2 + 2 \cdot 8 + 7 = 215$$

Note. When the base is absent in a representation, it is regarded to be 10 by default.

Different bases maybe used in different systems. For example, in computer science, it is conventional to represent the numbers in base 16 or 8. Another example is base 60 which was used by ancient Summerians in the 3^{rd} millennium BC. In order to avoid repeating the base numbers, we use a specific name for popular bases. You can find a list of such names in the following table.

§§§1.3 Base Conversion

After defining bases, the first problem that we face is defining the relationship between the numbers in different bases. For many of us, we can only make sense of numbers when they are represented in decimal system. For example, you may have no clue about the real value of $(1234)_5$, but you surely know what is 1234 (if we do not write the base, it is 10 by default).

1.3.2.1 Conversion from Base b to Base 10

In order to understand the meaning of numbers (their value) in a particular base b, we need to convert them to a number in base 10. In the previous given example, we showed how to convert $(327)_8$ to base 10. The process of converting base $b < 10$ to base 10 is directly resulted from definition (1.3.1). However, we have an issue when the base is larger than 10. Before stating the process of conversion, think about this: what happens if the base, b, is greater than 10? Then we have a problem in representing the digits. For example, in the *hexadecimal system* with base of 16, the digits must be less than 16. Therefore, we should be able to represent digits 10 to 15 in hexadecimal system. But how is it possible to have a two-digits number as one digit in an hexadecimal number? In order to avoid the confusion, we use the following notation for digits bigger than ten:

$$10 = \texttt{A}, \quad 11 = \texttt{B}, \quad 12 = \texttt{C}, \quad 13 = \texttt{D}, \quad 14 = \texttt{E}, \quad 15 = \texttt{F}.$$

Example.

$$\begin{aligned}(\texttt{2FE05})_{16} &= 2 \cdot 16^4 + 15 \cdot 16^3 + 14 \cdot 16^2 + 0 \cdot 16 + 5 \\ &= 131,072 + 61,440 + 3,584 + 5 \\ &= 196,101\end{aligned}$$

We know how to convert numbers in any base to a number in base 10. The next step is exactly the opposite: converting numbers in decimal system to other bases. This is quite interesting as well. Even it is possible that you have learned the method from school. However, instead of focusing on the method, let us focus on finding a way to do it.

1.3.2.2 Conversion from Base 10 to Base b

Suppose that we want to convert the number y in decimal system to a number in base b. In other words, we want to write y as $(x_n x_{n-1} \cdots x_1 x_0)_b$ so that $x_0, x_1, \cdots x_n$ are the digits of y when represented in base b. By definition, we know that y can be written as

$$y = b^n x_n + b^{n-1} x_{n-1} + \cdots + b^1 x_1 + x_0 \tag{1.3}$$

where $0 \leq x_i < b$ for $0 \leq i \leq n$. Our aim is to find the value of x_i's. Look at the equation carefully and try to understand how we can retrieve the digits in base b. If you are stuck,

then go forward. Rewrite equation (1.3) as

$$y = b \cdot \underbrace{(b^{n-1}x_n + b^{n-2}x_{n-1} + \cdots + x_1)}_{y_1} + x_0$$

We have written y as $y = by_1 + x_0$, which means that the remainder of y when divided by b is x_0. In fact, the rightmost digit of y in base b (x_0 here) is the remainder of y when divided by b. As you can see, we are simply using the division theorem here (does it make sense now?). Bases are related to divisibility after all!

To find the next digit, x_1, we have to divide the quotient of the above division, y_1, by b. The reason is the same as above: rewrite y_1 as

$$y_1 = b \cdot \underbrace{(b^{n-2}x_n + b^{n-3}x_{n-1} + \cdots + x_2)}_{y_2} + x_1$$

Therefore, x_1 is the remainder of y_1 when divided by b. We can find the next digit x_2 by finding the remainder of y_2 when divided by b. The digits $x_3, x_4, \cdots, x_{n-1}$ can be found similarly by continuing this process. The leftmost digit, x_n, is the quotient of the last division because we can no longer divide it by b (since the digits are all less than b).

Example. Let us find the representation of 215 in base 8 and base 2. Start with base 8 first. We initialize the process by dividing the given number by 8. The remainder of this division is the rightmost digit of 215 in base 8. Then we divide the quotient by 8 again. The remainder of this division is the digit before the rightmost one. Since the quotient of this division is less than 8, the process is over. Using long division:

$$\begin{array}{r} 26 \\ 8\overline{)215} \\ \underline{160} \\ 55 \\ \underline{48} \\ 7 \end{array} \qquad \begin{array}{r} 3 \\ 8\overline{)26} \\ \underline{24} \\ 2 \end{array}$$

Figure 1.1: Conversion process of 215 from decimal system to octal (base 8).

In different countries, people use different ways to demonstrate long division. The above way is usually used in English-speaking countries such as USA or Canada. In European and Asian countries, people (mostly) use the following way of doing long division:

$$\begin{array}{r|l} 215 & 8 \\ \hline -16 & 26 \\ \hline 55 & \\ -48 & \\ \hline 7 & \end{array} \qquad \begin{array}{r|l} 26 & 8 \\ \hline -24 & 3 \\ \hline 2 & \end{array}$$

Figure 1.2: Conversion process of 215 from decimal to octal with divisions done in a different way (common in Europe and Asia).

Thus, $215 = (327)_8$, which matches the result in previous section. To find 215 in base 2, we do the divisions as follows. If this is not how you do long divisions, just do them in your own way.

$$\begin{array}{r|l} 107 & 2 \\ \hline 215 & \\ 200 & \\ \hline 15 & \\ 14 & \\ \hline 1 & \end{array} \qquad \begin{array}{r|l} 53 & 2 \\ \hline 107 & \\ 100 & \\ \hline 7 & \\ 6 & \\ \hline 1 & \end{array} \qquad \begin{array}{r|l} 26 & 2 \\ \hline 53 & \\ 40 & \\ \hline 13 & \\ 12 & \\ \hline 1 & \end{array} \qquad \begin{array}{r|l} 13 & 2 \\ \hline 26 & \\ 20 & \\ \hline 6 & \\ 6 & \\ \hline 0 & \end{array} \qquad \begin{array}{r|l} 6 & 2 \\ \hline 13 & \\ 12 & \\ \hline 1 & \end{array} \qquad \begin{array}{r|l} 3 & 2 \\ \hline 6 & \\ 6 & \\ \hline 0 & \end{array} \qquad \begin{array}{r|l} 1 & 2 \\ \hline 3 & \\ 2 & \\ \hline 1 & \end{array}$$

Figure 1.3: Conversion process of 215 from decimal to binary (base 2).

Reading from right to left, the quotient of the first division is the leftmost digit, and the remainders of divisions form the other digits. So, the result is $(11010111)_2$.

Example. Assume we want to convert the number 196 101 to base 16.

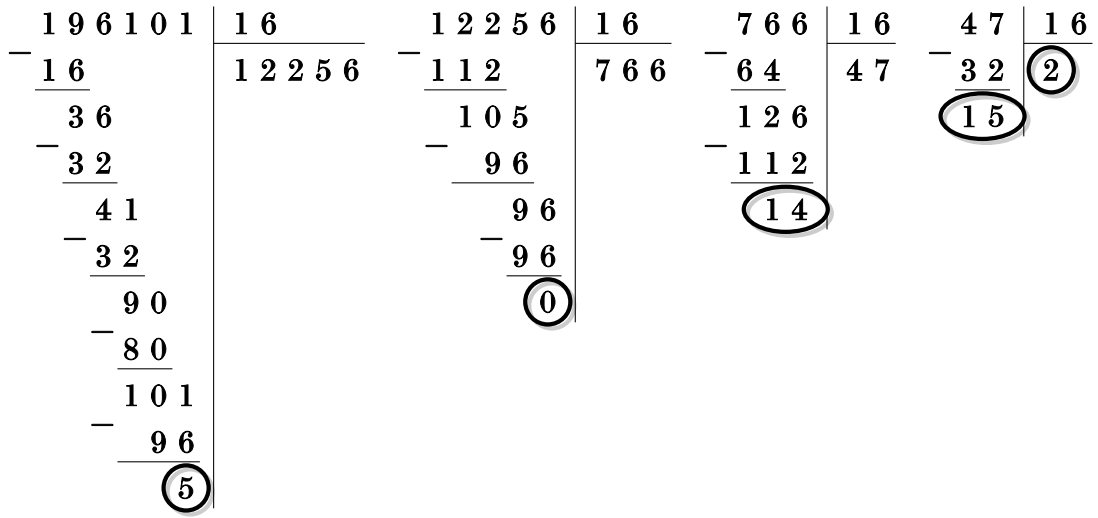


Figure 1.4: Conversion process of 196 101 from decimal to hexadecimal (base 16).

If you write down the divisions like we did[10] in figure (1.4), you can see that the last quotient is the most significant digit and the remainders of the divisions (from right to left) form the other digits (as you move from the last remainder to the first one, the significance of the digits decreases). We have drawn circles around those digits. Finally, writing 15 as F and 14 as E, we have

$$196\,101 = (2\mathrm{F}\,\mathrm{E}05)_{16}$$

1.3.2.3 Conversion Rules for Certain Bases

Assume that we want to convert a number in base 2 to base 8. How should it be done? One approach is to convert the number to base 10 first, and then convert it to base 8. You should be able to do this procedure by now. However, we prefer to do the conversion in one step, if possible, rather than two steps.

Let $x = (a_n a_{n-1} \cdots a_1 a_0)_2$ be our binary number, where a_i is either 0 or 1 for $0 \leq i \leq n$. Assume that we have converted this number to base 8 and the result is $x = (b_m b_{m-1} \cdots b_1 b_0)_8$, where $0 \leq b_j \leq 7$ for $0 \leq j \leq m$. Our aim is to find the relation between a_i's and b_j's. It might seem a bit difficult to find a relation, but it will be clear if you write the expansion of x in both bases. For base 2, we can represent x as

$$x = 2^n a_n + 2^{n-1} a_{n-1} + \cdots + 2^1 a_1 + a_0$$

Start clustering a_i digits in groups of 3, starting at the right. For convenience, assume that $n+1$ is divisible by 3 (because there are $n+1$ digits $a_0, a_1, \cdots, a_n$ and we are putting them in groups of size 3). Other cases when number of digits is not divisible by 3 will be discussed later. Then, x can be represented as

$$(2^n a_n + 2^{n-1} a_{n-1} + 2^{n-2} a_{n-2}) + \\ (2^{n-3} a_{n-3} + 2^{n-4} a_{n-4} + 2^{n-5} a_{n-5}) + \cdots + (2^2 a_2 + 2^1 a_1 + a_0)$$

[10]Thanks to AndréC for writing the LaTeX code for the figure.

which is equal to

$$2^{n-2}\left(2^2a_n+2a_{n-1}+a_{n-2}\right)+$$
$$2^{n-5}\left(2^2a_{n-3}+2a_{n-4}+a_{n-5}\right)+\cdots+2^0\left(2^2a_2+2a_1+a_0\right)$$

Since $2^a=8^{a/3}$ for all real numbers a, we can write the above as

$$8^{\frac{n-2}{3}}\underbrace{\left(2^2a_n+2a_{n-1}+a_{n-2}\right)}_{b_m}+$$
$$8^{\frac{n-5}{3}}\underbrace{\left(2^2a_{n-3}+2a_{n-4}+a_{n-5}\right)}_{b_{m-1}}+\cdots+8^0\underbrace{\left(2^2a_2+2a_1+a_0\right)}_{b_0}$$

The power of 8 in all of the terms in the above sum is an integer (why?). Note that the number $2^2a_i+2a_{i-1}+a_{i-2}$ is actually $(a_ia_{i-1}a_{i-2})_2$, and so it is a non-negative integer less than or equal to $(111)_2=7$. This means that $2^2a_i+2a_{i-1}+a_{i-2}$ is acceptable as a digit in base 8 (remember that digits in base b should be less than b and non-negative). Now look at the last line of the above equations. It is of the form $8^mb_m+8^{m-1}b_{m-1}+\cdots+8b_1+b_0$. We have therefore found a relation between digits in base 2 and base 8:

$$\begin{aligned}m&=\frac{n-2}{3}\\ b_j&=2^2a_{3j+2}+2a_{3j+1}+a_{3j}\\ &=(a_{3j+2}a_{3j+1}a_{3j})_2\end{aligned}$$

There is only one point remaining: we first assumed the number of digits of the binary number is divisible by 3 so that we can group them. What if number of digits is not divisible by 3? It is not actually a problem. Put one or two zeros at the left side of the binary number and make the number of digits divisible by 3, then continue the process.

The above result looks a bit scary, but it is really simple in plain English, explained in the following theorem.

Theorem 1.3.1 (Base 2 to 8 Conversion Rule). *To convert a binary number to base* 8 *directly, start grouping the* 0 *and* 1 *digits of the number in groups of* 3*. If number of digits of the binary number is not divisible by* 3*, put one or two zeros at the left side of the number to make it so, and then group the digits. Then convert each of these groups into one octal digit (a digit in base* 8*)and rewrite the number. Conversion is done.*

Example. Let us convert $(1\,010\,011\,010)_2$ to base 8. Number of digits is 10, which is not divisible by 3. So we add two zeros to the left and start the process with the number $(001\,010\,011\,010)_2$. Now,

$$(001)_2=(1)_8,\quad (010)_2=(2)_8,\quad (011)_2=(3)_8,\quad (010)_2=(2)_8$$

Hence, $(1\,010\,011\,010)_2=(1232)_8$.

To convert a number from base 8 to base 2 one can do the converse process. For the sake of completeness, we include it here.

Theorem 1.3.2 (Base 8 to 2 Conversion Rule). *To convert an octal number to base 2 directly, convert each digit to a three digit number in base 2 and put all these three digit numbers together.*

Example. Let us convert $(2051)_8$ to a binary number. We have

$$(2)_8 = (\mathbf{010})_2, \quad (0)_8 = (\mathbf{000})_2, \quad (5)_8 = (\mathbf{101})_2, \quad (1)_8 = (\mathbf{001})_2$$

and the result is

$$(2051)_8 = (10\,000\,101\,001)_2$$

Notice that the zero as the most significant digit is meaningless and must be removed after the conversion is done. We suggest you to do the conversion in a two-step method (from base 8 to base 10 and then to base 2) to verify the answer.

You can convert a binary number to base 16 just by clustering the digits into groups of 4 and convert each group to a hexadecimal number. In general, one can use a similar approach to convert a binary number to base 2^n (and vice versa). However, the cases where n is larger than 4 are rarely used.

Similar approaches can be used for conversion between other numbers as well. For example, to convert base 3 to base 9, one should start grouping the digits in groups of 2 and then do the conversion. The theorems are pretty similar to the above and we do not mention them here.

§§1.4 Floor and Ceiling

Let us discuss a classical problem.

Problem 1.4.1. How many integers between 10 and 100 are divisible by 7?

First, we count the multiples of 7 less than 100: 7, 14, 21, 28, 35, 42, 49, 56, 63, 70, 77, 84, 91, and 98. We don't need go any further since it will make the multiple larger than 100. Among these multiples, we should not consider 7 since we are asked between 10 and 100. This gives us the intuition behind the problem. We first find the number of multiples of 7 between 1 and 100, which is 14. Then, subtract the number of multiples that are less than 10, i.e., those which are between 1 and 9. In this case, only 7 itself would be such a multiple. Therefore, the answer to the problem is $14 - 1 = 13$. In fact, the problem is converted into two sub-problems:

1. how many integers from 1 to 100 are divisible by 7?

2. how many integers from 1 to 10 are divisible by 7?

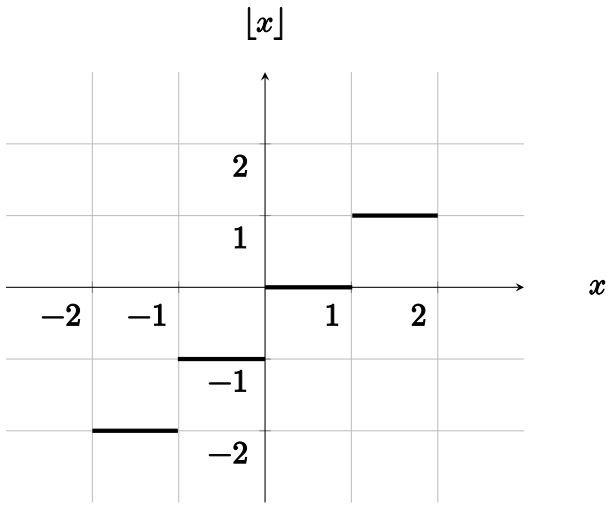


Figure 1.5: The floor function $\lfloor x \rfloor$ for $-2 \leq x \leq 2$.

These two sub-problems are basically the same. Therefore, we only need to answer the general question that how many integers in the interval $[1 : x]$ are divisible by n. The result is actually the quotient of the division x/n (why?). Consequently, rises the definition of the *floor function*.

Floor Function and Fractional Part. We call the function $\lfloor x \rfloor : \mathbb{R} \to \mathbb{Z}$ the *floor function* and for every real x, $\lfloor x \rfloor$ (read *floor of* x) is the largest integer less than or equal to x. Moreover, we denote by $\{x\}$ the *fractional part of* x, which is equal to $x - \lfloor x \rfloor$.

Example. $\lfloor 3.1415 \rfloor = 3$, $\lfloor -2 \rfloor = -2$, and $\lfloor 5 \rfloor = 5$. Figure 1.5 shows the value of $\lfloor x \rfloor$ for x between -2 and 2. For positive real numbers, the fractional part is simply the the non-integer part of the number. For example, the fractional part of 3.14 is 0.14. However, the definition of fractional part for negative real numbers may be deceptive. For instance, the fractional part of -3.14 is not 0.14, but

$$\begin{aligned} \{-3.14\} &= -3.14 - (-4) \\ &= 0.86 \end{aligned}$$

We can generalize the above problem now. The number of integers between two natural numbers a and b (inclusive) which are divisible by n is

$$\left\lfloor \frac{b}{n} \right\rfloor - \left\lfloor \frac{a-1}{n} \right\rfloor + 1$$

(Can you see why we are using $a-1$ in the second fraction?) Here, we have assumed that $b \geq a$.

Proposition 1.4.2 (Properties of Floor Function). *For any two reals x and y and any two integers m and n,*

1. $x \geq \lfloor x \rfloor > x - 1$,
2. *if $n \leq x$, then $n \leq \lfloor x \rfloor$,*

3. $\lfloor x+n \rfloor = \lfloor x \rfloor + n$,
4. *if* $x < y$, *then* $\lfloor x \rfloor \leq \lfloor y \rfloor$,
5. $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x+y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$,
6. $\lfloor \lfloor x \rfloor \rfloor = \lfloor x \rfloor$,
7. *if* x *is an integer,* $\lfloor x \rfloor + \lfloor -x \rfloor = 0$. *Otherwise, it equals* 1.

Example. The inequality $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x+y \rfloor$ (as seen in part 5) is sometimes referred to as the *triangle inequality of floor function*. You can easily check why this inequality holds and find the condition in which it becomes an equality. Put $x = 3.6$ and $y = 2.5$. Then, $\lfloor x \rfloor + \lfloor y \rfloor = 5$, which is strictly less than $\lfloor x+y \rfloor = 6$. The reason why we have a strict inequality here is somewhat obvious now: 0.6 and 0.5 add up to 1.1, which is more than one. You can easily check that only when $\{x\} + \{y\}$ is less than one, the equality case occurs. Otherwise, the inequality is strict.

Proof. 1. Let $\lfloor x \rfloor = k$. By definition, k is the greatest integer not exceeding x, so $x \geq k$ and $x < k+1$.

2. $n \leq x = \lfloor x \rfloor + \{x\} < \lfloor x \rfloor + 1$, and since n is an integer, $n \leq \lfloor x \rfloor$.

3. By definition, $\lfloor x \rfloor \leq x$ and so $\lfloor x \rfloor + n \leq x + n$. On the other hand, again by definition, $x < \lfloor x \rfloor + 1$. Therefore

$$\lfloor x \rfloor + n \leq x + n < \lfloor x \rfloor + n + 1$$

This means that $\lfloor x \rfloor + n$ is the largest integer less than or equal to $x+n$ and hence $\lfloor x+n \rfloor = \lfloor x \rfloor + n$.

4. Write $x < y$ as $\lfloor x \rfloor + \{x\} < \lfloor y \rfloor + \{y\}$ and then $\lfloor x \rfloor < \lfloor y \rfloor + \{y\} - \{x\}$. Now by parts 2 and 3,

$$\begin{aligned} \lfloor x \rfloor &\leq \lfloor \lfloor y \rfloor + \{y\} - \{x\} \rfloor \\ &= \lfloor y \rfloor + \left\lfloor \overbrace{\{y\} - \{x\}}^{<1} \right\rfloor \\ &= \lfloor y \rfloor \end{aligned}$$

5. Let $\lfloor x \rfloor = a$, $\lfloor y \rfloor = b$, $\{x\} = a_1$, and $\{y\} = b_1$. By 2, $a_1, b_1 \geq 0$ and so

$$a + b \leq a + a_1 + b + b_1$$

Sine $a+b$ is an integer, applying part 2 we find

$$\begin{aligned} \lfloor x \rfloor + \lfloor y \rfloor &= a + b \\ &\leq \lfloor a + a_1 + b + b_1 \rfloor \\ &= \lfloor x + y \rfloor \end{aligned}$$

On the other hand, by part 3 we observe that

$$\begin{aligned}\lfloor x+y\rfloor &= \lfloor a+a_1+b+b_1\rfloor \\ &= a+b+\lfloor a_1+b_1\rfloor \\ &= \lfloor x\rfloor+\lfloor y\rfloor+\lfloor\overbrace{a_1+b_1}^{<2}\rfloor \\ &\leq \lfloor x\rfloor+\lfloor y\rfloor+1\end{aligned}$$

6. $\lfloor x\rfloor$ is an integer and the floor of every integer is equal to itself.

7. This is immediately implied from definition.

□

Proposition 1.4.3 (Properties of Fractional Part). *For any real x,*

1. $0\leq\{x\}<1$,

2. $\{x+n\}=\{x\}$,

3. $\{\{x\}\}=\{x\}$,

4. *if x is an integer, $\{x\}+\{-x\}$ is zero, otherwise it equals* 1.

Proofs are straightforward and we leave them for the reader as an exercise.

Now, we get to the other way of solving problem 1.4.1. First, we subtracted the number of multiples less than 10. This time we find out the first multiple of 7 that is *greater than or equal to* 10, and the greatest multiple less than or equal to 100 (this part is same as before). $14=7\cdot 2$ is the first multiple of 7 greater than 10. Since $98=7\cdot 14$ is the largest multiple of 7 less than 100, the answer to the problem would be the number of integers between 2 and 14 (inclusive). There are $14-2+1=13$ such integers. Consequently, this makes us define *ceiling*. Try to make sense how this relates to the properties of this function.

Ceiling Function. We call the function $\lceil x\rceil:\mathbb{R}\to\mathbb{Z}$ the *ceiling function* and for every real x, $\lceil x\rceil$ (read *ceiling of x*) is the smallest integer greater than or equal to x.

Example. $\lceil 3.14\rceil=4$ and $\lceil 4\rceil=4$. Also $\lceil -4.1\rceil=-4$ whereas $\lceil 4.1\rceil=5$. As seen in Figure 1.6, similar to the floor function, the plot of the ceiling is like a chain of steps. Every two real numbers which lie between two consecutive integers have the same ceiling and floor value. Compare the plots of these two functions.

Proposition 1.4.4 (Properties of Ceiling Function). *For any two reals x,y and any two integers m,n,*

1. $x\leq\lceil x\rceil<x+1$

2. *if $n\geq x$, then $n\geq\lceil x\rceil$*

3. $\lceil x+n\rceil=\lceil x\rceil+n$

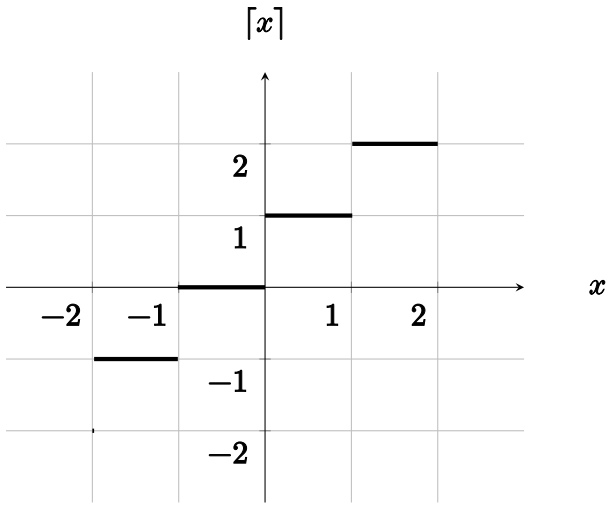


Figure 1.6: The ceiling function $\lceil x \rceil$ for $-2 \leq x \leq 2$.

4. *if* $x < y$, *then* $\lceil x \rceil \leq \lceil y \rceil$
5. $\lceil x \rceil + \lceil y \rceil - 1 \leq \lceil x + y \rceil \leq \lceil x \rceil + \lceil y \rceil$
6. $\lceil \lceil x \rceil \rceil = \lceil x \rceil$
7. *if* x *is an integer,* $\lceil x \rceil + \lceil -x \rceil = 0$. *Otherwise, it equals* 1
8. $\lceil x \rceil \geq x \geq \lfloor x \rfloor$

The proofs are pretty much the same as those of floor function and we do not provide them here.

Theorem 1.4.5. *For any two positive integers* n *and* k, *the following equation holds*

$$\left\lfloor \frac{n+1}{k} \right\rfloor - \left\lfloor \frac{n}{k} \right\rfloor = \begin{cases} 1 & \text{if } k \mid n+1 \\ 0 & \text{otherwise} \end{cases}$$

$$\left\lfloor \frac{n+1}{k} \right\rfloor^2 - \left\lfloor \frac{n}{k} \right\rfloor^2 = \begin{cases} 2\frac{n+1}{k} - 1 & \text{if } k \mid n+1 \\ 0 & \text{otherwise} \end{cases}$$

Proof. We will prove the first identity. The second one can be proved in a similar way. Let $n + 1 = kq + r$ for some positive integers q and r such that $0 \leq r < k$. Then,

$$\begin{aligned} \left\lfloor \frac{n+1}{k} \right\rfloor - \left\lfloor \frac{n}{k} \right\rfloor &= \left\lfloor \frac{kq+r}{k} \right\rfloor - \left\lfloor \frac{kq+r-1}{k} \right\rfloor \\ &= \left\lfloor q + \frac{r}{k} \right\rfloor - \left\lfloor q + \frac{r-1}{k} \right\rfloor \\ &= \left(q + \left\lfloor \frac{r}{k} \right\rfloor \right) - \left(q + \left\lfloor \frac{r-1}{k} \right\rfloor \right) \\ &= \left\lfloor \frac{r}{k} \right\rfloor - \left\lfloor \frac{r-1}{k} \right\rfloor \end{aligned}$$

Now, since $r < k$, if $r \neq 0$, both $\lfloor r/k \rfloor$ and $\lfloor (r-1)/k \rfloor$ are zero and so is their difference. However, when $r = 0$, we have $\lfloor r/k \rfloor = 0$ and $\lfloor (r-1)/k \rfloor = -1$ and in this case,

$$\left\lfloor \frac{n+1}{k} \right\rfloor - \left\lfloor \frac{n}{k} \right\rfloor = 1$$

The proof is complete. □

§§§1.4 Fractions and Increasing Functions

Theorem 1.4.6. *Let x be a real number. Then for every positive integers n and any integer m,*

$$\left\lfloor \frac{x+n}{m} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor + n}{m} \right\rfloor$$
$$\left\lceil \frac{x+n}{m} \right\rceil = \left\lceil \frac{\lceil x \rceil + n}{m} \right\rceil$$

Proof. We only show the equality occurs for floor function. The proof for ceiling function is almost the same and is left as an exercise to the reader. Let $f : \mathbb{R} \to \mathbb{R}$ be a function defined by $f(x) = (x+n)/m$. We want to show that $\lfloor f(x) \rfloor = \lfloor f(\lfloor x \rfloor) \rfloor$. We know that $\lfloor x \rfloor \leq x$. If $\lfloor x \rfloor = x$ (i.e., if x is an integer) there is nothing to prove. So, suppose that $\lfloor x \rfloor < x$. The function $f(x)$ is strictly increasing. That is, if $x_1 < x_2$ for two reals x_1 and x_2, then $f(x_1) < f(x_2)$. Therefore $\lfloor x \rfloor < x$ implies $f(\lfloor x \rfloor) < f(x)$. Now by part 4 of proposition 1.4.2,

$$\lfloor f(\lfloor x \rfloor) \rfloor \leq \lfloor f(x) \rfloor .$$

We will show that $\lfloor f(\lfloor x \rfloor) \rfloor < \lfloor f(x) \rfloor$ does not happen. Suppose on the contrary that it does happen. Let $k = \lfloor f(x) \rfloor$ and $y = km - n$. Then,

$$\begin{aligned} f(y) &= \frac{y+n}{m} \\ &= \frac{(km-n)+n}{m} \\ &= k \\ &= \lfloor f(x) \rfloor \end{aligned}$$

So $f(y) = \lfloor f(x) \rfloor \leq f(x)$, which implies $y \leq x$ (because f is strictly increasing). Also, $y > \lfloor x \rfloor$ because otherwise $\lfloor f(x) \rfloor = f(y) \leq f(\lfloor x \rfloor)$ and by part 2 of proposition 1.4.2, $\lfloor f(x) \rfloor \leq \lfloor f(\lfloor x \rfloor) \rfloor$, which is in contradiction with our assumption. This means that we have found an integer y such that $\lfloor x \rfloor < y \leq x$. This is obviously in contradiction with the definition of $\lfloor x \rfloor$ (since x is non-integer). Therefore, $\lfloor f(x) \rfloor = \lfloor f(\lfloor x \rfloor) \rfloor$ and we are done. □

Corollary 1.4.7. *For any given real numbers $x, a_1, a_2, \dots, a_n$, we have*

$$\lfloor \dots \lfloor \lfloor x/a_1 \rfloor /a_2 \rfloor \dots /a_n \rfloor = \left\lfloor \frac{x}{a_1 a_2 \dots a_n} \right\rfloor$$
$$\lceil \dots \lceil \lceil x/a_1 \rceil /a_2 \rceil \dots /a_n \rceil = \left\lceil \frac{x}{a_1 a_2 \dots a_n} \right\rceil$$

The above theorem can be generalized in this way:

Theorem 1.4.8. *Let f be any continuous and strictly increasing function with the property that if $f(x)$ is an integer, then so is x. Then,*

$$\lfloor f(\lfloor x \rfloor) \rfloor = \lfloor f(x) \rfloor$$
$$\lceil f(\lceil x \rceil) \rceil = \lceil f(x) \rceil$$

Problem 1.4.9. Prove that for every positive real x, the following relations hold

$$\left\lfloor \sqrt{\lfloor x \rfloor} \right\rfloor = \lfloor x \rfloor$$
$$\left\lceil \sqrt{\lceil x \rceil} \right\rceil = \lceil x \rceil$$

§§§1.4 Number of Digits

There is a reason why we have explained logarithms in details even though they are part of elementary school teachings. A good number of students can not understand the meaning of logarithm properly. Let's show a problem so you realize what we mean.

Question 1.4.10. How many digits does 57 have in base 2?

Solution. First, think of a much simpler question: how many digits does 57 have in base 10? The answer is obviously 2 digits. The reason is that any number between 10 and 100 has two digits in decimal system. In other words, the inequality $10 < 57 < 10^2$ tells us that 57 has two digits in base 10.

In general, in order to find number of digits of an integer n in base b, we must find two consecutive powers of b such that n lies between them. In fact, if $b^m < n < b^{m+1}$, then n has $m+1$ digits in base b.

In case where $n = 57$ and $b = 2$, the required inequality is $2^5 < 57 < 2^6$. Therefore, 57 has six digits when written in binary. Indeed, $57 = (111001)_2$.

We can now generalize this problem to the following proposition.

Proposition 1.4.11. *Let b and n be integers bigger than 1. Number of digits of n when presented in base b is $\lfloor \log_b n \rfloor + 1$.*

Proof. As stated in the above solution, suppose that m is the unique integer for which $b^m < n < b^{m+1}$. Then, the number of digits of n in base b is $m+1$. That is, it suffices to prove that $m = \lfloor \log_b n \rfloor$. Since b is larger than 1, we know that logarithm to base b

is a strictly increasing function. This means that we can take logarithm to base b from $b^m < n < b^{m+1}$ and the direction of the inequalities will not change. In other words,

$$\begin{aligned}\log_b b^m &< \log_b n \\ &< \log_b b^{m+1}\end{aligned}$$

which gives $m < \log_b n < m+1$. Since m is an integer, by definition of floor function, $m = \lfloor \log_b n \rfloor$. □

§§§1.4 Power of a Prime in a Number

In a lot of cases, it just happens that we need to calculate the highest power of a prime p that divides an integer n. We denote this by $v_p(n)$. Determining how many zeros there are at the end of $n!$ is a famous problem. Clearly, the number of zeros at the end of any number equals the highest power of 10 which divides that number, and this is an example of where we need to use this function.

Definition. We define $v_p(x)$ to be the greatest power in which a prime p divides x. In particular, if $v_p(x) = \alpha$, then $p^\alpha \mid x$ but $p^{\alpha+1} \nmid x$. We also write $p^\alpha \| x$, if and only if $v_p(x) = \alpha$.

Example. The greatest power of 3 that divides 63 is 3^2. because $3^2 = 9 \mid 63$ but $3^3 = 27 \nmid 63$. in particular, $3^2 \| 63$ or $v_3(63) = 2$.

Example. If p and q are two different prime numbers, then $v_p(p^\alpha q^\beta) = \alpha$. This can also be shown as $p^\alpha \| p^\alpha q^\beta$.

Proposition 1.4.12. *For any two positive integers x and y, and any prime p, we have*

$$\begin{aligned}v_p(xy) &= v_p(x) + v_p(y) \\ v_p(x+y) &\geq \min\left\{v_p(x), v_p(y)\right\}\end{aligned}$$

Proof. The first equation follows from the product rule of exponentiation ($a^s \cdot a^t = a^{s+t}$). To make sense the other equation, you can think of a simple example: take $x = 9$ and $y = 18$. Obviously, 3^3 does not divide any of x or y, but it divides their sum. □

Note. $v_p(0) = \infty$ for all primes p.

Theorem 1.4.13 (Legendre's Theorem). *Let p be a prime and n be a positive integer. Then*

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

Proof. By definition, $n!$ is the product of first n positive integers. Therefore, by proposition 1.4.12,

$$v_p(n!) = v_p(1)v_p(2)\cdots v_p(n)$$

This means that we have to find the largest power of p in each of integers $1, 2, \cdots, n$. As we were finding a solution for problem 1.4.1, we found out the answer to the question that "how many integers between 1 and n are divisible by p¡' The answer is $\lfloor n/p \rfloor$, the first term in the sum. Similarly, there are $\lfloor n/p^2 \rfloor$ numbers among these n numbers which are divisible by p^2. It is now clear that $v_p(n!)$ is the sum of $\lfloor n/p \rfloor, \lfloor n/p^2 \rfloor, \lfloor n/p^3 \rfloor, \cdots$. We have chosen the upper bound of infinity since the value these floors will be zero after somewhere. If you want to write a sum which includes only non-zero terms, the upper bound would be $v_p(n)$ (why?). □

There is another way for finding $v_p(n!)$ using bases. Before we state the alternative version of Legendre's theorem, we need a definition.

Definition. Let n be a positive integer and let p be a prime number. We denote by $s_p(n)$ the sum of the standard base p digits of n. That is, if $n = (n_k n_{k-1} \ldots n_1 n_0)_p$, then $s_p(n) = n_k + n_{k-1} + \cdots + n_1 + n_0$.

Example. $10 = (20)_5$, and so $s_5(10) = 2$.

Theorem 1.4.14. *Let p be a prime number and let n be a positive integer. Then*

$$v_p(n!) = \frac{n - s_p(n)}{p - 1}$$

Proof. Assume that the base p representation of n is $(n_k n_{k-1} \ldots n_1 n_0)_p$. So $n = n_k p^k + n_{k-1}p^{k-1} + \cdots + n_1 p + n_0$ and

$$\begin{aligned}\left\lfloor \frac{n}{p^i} \right\rfloor &= \left\lfloor \frac{n_k p^k + n_{k-1}p^{k-1} + \cdots + n_1 p + n_0}{p^i} \right\rfloor \\ &= n_k p^{k-i} + n_{k-1}p^{k-i-1} + \cdots + n_{i+1}p + n_i\end{aligned}$$

for any integer $1 \leq i \leq k$. Now by Legendre's theorem,

$$\begin{aligned}
v_p(n!) &= \sum_{i=1}^{k} \left\lfloor \frac{n}{p^i} \right\rfloor \\
&= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^k} \right\rfloor \\
&= \quad n_k p^{k-1} + n_{k-1} p^{k-2} + \cdots + n_2 p + n_1 \\
&\quad + n_k p^{k-2} + n_{k-1} p^{k-3} + \cdots + n_2 \\
&\quad \vdots \qquad\qquad \vdots \\
&\quad + n_k p \quad + n_{k-1} \\
&\quad + n_k \\
&= \sum_{i=1}^{k} n_i (p^{i-1} + p^{i-2} + \cdots + p + 1) \\
&= \sum_{i=1}^{k} n_i \frac{p^i - 1}{p - 1} \\
&= \frac{\displaystyle\sum_{i=0}^{k} n_i p^i - \sum_{i=0}^{k} n_i}{p - 1} \\
&= \frac{n - s_p(n)}{p - 1}
\end{aligned}$$

□

§§§1.4 Kummer's Theorem

It may seem difficult to find a relation for the largest power of a prime p that divides a binomial coefficient $\binom{m}{n}$. In 1852, Kummer published an article in which he introduced a very simple way to find $v_p\left(\binom{m}{n}\right)$.

Theorem 1.4.15 (Kummer's Theorem). *Let p be a prime and let m and n be positive integers such that $n \leq m$. Take s to be the number of carries when n is added to $m - n$ in base p. Then $s = v_p\left(\binom{m}{n}\right)$.*

To make a good sense of this theorem, we provide an example and then move to the proof.

Example. Let us find $v_3\left(\binom{28}{11}\right)$. First, find the base-3 representation of 11 and $28 - 11 = 17$:

$$\begin{aligned}
11 &= (102)_3 \\
17 &= (122)_3
\end{aligned}$$

Now we do the columnar addition to see how many carries happen when we add $(1001)_3$ and $(122)_3$:

$$\begin{array}{r} {\scriptstyle 1\,1\,1\,} \\ 1\,0\,2 \\ +\ 1\,2\,2 \\ \hline 1\,0\,0\,1 \end{array}$$

We see that three carries happen. Therefore, Kummer's theorem tells us that $\binom{28}{11}$ is divisible by 3^3 but not by 3^4. If we calculate the value of this binomial coefficient, we obtain

$$\begin{aligned} \binom{28}{11} &= 21474180 \\ &= 2^2 \times 3^3 \times 5 \times 7 \times 13 \times 19 \times 23 \end{aligned}$$

which verifies our result.

Let us prove Kummer's theorem now.

Proof. Let the representation of m, n, and $m-n$ in base p be

$$\begin{aligned} m &= m_k p^k + m_{k-1} p^{k-1} + \cdots + m_1 p + m_0 \\ n &= n_k p^k + n_{k-1} p^{k-1} + \cdots + n_1 p + n_0 \\ m-n &= q_k p^k + q_{k-1} p^{k-1} + \cdots + q_1 p + q_0 \end{aligned}$$

Let's find the number of carriers in addition of m and $m-n$ in base p. We can write

$$\begin{aligned} q_0 + n_0 &= m_0 + x_1 p \\ q_1 + n_1 + x_1 &= m_1 + x_2 p \\ &\vdots \\ q_k + n_k + x_k &= m_k \end{aligned}$$

where x_i denotes the carry at the $(i-1)^{th}$ digit from the right (it's either one or zero). Adding all the above equations, we find

$$\begin{aligned} (q_k + q_{k-1} + \cdots + q_0) + (n_k + n_{k-1} + \cdots + n_0) = (m_k + m_{k-1} + \cdots + m_0) \\ + (p-1)(x_k + x_{k-1} + \cdots + x_0) \end{aligned}$$

Therefore, the number of carries in the addition is

$$\begin{aligned} s &= x_k + x_{k-1} + \cdots + x_0 \\ &= \frac{(q_k + q_{k-1} + \cdots + q_0) + (n_k + n_{k-1} + \cdots + n_0) - (m_k + m_{k-1} + \cdots + m_0)}{p-1} \end{aligned}$$

We will use the fact that

$$v_p\left(\binom{m}{n}\right) = v_p(m!) - v_p(n!) - v_p((m-n)!)$$

along with Theorem 1.4.14 to show that $s = v_p\left(\binom{m}{n}\right)$. By Theorem 1.4.14, we know that for every positive integer a,

$$v_p(a!) = \frac{a - s_p(a)}{p-1}$$

where $s_p(a)$ denotes the sum of the standard base p digits of a. Therefore,

$$\begin{aligned} v_p\left(\binom{m}{n}\right) &= \frac{m - s_p(m)}{p-1} - \frac{n - s_p(n)}{p-1} - \frac{(m-n) - s_p(m-n)}{p-1} \\ &= \frac{m - (m_k + m_{k-1} + \cdots + m_0)}{p-1} \\ &\quad - \frac{n - (n_k + n_{k-1} + \cdots + n_0)}{p-1} \\ &\quad - \frac{(m-n) - (q_k + q_{k-1} + \cdots + q_0)}{p-1} \\ &= \frac{(q_k + q_{k-1} + \cdots + q_0) + (n_k + n_{k-1} + \cdots + n_0) - (m_k + m_{k-1} + \cdots + m_0)}{p-1} \\ &= s \end{aligned}$$

The proof is complete. □

Corollary 1.4.16. *Let p be a prime and let n be a positive integer. For any positive integer k such that $0 < k \leq p^n$,*

$$v_p\left(\binom{p^n}{k}\right) = n - v_p(k)$$

Proof. When you add $p^n - k$ and k in base p, you get a 1 followed by n zeros. Starting the addition from the rightmost digits and moving to the left, you get a carry as soon as both digits in the column are not zero. In other words, the first carry happens at the first (rightmost) non-zero of k in base p and you will have a carry for all digits after that. So, we are searching for the rightmost non-zero digit of k in base p. This is exactly the $(v_p(k)+1)^{th}$ digit (why?). Thus, the number of carries would be

$$(n+1) - (v_p(k)+1) = n - v_p(k),$$

which is what we wanted. □

Problem 1.4.17. Let p be a prime and let m, n be positive integers. If $p^m < n < p^{m+1}$, prove that $v_p\left(\binom{n}{k}\right) \leq m$ for every positive integer $k \leq n$.

Solution. The condition $p^m < n < p^{m+1}$ means that n has $m+1$ digits when represented in base p. By Kummer's theorem, $v_p\left(\binom{n}{k}\right)$ is the number of carries in addition $k + (n-k)$ in base p. Obviously, the number of carries must be less than number of digits of n in base p (why?). The conclusion follows.

We will provide another solution for problem 4.4.10 stated in section 4.4.

Problem 1.4.18 (China 2015). Determine all integers k such that there exists infinitely many positive integers n satisfying

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

Solution. We already know that $n+1 \mid \binom{2n}{n}$ (see solution of problem 4.4.10). We will prove that all integers except $k = 1$ satisfy the given condition. First, let us handle the case $k = 0$. In this case, choose $n = 2^m$ for any integer $m \geq 2$. By Kummer's Theorem, $v_2\left(\binom{2n}{n}\right) = 1$. On the other hand, $4 \mid n$, thus $n \nmid \binom{2n}{n}$.

For $k \neq 0, 1$, take any $m \geq 3 + \log_2 |k|$, and choose $n = 2^\alpha - k$. From Kummer's theorem, $v_2\left(\binom{2n}{n}\right) \leq m - 1$, but $n + k = 2^m$. That is, $n + k \nmid \binom{2n}{n}$ for our choice of n.

Problem 1.4.19. Let n be a positive integer. Show that n divides $\binom{n}{k}$ for all k such that $1 \leq k \leq n - 1$ if and only if n is a prime.

Solution. We will first prove that n must be a power of a prime. Suppose the contrary. Take any prime divisor p of n and let $v = v_p(n)$. By Lucas' theorem, it follows that $p \nmid \binom{n}{p^v}$, which contradicts the assumption that $n \nmid \binom{n}{p^v}$. Thus, n must be a power of a prime.

Write $n = p^r$ for some prime p and positive integer r. if $r > 1$, then from corollary 1.4.16,

$$p^2 \nmid \binom{n}{p^{r-1}}$$

which is a contradiction. Therefore, $r = 1$ and n must be a prime.

§§1.5 Some Useful Facts

In this section, we provide some theorems which may help you solve problems more easily. Though you will find that we have emphasized not to be dependent on theorems or making them the core of solving problems, they help us a great deal and make our lives a lot easier. Therefore, you will find a lot of theorems in this book. But it does not mean in any way that theorems are the best way to improve in number theory. They merely help us speed up the process of solving problems. Nothing more. One could rediscover all the theorems while solving a problem and the end result would still be the same. The point is: you can get to the top of a mountain in many ways and the view is same. But the pleasure might be different based on the approach you take. If you use a helicopter to reach the peak of the mountain or climb all the way to the top. But definitely the latter approach brings you more pleasure. Anyway, we hope you understand our primary intention.

Theorem 1.5.1. *Two integers a and b are of the same parity if and only if their sum and difference is even. Equivalently, they are of different parity if their sum and difference is odd.*

Corollary 1.5.2. *Exactly one of the two integers a and b is even if and only if $a \pm b$ is odd.*

Theorem 1.5.3. *Every positive integer n can be written in the form $n = 2^k s$, where k is a non-negative integer and s is an odd positive integer.*

Note.

1. Here, k is the largest power of 2 that divides n. Therefore, s must be odd. Moreover, s is the largest odd divisor of n. Notice that if n is odd, then $k = 0$ and $s = n$.

2. One can write any positive integer n as $n = p^k s$, where p is a prime, k is a non-negative, and s is an integer relatively prime to p. The case $p = 2$ (above theorem) is usually used in problem solving (and sometimes even in some combinatorics problems).

Problem 1.5.4. Let n be a positive integer and let $S = \{1, 2, \cdots, 2n\}$. Choose $n + 1$ numbers $a_1, a_2, \cdots, a_{n+1}$ out of S so that

$$a_1 < a_2 < \cdots < a_{n+1}$$

Prove that $a_i \mid a_j$ for some integers $1 \leq i, j \leq n + 1$ with $i \neq j$.

Solution. Write all members of S in the form $2^\alpha \beta$, where α is non-negative and β is the odd factor. There are exactly n odd numbers among $1, 2, \cdots, 2n$. Therefore, by pigeonhole principle[11], among $n + 1$ selected numbers $a_1, a_2, \cdots, a_{n+1}$, there exist at least two numbers a_i and a_j (with $i \neq j$) which have the same odd factor. In other words,

$$a_i = 2^{\alpha_1} \beta$$
$$a_j = 2^{\alpha_2} \beta$$

Now, $a_i \mid a_j$ if $\alpha_1 \leq \alpha_2$, and $a_j \mid a_j$ otherwise.

Theorem 1.5.5. *Every composite positive integer n can be written as ab where a and b are relatively prime positive integers larger than 1.*

Theorem 1.5.6. *$(n-1)!$ is divisible by n if and only if $n > 4$ is a composite integer or $n = 1$.*

Proof. The case $n = 1$ is trivial. For $n = 2, 3, 4$ we can check by hand. For $n > 4$, if n is a prime, n does not share a factor with any of $1, 2, \cdots, n - 1$. Consequently, n does not divide their product $(n - 1)!$. If n is composite, we can write $n = ab$ with a and b larger than n and $a \neq b$. Since $a \neq b$ and $(n - 1)!$ contains both a and b in the product, $n = ab \mid (n - 1)!$. □

[11]The pigeonhole principle states that if n items are put into m containers, with $n > m$, then at least one container must contain more than one item.

Theorem 1.5.7 (Four Numbers Theorem). *Let a, b, c, and d be four positive integers such that $ab = cd$. Then there exist four positive integers r, s, t and u so that*

$$a = rs$$
$$b = tu$$
$$c = rt$$
$$d = su$$

Proof. Let $(a, c) = g_1$. By proposition (1.2.8), there exist integers x_1 and y_1 such that $a = g_1 x_1$ and $c = g_1 y_1$ with $x_1 \perp y_1$. Also, let $(b, d) = g_2$, then there exist integers x_2 and y_2 such that $b = g_2 x_2$ and $d = g_2 y_2$ with $x_2 \perp y_2$. Substitute these equations into the given equation $ab = cd$ to get

$$g_1 g_2 x_1 x_2 = g_1 g_2 y_1 y_2$$

or simply $x_1 x_2 = y_1 y_2$. We claim that $x_1 = y_2$ and $x_2 = y_1$. To prove this claim, we use a trick. Observe that $x_1 x_2 = y_1 y_2$ means $x_1 \mid y_1 y_2$. The second part of Proposition (1.2.4) tells us that since $x_1 \perp y_1$, we must have $x_1 \mid y_2$. With the same reasoning, one can show that $y_2 \mid x_1$. It follows by proposition (1.1.3) that $x_1 = y_2$. One can similarly show that $x_2 = y_1$. Compare the parameters in the theorem with the ones we just used and take $r = g_1, s = x_1, t = x_2$, and $u = g_2$. The proof is complete. □

Theorem 1.5.8. *For positive integers a, b, n, and e, suppose that $a \perp b$ and $ab = n^e$. Then there exist positive integers x and y such that $a = x^e$ and $b = y^e$. In other words, if product of two relatively prime positive integers is a perfect e^{th} power, then both of them should be perfect e^{th} powers.*

Proof. Let us consider the prime factorization of a and b as the following.

$$a = p_1^{e_1} \cdots p_k^{e_k}$$
$$b = q_1^{f_1} \cdots q_\ell^{f_\ell}$$

Then,

$$ab = p_1^{e_1} \cdots p_k^{e_k} q_1^{f_1} \cdots q_\ell^{f_\ell}$$

From uniqueness of prime factorization, the only prime factors of n must be $p_1, \cdots, p_k$ and $q_1, \cdots, q_\ell$. Let $n = p_1^{a_1} \cdots p_k^{a_k} q_1^{b_1} \cdots q_\ell^{b_\ell}$. Then

$$n^e = p_1^{a_1 e} \cdots p_k^{a_k e} q_1^{b_1 e} \cdots q_\ell^{b_\ell e}$$

Since $ab = n^e$, we get

$$p_1^{e_1} \cdots p_k^{e_k} q_1^{f_1} \cdots q_\ell^{f_\ell} = p_1^{a_1 e} \cdots p_k^{a_k e} q_1^{b_1 e} \cdots q_\ell^{b_\ell e}$$

The exponents of the primes in both sides must be equal. Therefore, $e_i = a_i e$ (for $i = 1, 2, \ldots, k$) and $f_j = b_j e$ (for $j = 1, 2, \ldots, \ell$). Therefore,

$$a = \left(p_1^{a_1} \cdots p_k^{a_k}\right)^e$$
$$b = \left(q_1^{b_1} \cdots q_\ell^{b_\ell}\right)^e$$

which proves the claim. □

Note. You should think about why we considered the prime factorization and try to understand what led us into that way of thinking.

Corollary 1.5.9. *If a and b are relatively prime positive integers such that ab is a perfect square, then a and b both are perfect squares.*

Theorem 1.5.10. *Let a, b, and c be positive integers such that $ab = c^2$. Then there exist integers g, u, and v with $u \perp v$ so that*

$$\begin{aligned} a &= gu^2 \\ b &= gv^2 \\ c &= guv \end{aligned}$$

Proof. Let $g = (a, b)$. Then there exist relatively prime integers x and y such that $a = gx$ and $b = gy$. Then $g^2xy = c^2$ so that $g^2 \mid c^2$, or $g \mid c$ (see the example provided right after proposition (1.2.1) for a proof). This implies that there exists some positive integer k for which $c = gk$. Substituting this into the equation, we find $k^2 = xy$ with $x \perp y$. From corollary (1.5.9), there exist integers u and v such that $x = u^2$ and $y = v^2$. Thus, $a = gu^2, b = gv^2$, and $c = guv$. □

Now, we introduce a simple but really useful method for factorization: Simon's Favorite Factorization Trick[12], or SFFT in brief.

Proposition 1.5.11 (SFFT). *For any real numbers x, y, j, and k, the following relation holds:*

$$xy + xk + yj + jk = (x + j)(y + k)$$

Two special common cases are

$$\begin{aligned} xy + x + y + 1 &= (x + 1)(y + 1) \\ xy - x - y + 1 &= (x - 1)(y - 1) \end{aligned}$$

Let's see the motivation behind this trick. Once Mr. Simon was studying number theory, he found this problem: find all positive integers x and y such that $xy - x + y = 49$. Simon probably hates expressions of this form because he cannot factorize them. However, if he adds -1 to both sides of his equation, he finds the nice and factored form $(x + 1)(y - 1) = 48$, which is much easier to solve than the original equation. In fact, to solve the factorized equation, he only needs to find the divisors of 48 (see theorem Theorem 1.5.15 for more details). If you look closely, SFFT is inspired by the so-called Completing the Square Method:

$$x^2 + kx + \frac{k^2}{4} = \left(x + \frac{k}{2}\right)^2$$

In fact, the act of adding jk to $xy + xk + yj$ in order to be able to factor it could be called completing the rectangle in analogy to the famous *completing the square* trick.

[12]Named after Simon Rubinstein-Salzedo, a member of AoPS.

Theorem 1.5.12. *If N is the least common multiple of positive integers upto n, that is, $N = [1, 2, \cdots, n]$, then for a prime p, the maximum integer α for which $p^\alpha \mid N$ is the unique non-negative integer α so that $p^\alpha \leq n < p^{\alpha+1}$. In other words, if p_i is a prime less than or equal to n, and for that prime, α_i is the unique integer such that $p_i^{\alpha_i} \leq n < p_i^{\alpha_i+1}$ then,*

$$N = p_1^{\alpha_1} \cdots p_k^{\alpha_i}$$

We can write α_i in terms of n and p_i using logarithm. Actually, α_i is the greatest non-negative integer less than or equal to $\log_{p_i}(n)$.

The proof in fact follows from the definition of least common multiple. Try some examples yourself and prove it. Also, we often use this kind of argument using logarithm to find some boundaries in some problems.

Theorem 1.5.13. *The square of every odd integer leaves a remainder of 1 when divided by 8.*

Proof. We can write each odd integer n in the form $n = 2k - 1$ for some $k \in \mathbb{Z}$. Then

$$\begin{aligned} n^2 &= (2k-1)^2 \\ &= 4k^2 - 4k + 1 \\ &= 4k(k-1) + 1 \end{aligned}$$

Since one of k or $k-1$ must be even (why?), we can write $k(k-1) = 2\ell$ for some integer ℓ. Then $n^2 = 8\ell + 1$, and so n^2 leaves a remainder of 1 when divided by 8. □

Theorem 1.5.14. *Every number of the form $4k + 3$ has at least one prime factor of the form $4k + 3$.*

Proof. The idea comes from the fact that if we multiply two numbers of the form $4k+1$, say $4a + 1$ and $4b + 1$, the result will be

$$\begin{aligned} (4a+1)(4b+1) &= 16ab + 4a + 4b + 1 \\ &= 4(4ab + a + b) + 1 \end{aligned}$$

which is, again, of the form $4k + 1$. Clearly, all prime factors of a number n of the form $4k+3$ are odd, and therefore are either of the form $4k+1$ or $4k+3$. If all prime factors of n are of the form $4k+1$, then by the logic represented in above lines, any product of powers of these primes, including n, should be of the form $4k + 1$. So, we get a contradiction and there exists at least one prime factor of n which is of the form $4k + 3$. □

Theorem 1.5.15. *Let n be a positive integer. The number of pairs (a, b) of positive integers which satisfy the equation*

$$ab = n$$

is $\tau(n)$, where $\tau(n)$ is the number of positive divisors of n.

The following example gives you an idea for the proof.

Example. Take $n = 6$. The only positive divisors of n are $1, 2, 3$, and 6. Therefore, $\tau(6) = 4$. On the other hand, the equation $ab = 6$ has exactly four solutions $(1, 6), (2, 3), (3, 2)$, and $(6, 1)$.

We will study $\tau(n)$ in details in Chapter Chapter 3.

Theorem 1.5.16. *Every prime greater than 3 is either of the form $6k + 1$ or of the form $6k - 1$.*

Proof. Consider an integer n. By definition (1.1), the minimum absolute remainder r of n upon division by 6 has the property that $|r| \leq 6/2 = 3$. In other words, r can have the values $1, 2, 3, -1, -2$, and -3. For this reason, we can write an integer in exactly one of the following forms:

$$6k - 2, 6k - 1, 6k, 6k + 1, 6k + 2, 6k + 3$$

Numbers of the form $6k - 2, 6k + 2, 6k, 6k + 3$ cannot be prime because the first two are divisible by 2 and the last two are divisible by 3. Thus, if n is a prime, it must be either $6k - 1$ or $6k + 1$. □

Using the above theorem, we can prove the following.

Theorem 1.5.17. *For a prime $p > 3$, $24 \mid p^2 - 1$.*

Proof. We can assume $p = 6k \pm 1$ for some integer k. So

$$\begin{aligned} p^2 &= (6k \pm 1)^2 \\ &= 36k^2 \pm 12k + 1 \\ &= 12k(3k \pm 1) + 1 \end{aligned}$$

Note that $(k) + (3k \pm 1)$ is odd. From corollary (1.5.2), k and $3k \pm 1$ have different parity and $k(3k \pm 1)$ is divisible by 2. Let $k(3k \pm 1) = 2\ell$, then $p^2 = 24\ell + 1$, or $p^2 - 1 = 24\ell$, which proves the theorem. □

Theorem 1.5.18. *If the sum of two positive integers is a prime, they are relatively prime to each other.*

Proof. Assume that $a + b = p$, where p is a prime. If $(a, b) = g$ then there exist relatively prime positive integers x and y for which $a = gx$ and $b = gy$. So,

$$p = a + b = g(x + y)$$

which means g divides p. Since p is a prime, its only divisors are itself and 1. Hence, the only possible values for g are 1 and p. However, $g = p$ cannot happen since otherwise $x + y = 1$ would lead to one of x or y being zero. Thus, $(a, b) = g = 1$. □

Theorem 1.5.19. *For any positive integer n,*

$$a^n - b^n = (a - b)\left(a^{n-1} + a^{n-2}b + \cdots + b^{n-1}\right)$$

Furthermore, if n is odd, then

$$a^n + b^n = (a + b)\left(a^{n-1} - a^{n-2}b + \cdots + b^{n-1}\right)$$

Proof. We can just use induction on n, but we will try to avoid using induction as much as possible. For the first identity, define

$$S = a^{n-1} + a^{n-2}b + \cdots + b^{n-1}$$

Then, $aS = a^n + a^{n-1}b + \cdots + b^{n-1}a$ and $bS = a^{n-1}b + a^{n-2}b^2 + \cdots + b^n$. Subtracting, we obtain

$$(a-b)S = a^n - b^n$$

which finishes the proof. The second identity can be proved by using the first identity and the fact that when n is odd, we have $a^n + b^n = a^n - (-b)^n$. □

Corollary 1.5.20. *Let a and b be any two integers. Then $a - b$ divides $a^n - b^n$ for all positive integers n. Also, $a + b$ divides $a^n + b^n$ for odd n.*

Theorem 1.5.21. *Let a, m, and n be positive integers. Then, $a^m - 1 \mid a^n - 1$ if and only if $m \mid n$.*

Proof. We will first show that if $m \mid n$, then $a^m - 1 \mid a^n - 1$. Notice that if $m \mid n$, that there exists a positive integer h such that $n = mh$, and so,

$$\begin{aligned} a^n - 1 &= a^{mh} - 1 \\ &= \left(a^m\right)^h - 1 \end{aligned}$$

Let $x = a^m$. By corollary (1.5.20), $x - 1 = a^m - 1$ divides $x^h - 1 = a^n - 1$, as desired.

Let us now show the other side. If $a^m - 1 \mid a^n - 1$, then,

$$a^m - 1 \mid a^n - 1 - (a^m - 1) = a^n - a^m = a^m(a^{n-m} - 1)$$

Since $a^n - 1 \perp a^m$ (why?), we have $a^n - 1 \mid a^{n-m} - 1$ by second part of proposition (1.2.4). Repeating the same process, we find $a^n - 1 \mid a^{n-2m} - 1$. This suggests us to take $n = mq + r$ so that $0 \leq r < m$. Then, we will have $a^n - 1 \mid a^{n-mq} - 1 = a^r - 1$. Evidently, $a^r - 1 < a^m - 1 \leq a^n - 1$, which forces $a^r - 1 = 0$. So, $r = 0$ and $n = mq$. The proof is complete. □

Theorem 1.5.22. *If $a^k - 1$ is a prime for positive integers a and $k > 1$, then $a = 2$ and k must be a prime.*

Proof. As we already know,

$$a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + \cdots + a + 1)$$

If $a > 2$, then $a - 1$ will divide $a^k - 1$ which is absurd because $a^k - 1$ is a prime. So, a must be 2. Suppose that k is composite. Then, $k = p\ell$ for some prime p and integer $\ell > 1$. Therefore,

$$\begin{aligned} a^k - 1 &= \left(a^p\right)^\ell - 1 \\ &= \left(a^p - 1\right)\left(a^{p(\ell-1)} + a^{p(\ell-2)} + \cdots + 1\right) \end{aligned}$$

which is impossible. Hence, k must be a prime. □

Remark. The numbers of the form $2^n - 1$ are called *Mersenne numbers* and denoted by M_n. According to the theorem, if M_n is a prime, then n must also be a prime.

Theorem 1.5.23. *Let a and k be positive integers. If $a^k + 1$ is an odd prime, then a is even and k is a power of 2.*

See Problem 1.6.17 for a proof.

Remark. For the particular case when $a = 2$, the numbers $2^{2^n} + 1$ are called *Fermat numbers* and denoted by F_n. Notice that the reverse of the above theorem does *not* hold. That is, not all Fermat numbers are primes. For instance,

$$F_5 = 2^{2^5} + 1 = 4\,294\,967\,297 = 641 \times 6\,700\,417$$

Theorem 1.5.24. *For two relatively prime positive integers a and b,*

$$(a^m - b^m, a^n - b^n) = a^{(m,n)} - b^{(m,n)}$$

Proof. Here, we will use Euclidean algorithm as the idea is applicable to many similar problems. If $m = n$, the result is trivial since both sides are $a^m - b^m$. So, we can take $m > n$ without loss of generality[13]. Then we can write $m = n + k$ for some $k \in \mathbb{N}$. Therefore,

$$\begin{aligned} a^m - b^m &= a^{n+k} - b^{n+k} \\ &= a^n(a^k - b^k) + b^k(a^n - b^n) \end{aligned}$$

Thus, by Euclidean algorithm,

$$\begin{aligned} (a^m - b^m, a^n - b^n) &= (a^n(a^k - b^k) + b^k(a^n - b^n), a^n - b^n) \\ &= (a^n(a^k - b^k), a^n - b^n) \end{aligned}$$

Since a and b are relatively prime, $a^n \perp a^n - b^n$ (why?). This gives us

$$(a^m - b^m, a^n - b^n) = (a^n - b^n, a^k - b^k)$$

Note that, this is the descending step of Euclidean algorithm! If we repeat the same process a couple of times, we would eventually reach (m, n) in the exponent. □

As a conclusion to this chapter, we define *factorial* and *binomial coefficient*.

Factorial. Let n be a positive integer. The *factorial* of n, denoted by $n!$, is the product of all positive integers less than or equal to n. That is,

$$n! = 1 \times 2 \times \cdots \times n$$

For convenience, we define 0! to be one.

Binomial Coefficient. Let n and k be non-negative integers such that $k \leq n$. The *Binomial Coefficient* indexed by n and k is denoted by $\binom{n}{k}$ (read "*n choose k*") and is equal to

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

[13] Wherever there is symmetry, don't forget to use this trick!

Proposition 1.5.25. *The binomial coefficient is an integer.*

Hint. Use Problem 6.2 in chapter Chapter 6.

You are probably familiar with the *binomial theorem*. We state this theorem here because of its high importance but do not prove it. Interested reader may see some related identities in PBinomial Theorem and Binomial Identities.

Theorem 1.5.26 (Binomial Theorem). *For any positive integer n,*

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{1}ab^{n-1} + b^n$$

Theorem 1.5.27. *Let n be a positive integer. Then, n is a prime if and only if n divides $\binom{n}{k}$ for all $0 < k < n$.*

For now, we will be proving only the first part.

Proof. We already know that

$$k\binom{p}{k} = p\binom{p-1}{k-1}$$

Obviously, the right side is divisible by p, so must be the left side. From the definition of prime numbers, $p \perp k$. So, by the second part of the previous proposition, we can say p must divide $\binom{p}{k}$. □

§§1.6 Solved Problems

Well, now that we have a basic understanding of how divisibility relations work, it is the time to see how to apply those propositions to solve problems. Let us start with some really easy problems so that the reader has a firm idea about how to approach a problem. We will gradually discuss more difficult problems. Most importantly, we will not focus on how to use theorems to solve problems or implement them. We want to improve the intuitive ability of the reader instead.

Problem 1.6.1. Find all positive integers n so that n divides $n+3$.

This can be solved in a variety of ways. Before we solve this, it would be pleasant to share some experience. This may not directly help readers understand how to solve the problem, but it may help them understand how different people think when they encounter a problem.

The first author was coaching a group of average students who barely had the idea of problem solving back in 2014. After showing them some basic facts about divisibility, he threw this problem at them. Here is how they approached it: most of them started trial and error to find the solution. They were checking different values for n to see

if they satisfy the condition. Not all student could realize that this method will not work in general *for all numbers* even if you find some initial solutions. One or two of the students went for the idea that if n divides $n+3$, then $n+3$ is at least twice n. However, when increasing n, $2n$ becomes larger than $n+3$ after some n, and this leads to a solution. Another student solved the problem in the old fashioned way: by division process. That is, he divided $n+3$ by n and found out that n must divide 3. Other than those few students, most of them got that $n=1$ and $n=3$ work but could not prove that these are the only solutions. In fact, that is the most difficult part of solving a number theory problem.

When you encounter a problem in mathematics, you probably come up with an assumption. For instance, in this problem, you may assume that the only solutions are 1 and 3. Most of the times our observations are true, but in many cases there are counter examples or some cases where our assumption fails. In our problem, if we just say the only solutions to the problem are 1 and 3 without proving it, we must tolerate comments such as "How do you know there is not any large n which is also a solution?" That is why we have to prove everything we claim is true. Of course, if our claim is implied from a well-known theorem in mathematics, we can skip the proof and refer to the theorem. However, if the claim is totally new or relies on theorems which are not well known, we have to provide a proof. Obviously, the reader of your proof defines the famousness of the theorems you are allowed to use. There must be a huge difference in the way you solve a problem when you are explaining it to a math teacher or to a sixth grade student. By the way, when writing a solution to a problem at an olympiad test (or any other sophisticated exam), be careful not to consider every theorem obvious or well known. Whatever the problem is, try to prove every claim that you make.

A suggestion: while reading a solution, try to find the motivation behind its idea rather than understanding it or learning the technique used in the solution.

Solution (Old-fashioned Way). Since $n \mid n+3$, the fraction $\dfrac{n+3}{n} = 1 + \dfrac{3}{n}$ is a positive integer. This shows that $\dfrac{3}{n}$ must be an integer. Therefore, n divides 3 and the only possible values for n are 1 and 3.

Solution (A Smarter Way). We know that if $a \mid b$ and $a \mid c$, then $a \mid b-c$. But how can we know what to subtract? If m is a given constant, we can easily find all numbers n such that $n \mid m$ just as in the previous solution. See that the right side of $n \mid n+3$ has a variable n which is not constant. So, we need to remove it somehow. This is where divisibility rules come into play. We can now subtract $n \mid n$ from $n \mid n+3$ from to obtain $n \mid (n+3)-n = 3$ or $n \mid 3$. In words, n is a divisor of 3 which has namely two divisors 1 and 3. Thus, n can be 1 or 3.

Solution (Another Smart Solution). For positive integers a and b, if $a \mid b$, $b \geq a$. Now, since $n+3$ cannot be equal to n, if it has to be divisible by n, it must be at least twice n, i.e., $n+3 \geq 2n$. This forces $3 \geq n$ and so n is one of $1, 2$, or 3. There are only three values so we can check them by hand and get the answer.

Note the difference between the first and the second solution. There are pretty much no differences other than the fact that the latter is more systematic. You will eventually find that solving problems this way is particularly useful in Olympiads.

For now, we will keep the use of inequality in store and solve a few problems by twisting up left and right sides of divisibility relations.

Problem 1.6.2. Find all $n \in \mathbb{N}$ so that $n \mid 2n + 3$.

Solution. This time we have to remove n like before, but notice that there is an extra 2 attached.

We can overcome this easily: just see that $n \mid 2n$ and then it is the same as the previous problem: $n \mid 2n + 3 - 2n = 3$.

Problem 1.6.3. Find all $n \in \mathbb{N}$ so that $n + 1 \mid 3n + 4$.

Solution. The left side contains more than just a n, but it does not make any difference. We have $n + 1 \mid 3(n + 1) = 3n + 3$ and it is given in the problem that $n + 1 \mid 3n + 4$. Subtracting,

$$n + 1 \mid 3n + 4 - (3n + 3) = 1$$

which means $n+1$ must be 1. This is impossible because $n+1$ is a positive integer greater than 1.

Note. When dealing with a divisibility relation $k \mid m$ in which m is constant, there are $\tau(m)$ possible values for k, where $\tau(m)$ is the number of positive divisors of m (why?).

Try to do the following problem yourself before reading the solution.

Problem 1.6.4. Find all $n \in \mathbb{N}$ which satisfies $4n + 2 \mid 6n + 5$.

Solution. There are coefficients on both sides of divisibility now. Still it can be overridden but it is a bit tricky. See that $4n + 2 \mid 3(4n + 2) = 12n + 6$ and also $4n + 2 \mid 2(6n + 5) = 12n + 10$. Now that the coefficients are matched, we can subtract and find

$$4n + 2 \mid 12n + 10 - (12n + 6) = 4$$

So, $4n + 2$ must be one of $1, 2$, or 4. None of these values give a valid solution for n.

If you have not noticed already, this idea can be generalized to find all n satisfying $an + b \mid cn + d$, where a, b, c, and d are integers. Then what shall we multiply both sides with? Here is a hint: consider the lcm of a and c. Why a and c?

Problem 1.6.5. Find all positive integers n for which $8n + 9 \mid 12n + 5$.

Solution. Our working principle is: we want to eliminate the variables on the right side so we get a constant value. That is, we want the right side to be a number, not a variable. In order to do this, we must construct two divisibility relations to subtract from each other and get a constant value. In other words, we have to find a and b such that the difference of right sides of $8n + 9 \mid a(8n + 9)$ and $8n + 9 \mid b(12n + 5)$ does not include n. So, the coefficients of n must be equal in the two. The minimum value for this common

coefficient will be the lcm of 8 and 12, which is $[8, 12] = 24$. Therefore, $a = 3$ and $b = 2$ and hence,

$$8n + 9 \mid 3(8n + 9) = 24n + 27$$
$$8n + 9 \mid 2(12n + 5) = 24n + 10$$

Thus, $8n + 9 \mid 24n + 27 - (24n + 10) = 17$ and $8n + 9$ is either 1 or 17. The equation $8n + 9 = 1$ does give a valid solution. So, the only solution is obtained from $8n + 9 = 17$, which gives $n = 1$.

Problem 1.6.6 (Dhaka Divisional Olympiad, 2010). Find all positive integers n greater for which divides $n + 4$ and $n + 12$ for some positive integer n.

Solution. We are asked to find positive integers which would divide $n + 4$ and $n + 12$ both, no matter what. If d is such a positive integer then

$$d \mid n + 4$$
$$d \mid n + 12$$
$$d \mid (n + 12) - (n + 4) = 8$$

We immediately get that $d \in \{1, 2, 4, 8\}$.

Problem 1.6.7. Find all primes p so that $9p + 1$ is also a prime.

Solution. This can be done easily considering parity. When you encounter a problem with primes (especially if you are asked to find a prime), it may be helpful to separate the problem into two cases. The first case is $p = 2$ which works here. The second case is when p is odd. It is trivial that as p is odd, $9p + 1$ is even. However, we want $9p + 1$ be a prime. This is a contradiction because $9p + 1$ is larger than 2. Therefore, the only solution is $p = 2$ for which $9p + 1 = 19$ is also a prime.

Problem 1.6.8. Find all positive integers n so that $7n + 1 \mid 8n + 55$.

Solution. Since $[8, 7] = 56$, the two required relations would be

$$7n + 1 \mid 8(7n + 1) = 56n + 8$$
$$7n + 1 \mid 7(8n + 55) = 56n + 385$$

By subtracting, we find $7n + 1 \mid 377$. Now, we have to find divisors of 377. When you are stuck with finding divisors, instead of trying random numbers or testing the numbers $2, 3, 4, 5, \ldots$ serially to find if they divide 377, try a more efficient approach which reduces your effort significantly. By proposition (1.1.12), if n is composite, then it must have a prime factor less than or equal to $\sqrt{n}$. Since $\sqrt{377} \approx 19.4$, it suffices to check which primes less than or equal to 19 divide 377. These primes are $2, 3, 5, 7, 11, 13, 17, 19$.

- $2 \nmid 377$ since the rightmost digit is odd,
- $3 \nmid 377$ since the sum of digits is 17,
- $5 \nmid 377$ because the number ends in 7,

- $7 \nmid 377$ because $377 = 7 \cdot 53 + 6$,
- $11 \nmid 377$ as the difference of sum of altering digits is $(3 + 7) - 7 = 3$,
- $13 \mid 377$ because $37 + 4 \cdot 7 = 65 = 13 \cdot 5$.

So, we find the factorization of 377 to be $377 = 13 \cdot 29$. This means that $7n + 1$ is a divisor of $13 \cdot 29$. Notice that $7n + 1$ is a number which leaves remainder 1 when divided by 7. Therefore, look for numbers among 13, 29, 13, and 377 which leave a remainder of 1 when divided by 7. The only possibility is $7n + 1 = 29$, which gives $n = 4$.

Problem 1.6.9. Find all $n \in \mathbb{N}$ for which $n + 3$ divides $n^2 + 2$.

We should again remove the variables from the rights side of $n + 3 \mid n^2 + 2$. Here are two solutions for the problem.

Solution (First Solution). First, multiply $n + 3$ by n to get

$$n + 3 \mid n^2 + 3n$$

Now, subtract this from the given relation to find

$$n + 3 \mid 3n - 2$$

The problem is now similar to the ones we solved earlier. In fact, subtracting

$$n + 3 \mid 3n + 9$$
$$n + 3 \mid 3n - 2$$

we obtain $n + 3 \mid 11$ which immediately gives $n = 8$ as the only solution.

Solution (Second Solution). This one is more elegant. In order to avoid the second step, we can directly multiply $n + 3$ by $n - 3$ to obtain

$$n + 3 \mid n^2 - 9$$

Subtracting from the original relation, $n + 3 \mid n^2 + 2 - (n^2 - 9)$ or $n + 3 \mid 11$, and we find the same solution as before.

Problem 1.6.10. Find the greatest positive integer x for which

$$x + 10 \mid x^3 + 10$$

Solution. Since 3 is odd, we can use corollary (1.5.20) to write $x + 10 \mid x^3 + 10^3$. So,

$$x + 10 \mid (x^3 + 1000) - (x^3 + 10) = 990$$

and the answer is $x = 980$.

Problem 1.6.11. Find all positive integers n so that $n^6 + n^4$ is divisible by $7n + 1$.

Solution. How do we approach this problem? One idea is to go ahead like we did in the first solution of problem (1.6.9), by eliminating powers of n one by one. Here is a better solution.

First write it as, $7n+1 \mid n^4(n^2+1)$. The problematic part is n^4. Many beginners make mistakes in such situations claiming that $7n+1$ does not divide n^4, and so $7n+1 \mid n^2+1$. This is wrong. In general, the following statement is wrong:

> For positive integers a, b, and c, if $a \mid bc$ and b is not divisible by a, then $a \mid c$.

This is another common mistake new problem solvers make. You can check this using an example: 14 divides $28 = 7 \times 4$ but 14 does not divide 7. But in this problem, we can still take n^4 off because n^4 is relatively prime to $7n+1$. Just notice that $7n+1$ leaves a remainder of 1 when divided by n, so $n \perp 7n+1$. Evidently, $n^4 \perp 7n+1$ by part 4 of proposition (1.2.4). Using part 2 of the same proposition, we can cancel out n^4 and get

$$7n+1 \mid n^2+1$$

Multiply n^2+1 by 49 to find $7n+1 \mid 49n^2+49$. On the other hand, $7n+1$ divides $(7n+1)(7n-1) = 49n^2-1$, and so,

$$7n+1 \mid (49n^2+49) - (49n^2-1) = 50.$$

Note that $7n+1$ leaves a remainder of 1 when divided by 7. Therefore, we look for divisors of 50 which leaves a remainder 1 when divided by 7. The divisors of 50 are $1, 2, 5, 10, 25$, and 50. Only 1 and 50 leave the desired property among these numbers. Since n is a positive integer, $7n+1 \geq 7 \cdot 1 + 1 = 8$. Therefore, $7n+1 = 50$ or $n = 7$.

Remark. We could handle the last part in another way. Write $7n+1 \mid (n^2+1)-(7n+1)$, so that

$$\begin{aligned} & 7n+1 \mid n^2-7n \\ \implies & 7n+1 \mid n(n-7) \end{aligned}$$

Again, $n \perp 7n+1$ implies $7n+1 \mid n-7$. If $n = 7$, we have a solution. Otherwise, $7n+1$ would have a larger value than $|n-7|$ and we get a contradiction.

Problem 1.6.12. If $ax+by = 1$, find (a, b).

Solution. Assume that $(a, b) = g$. Then we can find two relatively prime integers m and n so that $a = gm$ and $b = gn$. Setting these into the given equation, we observe $g(mx+ny) = 1$. This implies that g divides 1, and so $g = 1$.

Note. We can similarly show that $(x, y) = (x, b) = (a, y) = 1$.

Problem 1.6.13. Find the number of solutions to the equation

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{2015}$$

in positive integers.

Solution. We can rewrite the equation as

$$\frac{x+y}{xy} = \frac{1}{2015}$$

Multiplying both sides by $2015xy$, we find $xy = 2015(x+y)$. This can be represented as

$$(x-2015)(y-2015) = 2015^2$$

According to theorem Theorem 1.5.15, we get that the number of solutions is the number of positive divisors of 2015^2, $\tau(2015^2)$.

Note. Did you realize that this was actually SFFT? And what do you think the result would be if we considered solutions in integers (not necessarily positive)?

Problem 1.6.14. Find all $n \in \mathbb{N}$ such that $2^n + n \mid 8^n + n$.

Solution. There is 8 on the right side and 2 on the left side. Since $8 = 2^3$, this should certainly provoke us to use the fact that $a + b \mid a^3 + b^3$. In this case,

$$\begin{aligned} & 2^n + n \mid (2^n)^3 + n^3 \\ \implies & 2^n + n \mid 8^n + n^3 \\ \implies & 2^n + n \mid (8^n + n^3) - (8^n + n) \\ \implies & 2^n + n \mid n^3 - n \end{aligned}$$

Now we need to find all n such that $2^n + n \mid n^3 - n$. If you play around with the small values of n, you will clearly see that 2^n grows a lot faster than n^3. Since $2^n + n \mid n^3 - n$, we must have

$$2^n + n \leq n^3 - n.$$

The following lemma gives us the limit we need for n. Once again, you have to prove it. You can use induction to do so (can you use logarithm?).

Lemma 1.6.15. *For $n > 9$, the inequality $2^n + n > n^3 - n$ holds.*

By the lemma, if $n > 9$, there are no solutions. Now we are left with a few possibilities for n because n must be less than or equal to 9. We can easily check by hand that there are no solutions for this case as well.

Problem 1.6.16 (IMO 1959, Problem 1). Prove that for any integer n, the fraction

$$\frac{14n+3}{21n+4}$$

is irreducible.

Solution. We must make sense of the problem first. It asks to prove that a fraction is irreducible. That means the fraction cannot be simplified anymore. In other words, we must prove that the numerator $(14n+3)$ and denominator $(21n+4)$ of the fraction are relatively prime to each other. How do we prove this? We will show this in two ways:

1. Let $g = (14n+3, 21n+4)$. Then,

$$g \mid 14n+3$$
$$g \mid 21n+4$$

We already know we have to prove that $g = 1$. So, let us try to remove the n on the right side. Since $[14, 21] = 42$ and $42 = 14 \cdot 3 = 21 \cdot 2$, we can make use of the following two relations:

$$g \mid 3(14n+3) = 42n+9$$
$$g \mid 2(21n+4) = 42n+8$$

Thus, $g \mid (42n+9) - (42n+8) = 1$ and $g = 1$.

2. Take $14n+3 = gx$ and $21n+4 = gy$ for some integers x and y. Note that $3(14n+3) - 2(21n+4) = 1$, and so

$$3gx - 2gy = 1$$

or $g(3x-2y) = 1$. So, $g \mid 1$ and this gives us the same result $g = 1$.

Remark. You should understand that both solutions are essentially the same, but with different approaches or thinking styles.

Problem 1.6.17. Show that if a prime is of the form 2^n+1, then $n = 2^m$ for some integer m.

Solution. According to theorem Theorem 1.5.3, write $n = 2^m s$, where s is an odd positive integer. By theorem (1.5.19), we can write

$$\begin{aligned} p = 2^n + 1 = 2^{2^m s} + 1 &= \left(2^{2^m}\right)^s + 1 \\ &= \left(2^{2^m} + 1\right)\left(2^{2^m(s-1)} + 2^{2^m(s-2)} + \cdots + 2^{2^m} + 1\right) \end{aligned}$$

Clearly, as p is a prime, this is impossible unless $s = 1$. So $n = 2^m$.

Problem 1.6.18. Find all integer solutions to the equation

$$a(b+1) + b(c+1) + c(a+1) + abc = 0$$

Solution. Yes, this looks similar to SFFT. It has three variables instead of two, so we cannot directly use Simon's trick. However, if you already learned the motivation behind that trick, the form of the problem does not matter. Here, 1 is missing! Add it to both sides to get

$$abc + ab + bc + ca + a + b + c + 1 = 1$$

The left hand side shows you how SFFT looks like for three variables. Try to compute $(a+j)(b+k)(c+\ell)$ and remember it. You will soon realize that the left hand side of the above equation factors as $(a+1)(b+1)(c+1)$. Therefore,

$$(a+1)(b+1)(c+1) = 1$$

The rest of the solution is just case work. If the product of three integers equals 1, what can they be? The solutions are

$$(a, b, c) \in \{(0,0,0), (-2,-2,0), (-2,0,-2), (0,-2,-2)\}$$

Problem 1.6.19 (Turkey TST 2014, Day 2, Problem 4). Find all odd positive integers m and n such that

$$n \mid 3m+1$$
$$m \mid n^2+3$$

Solution. Do not panic! Even some TST problems can be solved using simple tricks. The general idea is to first see if there are infinitely many solutions. Check some numbers and some special values for m and n. For instance, put $m = n$ to see if it fits in. In this problem, we cannot find a pattern to construct infinitely many solutions, so we guess that there are finite solutions and continue. To be honest, many of such divisibility problems (with finite solutions) rely heavily on case working, and you need to know how to start the case work. One of the best ways to handle this situation is to find a limit for m and n. Remember the properties of divisibility from proposition (1.1.2). Limit means bounds, and bounds means inequality (see part 10 of that proposition). Actually, we will use the fact that if $a \mid b$ for positive integers a and b, then $a \leq b$. After we have found the limit, the case work begins.

Write $n \mid 3m+1$ as $3m+1 = nk$ or $m = \frac{nk-1}{3}$. Now try to rewrite the second divisibility relation as

$$\frac{nk-1}{3} \mid n^2+3$$
$$\overset{\times 3}{\Longrightarrow} nk-1 \mid 3n^2+9$$
$$\overset{\times k}{\Longrightarrow} nk-1 \mid 3n^2k+9k$$

On the other hand, we know that $nk-1 \mid 3n(nk-1) = 3n^2k-3n$. Subtract these two last divisibility relations to find

$$nk-1 \mid 3n+9k$$

which in turn implies $nk-1 \leq 3n+9k$. This inequality can be simplified using SFFT in this way:

$$nk-3n-9k \leq 1 \overset{\text{add } 27}{\Longrightarrow} (n-9)(k-3) \leq 28$$

Notice that we have found the limit we wanted! The solution is almost obvious from here on, because one can manually put all possible values for n and k such that $(n-9)(k-3) \leq 28$ and pick those which satisfy the problem conditions ($n \mid 3m+1$ and $m \mid n^2+3$). In order to avoid this tedious endeavor, we start a proper case work.

We start case work on the parameter k (you will know why). Since m is odd and $3m+1 = nk$, k is even. We check some possible values of k:

(a) If $k = 2$, then from $nk-1 \mid 3n+9k$ we have $2n-1 \mid 3n+18$, and thus

$$2n-1 \mid 2(3n+18)-3(2n-1) = 39$$

This means that $2n-1 = 1, 3, 13$, or 39. None of these values make a solution for the problem.

(b) If $k = 4$, then from $nk - 1 \mid 3n + 9k$ we have $4n - 1 \mid 3n + 36$, and thus

$$4n - 1 \mid 4(3n + 36) - 3(4n - 1) = 147$$

This means that $4n - 1 = 1, 3, 7, 21, 49$, or 147. Checking the values of n, we find that $n = 1$ and $n = 37$ satisfy the conditions of the problem and give us the solutions $(m, n) = (1, 1)$ and $(m, n) = (49, 37)$.

(c) If $k \geq 6$, then the inequality $(n - 9)(k - 3) \leq 28$ can be transformed to

$$\begin{aligned}(n - 9) &\leq \frac{28}{k - 3} \\ &\leq \frac{28}{3}\end{aligned}$$

which means $n \leq 9 + 28/3$. Since n is a positive integer, the latter inequality simplifies to $n \leq 18$ (why?). Also, n is odd, so we have to check only the numbers $n = 1, 3, 5, 7, 9, 11, 13, 15$, and 17. In this case, only $n = 13$ gives a valid solution (check it) and it is $(m, n) = (43, 13)$.

Finally, the solutions are

$$(m, n) \in \{(1, 1), (49, 37), (43, 13)\}$$

§§1.7 Exercises

Problem 1.7.1. Find all pairs of positive integers (x, y) for which

$$\frac{x^2+y^2}{x-y}$$

is an integer that divides 1995.

Problem 1.7.2. Let x, y, and z be integers such that

$$(x-y)^2+(y-z)^2+(z-x)^2 = xyz$$

Prove that $(x+y+z+6)$ divides $(x^3+y^3+z^3)$.

Problem 1.7.3. Let k and m, with $k > m$, be positive integers such that the number $km(k^2-m^2)$ is divisible by k^3-m^3. Prove that $(k-m)^3 > 3km$.

Problem 1.7.4. Let $F(n) = 13^{6n+1} + 30^{6n+1} + 100^{6n+1} + 200^{6n+1}$ and define

$$G(n) = 2F(n) + 2n(n-2)F(1) - n(n-1)F(2)$$

Prove by induction that for all integers $n \geq 0$, $G(n)$ is divisible by 7^3.

Problem 1.7.5. Prove that for every integer $n \geq 2$, there exist n different positive integers such that for any two of these integers a and b, $a+b$ is divisible by $a-b$.

Problem 1.7.6 (Iran Second Round 1994). Let $\overline{a_1a_2a_3\ldots a_n}$ be the representation of a $n-$digits number in base 10. Prove that there exists a one-to-one function like $f : \{0,1,2,3,\ldots,9\} \to \{0,1,2,3,\ldots,9\}$ such that $f(a_1) \neq 0$ and the number $\overline{f(a_1)f(a_2)f(a_3)\ldots f(a_n)}$ is divisible by 3.

Problem 1.7.7 (Slovenia 2010). Let a, b, and c be three positive integers. Prove that $a^2+b^2+c^2$ is divisible by 4 if and only if a, b, and c are all even.

Problem 1.7.8 (ILL 1990, THA1). Let m be an odd positive integer not divisible by 3. Prove that

$$\left\lfloor 4^m - (2+\sqrt{2})^m \right\rfloor$$

is divisible by 112.

Note: for any real number x, $\lfloor x \rfloor$ is the largest integer not exceeding x.

Hint. Show that each term is equal to $4^m - (2+\sqrt{2})^m - (2-\sqrt{2})^m$.

Problem 1.7.9. Let $P_n = (19+92)(19^2+92^2)\cdots(19^n+92^n)$ for each positive integer n. Determine, with proof, the least positive integer m, if it exists, for which P_m is divisible by 33^{33}.

Problem 1.7.10. Prove that we can choose 2^n numbers from 2^{n+1} positive integers such that their sum is divisible by 2^n.

Problem 1.7.11 (Baltic Way 1993). Prove that for any odd positive integer n, $n^{12} - n^8 - n^4 + 1$ is divisible by 2^9.

Problem 1.7.12. Let m and n be two positive integers. Does there exist positive integers a, b, and c all greater than m such that abc is divisible by $a+n$, $b+n$, and $c+n$?

Problem 1.7.13 (Baltic Way 1997). Prove that in every sequence of 79 consecutive positive integers written in the decimal system, there is a positive integer whose sum of digits is divisible by 13.

Problem 1.7.14 (Baltic Way 2006). A 12—digit positive integer consisting only of digits 1, 5, and 9 is divisible by 37. Prove that the sum of its digits is not equal to 76.

Problem 1.7.15. Prove that the number $19^{1976} + 76^{1976}$

1. is divisible by the (Fermat) prime number $F_4 = 2^{2^4} + 1$, and
2. is divisible by at least four distinct primes other than F_4.

Problem 1.7.16. Show that $5^n - 4n + 15$ is divisible by 16 for all positive integers n.

Problem 1.7.17. Prove, without using mathematical induction, that $5^{2n+2} - 24n - 25$ is divisible by 576.

Problem 1.7.18 (IMO 1979, Problem 1). If p and q are positive integers so that

$$\frac{p}{q} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{1318} + \frac{1}{1319}$$

prove that p is divisible with 1979.

Problem 1.7.19 (ILL 1970–1973, FIN1). Prove that $2^{147} - 1$ is divisible by 343.

Problem 1.7.20 (ISL 1998, NT7). Prove that for each positive integer n, there exists a positive integer with the following properties:

- It has exactly n digits.
- None of the digits is zero.
- It is divisible by sum of its digits.

Problem 1.7.21 (ISL 1998, NT1). Determine all pairs (x, y) of positive integers such that $x^2y + x + y$ is divisible by $xy^2 + y + 7$.

Problem 1.7.22 (Ukrain TST2008, P6). Prove that there exist infinitely many pairs (a, b) of natural numbers not equal to 1 such that $b^b + a$ is divisible by $a^a + b$.

Problem 1.7.23 (Japan Final Olympiads 2009, P1). Find all positive integers n such that $8^n + n$ is divisible by $2^n + n$.

Problem 1.7.24 (Romania JBMO TST2001). Determine all positive integers a, b, c, and d in the order $a < b < c < d$ with the property that each of them divides the sum of the other three.

Problem 1.7.25 (BrMO 2003, Modified). Determine all triples (x, y, z) of integers greater than 1 with the property that x divides $yz - 1$, y divides $zx - 1$ and z divides $xy - 1$.

Problem 1.7.26 (All Russian Olympiads, P10.7). Positive integers $x > 1$ and y satisfy the equation $2x^2 - 1 = y^{15}$. Prove that 5 divides x.

Problem 1.7.27. Find all pairs (a, b) of positive integers such that $2a - 1$ and $2b + 1$ are relatively prime and $a + b$ divides $4ab + 1$.

Problem 1.7.28. Determine all pairs (m, n) of positive integers such that $m > n$ and

$$1 = \gcd(n + 1, m + 1) = \gcd(n + 2, m + 2) = \cdots = \gcd(m, 2m - n)$$

Problem 1.7.29. Let $a_1, a_2, \ldots, a_n, \ldots$ be any permutation of all positive integers. Prove that there exist infinitely many positive integers i such that $\gcd(a_i, a_{i+1}) \leq \frac{3}{4}i$.

Problem 1.7.30. Let $x \geq 1$ be a real number. Prove or disprove that there exists a positive integer n such that $\gcd(\lfloor x \rfloor, \lfloor nx \rfloor) = 1$.

Note. Here $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x.

Problem 1.7.31. Find all pairs of positive integers (a, b) such that

$$ab = 160 + 90 \gcd(a, b)$$

Problem 1.7.32. Let a, b, and c be positive integers satisfying $\gcd(a, b) = \gcd(b, c) = \gcd(c, a) = 1$. Show that $2abc - ab - bc - ca$ cannot be represented as $bcx + cay + abz$ with non-negative integers x, y, z.

Problem 1.7.33. Let $\{a_n\}_{n \geq 1}$ be a sequence of positive integers such that if $i \neq j$, then

$$\gcd(a_i, a_j) = \gcd(i, j)$$

Prove that $a_n = n$ for all positive integers n.

Problem 1.7.34. Let a and b be two positive integers such that $a > b$. We know that $\gcd(a - b, ab + 1) = 1$ and $\gcd(a + b, ab - 1) = 1$. Prove that $(a - b)^2 + (ab + 1)^2$ is not a perfect square.

Problem 1.7.35. Let m and n be positive integers with $(m, n) = 1$. Find $(5^m + 7^m, 5^n + 7^n)$.

Problem 1.7.36. A function $f : \mathbb{N} \to \mathbb{N}$ is *multiplicative* if $f(mn) = f(m)f(n)$ for all relatively prime positive integers m and n. Define the function $f : \mathbb{N} \to \mathbb{N}$ as follows:

$$f(n) = \sum_{i=1}^{n} \gcd(i, n)$$

- Prove that the function f is multiplicative.
- Prove that for every positive integer a, the equation $f(x) = ax$ has a solution $x \in \mathbb{N}$.
- Prove that, for a positive integer a, the equation $f(x) = ax$ has exactly one solution $x \in \mathbb{N}$ if and only if a is a power of 2 (where $1 = 2^0$ is also considered as a power of 2).

Problem 1.7.37. Let $a_0, a_1, a_2, \cdots$ be a sequence of positive integers such that the greatest common divisor of any two consecutive terms is greater than the preceding term; in symbols, $\gcd(a_i, a_{i+1}) > a_{i-1}$. Prove that $a_n \geq 2^n$ for all $n \geq 0$.

Problem 1.7.38. Let p be prime, let n be a positive integer, show that

$$\gcd\left(\binom{p-1}{n-1}, \binom{p+1}{n}, \binom{p}{n+1}\right) = \gcd\left(\binom{p}{n-1}, \binom{p-1}{n}, \binom{p+1}{n+1}\right).$$

Problem 1.7.39. Prove that

$$\gcd\left(\binom{n}{1}, \binom{n}{2}, \cdots, \binom{n}{n-1}\right)$$

is a prime if n is a power of a prime, and 1 otherwise.

Problem 1.7.40. Let a, b, p, and q be positive integers such that

$$\frac{p^2+q^2}{a} = \frac{pq}{b}$$

and $\gcd(a, b) = 1$.

1. Show that pq is divisible by b.
2. Show that $\sqrt{a+2b}$ is an integer.

Problem 1.7.41. Prove that if a and b are positive integers such that $a+b = (a, b)+[a, b]$, then one of a or b divides the other.

Problem 1.7.42 (British Mathematical Olympiad 2005). The integer N is positive. There are exactly 2005 ordered pairs (x, y) of positive integers satisfying

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{N}$$

Prove that N is a perfect square.

Problem 1.7.43. Determine all positive integer numbers m and n such that

$$\frac{1}{m} + \frac{1}{n} - \frac{1}{mn} = \frac{2}{5}$$

Problem 1.7.44. Find all triples (a, b, c) of positive integers such that

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 1$$

Problem 1.7.45. Find all triples (x, y, z) of positive integers which satisfy

$$\frac{1}{x} + \frac{2}{y} + \frac{3}{z} = 1$$

Hint. Assume without loss of generality that x is the minimum of the three numbers and then apply SFFT.

§§2 Modular Arithmetic

§§2.1 Basic Modular Arithmetic

Consider the timestamp we use in our daily life. Certainly, there was a point when people started counting time. Then, why is it not something like, 2147483647? Rather we say something like 12.09 am (and there is a date of course, that separates two 12.09 am). The reason is, each time the hour hand in a clock crosses 12, it starts from 1 again, not 13. If the numbers kept going large, we would have a hard time realizing what time we are living in. Similarly, when the second hand ticks 60 times, it starts from 1 again (meaning it has been 1 minute, letting the minute hand tick once). Here, intentionally or inadvertently, we have been using what number theorists call modular arithmetic. The idea is, we keep the integers that leave the same remainder (when divided by a certain integer) in the same *class*. It will be clear afterwards what exactly we mean by class here when we discuss complete set of residue class.

Definition. For a non-zero integer m, integers a and b are *congruent modulo* m if and only if $m \mid a - b$. We show this by the notation

$$a \equiv b \pmod{m}$$

If m does not divide $a - b$, we say that a and b are not congruent modulo m and denote it by $a \not\equiv b \pmod{m}$.

Note.

1. It is clear that if $m \mid a - b$, then $-m \mid a - b$. So from now on, we assume that m is a *positive* integer.
2. If a is divisible by m, then $a \equiv 0 \pmod{m}$. So, for example, an integer a is even if and only if $a \equiv 0 \pmod{2}$.

Example. $3 \equiv 7 \pmod{4}$, $5^2 \equiv -1 \pmod{13}$, $n^2 - 1 \equiv 0 \pmod{n+1}$.

Proposition 2.1.1. *Assume that a and b are two integers and m is a positive integer. Then the following propositions are correct.*

i. *If a is divided by b with remainder r, then a is congruent to r modulo b.*

ii. *If $a \equiv b \pmod{m}$, then for any divisor d of m, $a \equiv b \pmod{d}$.*

iii. $a \equiv a \pmod{m}$. *We call this the reflexivity property of modular congruences.*

iv. *If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$. We call this the symmetry property.*

v. *If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$. We call this the transitivity property.*

vi. *If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a \pm c \equiv b \pm d \pmod{m}$ and $ac \equiv bd \pmod{m}$.*

vii. *If $a \equiv b \pmod{m}$, then for any integer k, $ka \equiv kb \pmod{m}$.*

Proposition 2.1.2. *If n is a positive integer and $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$.*

Proof. From the definition, $a \equiv b \pmod{m}$ means $m \mid a - b$. We know from Theorem 1.5.19 that

$$a^n - b^n = (a - b)\left(a^{n-1} + a^{n-2}b + \cdots + b^{n-1}\right)$$

This gives $a - b \mid a^n - b^n$. So $m \mid a^n - b^n$, or $a^n \equiv b^n \pmod{m}$. □

Proposition 2.1.3. *If $f(x)$ is a polynomial with integer coefficients and $a \equiv b \pmod{m}$, then $f(a) \equiv f(b) \pmod{m}$.*

Proof. Assume $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Use Proposition (2.1.2) to get $a_i a^i \equiv a_i b^i \pmod{m}$ and add up all the terms. □

Proposition 2.1.4. *If a is an integer and n is a positive integer, then exactly one of the following relations holds.*

$$\begin{aligned} a &\equiv 0 \pmod{n} \\ a &\equiv 1 \pmod{n} \\ &\vdots \\ a &\equiv n-1 \pmod{n} \end{aligned}$$

Theorem 2.1.5. *Let m be a positive integer and a, b, and c be integers. Then*

(a) *If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = d$, then*

$$a \equiv b \mod \left(\frac{m}{d}\right)$$

We will call this the cancellation rule for congruence.

(b) *If $b \equiv c \pmod{m}$, then $\gcd(b, m) = \gcd(c, m)$.*

Before we prove it, let us see some examples. Usually, $ac = bc$ implies $a = c$ in equations and so far we have seen congruences maintain equation relations. However, is this any different in division? This is another trap you may fall into.

Since 15 divides $35 - 20$, $5 \cdot 7 \equiv 5 \cdot 4 \pmod{15}$. If we could just do division, this would give us

$$7 \equiv 4 \pmod{15}$$

which is clearly false. But, why? Here is the reason: $15 = 5 \cdot 3$. And when we canceled 5 without thinking where that 5 came from in 15, we accidentally took out the only portion where 5 came from. So we can not do that recklessly. However, this also means that if we took out 5 from all sides, it would be true:

$$7 \equiv 4 \pmod{3}$$

Proof.

(a) The greatest common factor of c and m is d, so there exist integers c_1 and m_1 such that

$$\begin{aligned} c &= c_1 d \\ m &= m_1 d \\ \gcd(c_1, m_1) &= 1 \end{aligned}$$

Since $ac \equiv bc \pmod{m}$, we have $m = m_1 d \mid (a-b)c = (a-b)c_1 d$. Canceling d from both sides, we get $m_1 \mid (a-b)c_1$. But $\gcd(c_1, m_1) = 1$, and so by Proposition 1.2.4, we get $m_1 \mid a - b$. Thus,

$$a \equiv b \pmod{m_1}$$

as desired.

(b) Because $b \equiv c \pmod{m}$, there exists an integer k for which $b - c = mk$. So $\gcd(b, m) \mid c$. On the other hand, from definition of gcd, it is clear that $\gcd(b, m) \mid m$. Now by proposition 1.2.3 we have $\gcd(b, m) \mid \gcd(c, m)$. Similarly, one can show that $\gcd(c, m) \mid \gcd(b, m)$. Using Proposition 1.1.3, we get $\gcd(c, m) = \gcd(b, m)$.

□

Arithmetic Progression. A sequence $a_1, a_2, a_3, \cdots$ of real numbers is called an *arithmetic sequence*, *arithmetic progression*, or *AP* if each new term of the sequence is obtained by adding a constant real number d, called the *common difference*, to the preceding term. In other words, the terms of an arithmetic progression are of the form

$$a, a + d, a + 2d, a + 3d, \cdots$$

where a is the *initial term* of the sequence.

Example. The sequence of odd numbers is an AP. The following sequence

$$-3, 2, 7, 12, 17, \cdots$$

which includes numbers of the form $5k + 2$ for $k = -1, 0, 1, \cdots$, is also an arithmetic sequence with initial term -3 and common difference 5.

Corollary 2.1.6. *All terms of an arithmetic progression are equivalent modulo the common difference.*

What is the sum of the terms of an arithmetic progression? Obviously, if the sequence has *infinite* number of terms, that is, if it has infinitely many terms, then the sum is not a finite number as the common difference is constant[1]. However, when the arithmetic progression is finite (such as, a portion of the sequence), the sum of all its elements is finite as well. So we often consider partial sum of such a series.

$$\begin{aligned}\sum_{i=1}^{n} a_i &= a_1 + a_2 + \ldots + a_n \\ &= a + (a+d) + \ldots + (a + (n-1)d) \\ &= na + d\,(1 + 2 + \ldots + (n-1))\end{aligned}$$

Since, $1 + 2 + \ldots + n = n(n-1)/2$,

$$\sum_{i=1}^{n} a_i = \frac{n}{2}\,(2a_1 + (n-1)d)$$

Geometric Progression. A sequence $a_1, a_2, a_3, \cdots$ of real numbers is called an *geometric sequence*, *geometric progression*, or *GP* if each new term of the sequence is obtained by multiplying the previous term by a constant real number r, called the *common ratio*. In other words, the terms of an arithmetic progression are of the form

$$a, ar, ar^2, ar^3, \cdots$$

where a is the *initial term* of the sequence.

Example. The sequence of powers of 2 is a geometric progression. The sequence

$$\frac{1}{2}, \frac{1}{6}, \frac{1}{18}, \frac{1}{54}, \cdots$$

is a GP with initial term $1/2$ and common ratio $1/3$.

Similar to arithmetic progressions, the sum of terms of a finite geometric progression is always possible to find. An interesting question would be what happens if we add all the terms of an *infinite* geometric sequence? For example, what is the value of the following sum?

$$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots$$

[1] we say that it *diverges*.

This is not a finite sequence. But is the sum divergent or convergent? The terms of the above sequence are gradually decreasing and approach zero. To see this, notice that the ninth term is

$$\frac{1}{256} = 0.00390625$$

which is very close to zero. So, on a second thought, we can guess that the given sum has a finite value. In general, when the absolute value of common ratio of a geometric progression is less than one, that is, when the absolute value of each term of the sequence is smaller that its preceding term, then the *geometric series* (either finite or infinite) has a finite value[2]. We will see this from a different point of view. This is due to *Chamok Hasan*, a teacher of the first author.

Consider a pumpkin. Let us assume that it is totally symmetrical. Now, divide it in half and put aside half of it. You have half of the pumpkin to yourself. Divide it in half again. Keep one to yourself and discard the other half. So now you have one fourth of the pumpkin. Again, cut it in half. Keep one, discard one. Now you have one eighth. See that if you keep going this way, you end up getting $\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \cdots$ and dividing them. And the fun fact is, you can keep doing this for as many times as you want. Obviously, if we put together all the parts again, we get the whole pumpkin. That is, if we take all the discarded portions and put them back, the pumpkin becomes whole again. This shows us without any rigorous proof that

$$\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \ldots = 1$$

Now you should be able to make sense how a sequence with infinite terms can have a finite sum. We have

$$\sum_{i=1}^{n} a_i = \frac{a\left(r^n - 1\right)}{r - 1}$$

Multiply the sum by $(r-1)$ to obtain

$$\begin{aligned}(r-1)\sum_{i=1}^{n} a_i &= (r-1)(ar^0 + ar^1 + \cdots + ar^{n-1}) \\ &= a(r-1)(1 + r + \cdots + r^{n-1}) \\ &= a(r^n - 1)\end{aligned}$$

We have used Theorem 1.5.19 to write the last line. Since $r \neq 1$, we can divide both sides by $r-1$ to get the desired result. Did you notice anything? In fact, this is a special case of what we encountered in divisibility. Recall the expansion of $a^n - b^n$ and try to find a correlation between the two. Take the geometric progression with $|r| < 1$, then the sum converges. More precisely,

$$\sum_{i \geq 1} a_i = \frac{a}{1-r}$$

[2]to put it differently, it *converges* to a fixed value.

Example.

- We can now compute $1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots$. In fact, this is an infinite geometric series with initial term $a=1$ and common ratio $r=\frac{1}{2}<1$. Thus,

$$\sum_{i\geq 0}\left(\frac{1}{2}\right)^i=\frac{1}{1-\frac{1}{2}}=2$$

- Suppose that we want to find

$$2+(-6)+18+(-54)+\cdots+(-39366)+118098$$

This is a geometric sequence with common ratio -3 and initial term 2. The last term equals $2(-3)^{10}$. So,

$$\sum_{i=0}^{10}2(-3)^i=\frac{2\left((-3)^{11}-1\right)}{(-3)-1}=88,573$$

§§2.2 Modular Exponentiation

In the early stage of problem solving, we all calculate big integers modulo an integer. For example, consider the next problem.

Problem 2.2.1. Define $a_n=6^n+8^n$. Find the remainder of a_{49} when divided by 49.

The first idea that crosses your mind might be calculating 6^{49} and finding the remainder when divided by 49. This would be a large integer and the calculation is really tedious, not to mention, pointless. A slight improvement would be multiplying 6 with 6 and taking modulo 49 each time. We need to do this for 49 times but at least, now we do not have to deal with that large numbers anymore. Let us call this *iterative exponentiation method.*

Suppose we want to find $c\equiv a^k \mod n$. The iterative exponentiation method computes the values $1=a^0,a^1,a^2,\cdots,a^k=c$ modulo n instead of directly calculating a^k modulo n. Suppose that we have computed a^i modulo n for some $i<k$ and the result is b. According to the above theorem, to calculate a^{i+1}, all we need to do is to compute $a\cdot b \mod n$. Obviously, $a\cdot b$ is much smaller than a^i when i is large. This is why this method takes less time for computations. Iterative exponentiation may be expressed as an algorithm as shown below.

Iterative Exponentiation Algorithm

1. Set $k_1\longleftarrow 0$ and $c\longleftarrow 1$.

2. Increase k_1 by 1.

k_1	$5^{k_1} \pmod{751}$	k_1	$5^{k_1} \pmod{751}$
1	5	11	358
2	25	12	288
3	125	13	689
4	625	14	441
5	121	15	703
6	605	16	511
7	21	17	302
8	105	18	8
9	525	19	40
10	372	20	200

Table 2.1: Applying iterative exponentiation method to find 5^{20} modulo 751.

3. Set $c \longleftarrow a \cdot c \pmod{n}$.

4. If $k_1 < k$, go to step 2. Otherwise return c.

Example. Let's compute 5^{20} modulo 751 by iterative exponentiation algorithm. Table 2.1 shows $5^i \mod 751$ for $i = 1$ to 20. As obtained from the table, $5^{20} \equiv 200 \pmod{751}$, which is in agreement with what we previously found.

Remark. In the above example where a is small (compared to modulus n), we can increase k_1 more than one unit in each iteration of the algorithm. For example, in above example, we could increase k_1 two units each time to compute $5^2, 5^4, \cdots, 5^{20}$. In this case, the number of calculations is divided by two and therefore there will be less time needed to find the result. This is done in general case but one must notice that when one increases k_1, say, two units at each step, he is in fact computing $a^2 \cdot c \mod n$ instead of $a \cdot c \mod n$ in step 3 of the algorithm to reduce the number of iterations of the algorithm. If a is small, there will be no difference in computation time. But if a is (too) large, computing $a^2 \cdot c \mod n$ may will be more time consuming and it may reduce the time efficiency of algorithm.

A more efficient method to do this is *modular exponentiation algorithm*. The beauty of this idea is that you can use it to compute big integers modulo n by hand. The idea actually inherits from binary representation. Consider the binary number $(101101)_2$. We discussed how to convert it to a decimal integer in base conversion. However, Masum uses a variation for faster mental calculation. Start from the left most digit (which always will be 1 if there is no leading 0). Initially, the decimal integer is 1. Now, go to the next digit. If it is 0, double the current value. If it is 1, double and add 1. Since the next digit is 0, we have 2. Next digit is 1. So it will become $2 \cdot 2 + 1 = 5$. Next digit is 1 as well. It will be $5 \cdot 2 + 1 = 11$. Next digit is 0, so we have $11 \cdot 2 = 22$. Next digit is 1, so it will be $22 \cdot 2 + 1 = 45$. There is no more digits left, so this is the desired value in decimal. You can verify that this indeed is the intended result. And more importantly, think why this works if you have not figured it out already!

We just saw a way of converting binary numbers into decimal. How does that help us in modular exponentiation? Assume that we want $a^k \pmod{n}$. We will not compute

it directly or iteratively. Instead, represent k in binary. Then, initially, the result is 1. Divide k by 2 and keep the remainder. If it is 1, multiply the current result by a and do the modulo operation, that is, $r \to ra \pmod{n}$. Also, set $a \to a^2 \pmod{n}$. Keep doing this until $k = 0$. In the end we will see $r \equiv a^k \pmod{n}$. Again, make sense why this works. Do the example above this way and see if the result matches. Algorithm to find $a^k \pmod{n}$.

Modular Exponentiation Algorithm ($a^k \pmod{n}$)

1. Set $R \longleftarrow 1$.
2. If $k = 0$, stop and return the value R. Otherwise, continue.
3. Divide k by 2, take the remainder r. That is, set $k \longleftarrow \lfloor k/2 \rfloor$.
4. Set $a \longleftarrow a^2 \pmod{n}$.
5. If $r = 1$, set $R \longleftarrow Ra \pmod{n}$.
6. Go to step 2.

However, we face another concern here. What if Ra is very large? We can take care of it the same way. Express a in binary and take modulo from there. Algorithm to find $ab \pmod{n}$ for large b.

1. Set $R = 1$.
2. If $b = 0$, return R, otherwise continue.
3. Set $b \longleftarrow \lfloor b/2 \rfloor$ and $r = b \pmod{2}$.
4. If $r = 1$, set $R \longleftarrow R + a \pmod{n}$.
5. Set $a = (2 \cdot a) \pmod{n}$.
6. Go to step 2.

We can call this *modular multiplication*. This way, we will not have to actually multiply two numbers to get the remainder. The proofs for the last two ideas were not shown deliberately. We expect that you can do it easily. By the way, did you notice something else too? In modular exponentiation, we do not have to iterate k times. The number of times we need to iterate is actually $\lfloor \log_2(k) \rfloor + 1$ (again, why?). Same goes for modular multiplication. Therefore, it is a very desirable improvement. In fact, these methods are highly used in primality tests or similar fields (we will discuss about primes in Chapter 4).

Notice that, we can write modular exponentiation algorithm in a better fashion.

Modular Exponentiation Algorithm - Cleaner Version ($a^k \pmod n$)

1. Set $R = 1$.
2. Represent k in binary. Assume $k = (x_0 x_1 \cdots x_l)_2$.
3. If $k = 0$, return R.
4. Find $r = (k \pmod 2)$.
5. If $r = 1$, set $R \longleftarrow Ra \pmod n$.
6. Set $k \longleftarrow \lfloor k/2 \rfloor$.
7. Set $a \longleftarrow a^2 \pmod n$.
8. Go to step 3.

Example. Let us calculate $5^{20} \pmod{751}$ this way. First, we need to find the binary representation of 20, which is $(10100)_2$. Then, we can write

$$5^{20} \equiv \underbrace{\left(\underbrace{\left(\overbrace{\left(\overbrace{\left(\underbrace{5^2}_{R_1}\right)^2 \cdot 5}^{R_2}\right)^2}^{R_3}\right)}_{R_4}\right)^2}_{R_5} \pmod{751}$$

This is how we proceed: we want to construct 5^{20}. The rightmost digit is zero. What happens if we remove this digit? The number gets divided by 2. This is identical to writing $5^{20} = 5^2 \cdot 5^{10}$. Therefore, we first compute $R_1 = 5^2$. We now need to construct 5^{10}. The binary representation of 10 is $(1010)_2$. Again, divide it by two to remove the rightmost zero. This time, we are doing this operation:

$$5^{20} = R_1 \cdot 5^2 \cdot 5^5$$

We must compute $R_2 = R_1 \cdot 5^2$ at this stage. Now, how do we construct 5^5 given its binary representation $(101)_2$, which does not end in zero? It's easy. We just have to write it as $1 + (100)_2$. Now, we have $(100)_2$ which ends in zero. In other words,

$$5^{20} = R_2 \cdot 5 \cdot 5^4$$

So, we calculate $R_3 = R_2 \cdot 5$ at this stage and try to construct 5^4. The rest of the solution is similar and we expect the reader to finish it. Try to find R_4 and R_5 for yourself. In case you want to check your answers, you can consult table 2.2.

i	1	2	3	4	5
R_i	25	625	121	372	200

Table 2.2: Applying modular exponentiation method to find 5^{20} modulo 751.

§§2.3 Residue Systems

Residue systems are very simple definitions which will help you make a good sense of some later-explained theorems such as Fermat's and Euler's.

2.3.0.1 Complete Residue Systems

The definitions and theorems below assume that m is a positive integer.

Definition. Two integers a and b are said to be members of the same residue class modulo m, if and only if $a \equiv b \pmod{m}$. Clearly, there are m distinct residues modulo m.

Definition. Let m be a positive integer. The set A is called a complete residue system modulo m if and only if every number is congruent to a unique element of A modulo m. In other words, A should be representing all the residue classes modulo m.

Example. $A = \{0, 1, \cdots, m-1\}$ is a complete residue system modulo m. So is $B = \{15, 36, -7, 27, 94\}$ modulo 5.

We will state two simple propositions without proof. The reader should be able to prove them on their own.

Proposition 2.3.1. *The set $A = \{a_1, a_2, \cdots, a_k\}$ is a complete residue set (or system) modulo m if and only if $k = m$ and $a_i \not\equiv a_j \pmod{m}$ for $i \neq j$.*

Proposition 2.3.2. *Let $A = \{a_1, a_2, \cdots, a_m\}$ be a complete residue set modulo m and let a, b be integers such that $a \perp m$. Then the set*

$$B = \{aa_1 + b, aa_2 + b, \cdots, aa_m + b\}$$

is also a complete residue set modulo m.

2.3.0.2 Reduced Residue Systems and Euler's Totient Function

We really wish that you have a firm grasp of *function*. However, if you are in 10th grade or below, there is a good chance, you are not familiar with the concept of functions very well. Since that is entirely a different topic, we restrain ourselves from discussing it. Make sure you at least realize what function actually is. Here, we will say a thing about function or two but it is not nearly enough for covering the fundamentals.

A *function* is like a machine. It takes a number as its input, *functions on the number*, and gives another number as its output with the property that each input is related to

exactly one output. This property seems logical. Consider a weighing scale designed to measure the weight of people. Obviously, a person cannot be both 70 and 75 kilograms at the same time. The weight of a person (in a specific time) is a constant number, and hence the weighing scale actually works as a function: it takes a person as its input, measures his weight, and then shows the person's weight as its input.

Another example would be a function that takes a real number x as its input and gives x^2 as its output. For convenience, we can call this function $f : \mathbb{R} \to \mathbb{R}$ and write its *relation* as $f(x) = x^2$ for all $x \in \mathbb{R}$. The notation $f : \mathbb{S} \to \mathbb{T}$ means that the function f takes its inputs from the *domain* S (the set of inputs) and assigns them an output from the *codomain* T (the set of outputs and maybe some additional elements). For the previous example, we see that both domain and codomain of f are $\mathbb{R}$. However, the *range* (or *image*) of f, which is the set containing only outputs of f, is $\mathbb{R}^+$, the set of all positive real numbers.

Euler's Totient Function. For every positive integer $n > 1$, $\varphi(n)$ is the number of positive integers less than or equal to n which are relatively prime to n. We call this function Euler's phi function (or totient[3] function).

Example. $\varphi(5) = 4$ and $\varphi(10) = 4$.

We will investigate properties of this function in details in Chapter 3. For now let's just assume the following claims are true.

Proposition 2.3.3 (Properties of Euler's Totient Function). *Let m and n be two positive integers.*

(a) φ is a multiplicative function. That is, if $m \perp n$, then

$$\varphi(mn) = \varphi(m) \cdot \varphi(n)$$

(b) For all $n \geq 3$, $\varphi(n)$ is even.

(c) φ is neither increasing[4], injective[5] nor surjective[6].

(d) If n is factorized as $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, then

$$\begin{aligned}\varphi(n) &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right) \\ &= p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdots p_k^{\alpha_k - 1} (p_1 - 1) \cdots (p_k - 1)\end{aligned}$$

Why do we require function in congruence? Moreover, Euler's totient function? Before you decide it sounds irrelevant, take a look at the following example.

[3] You might be wondering what totient means. In Latin, tot means so many. The suffix of iens is probably from the Sanskrit.

[4] The function f is increasing if for $a_1 > a_2$, we have $f(a_1) > f(a_2)$.

[5] The function f is injective if for $a_1 \neq a_2$, we have $f(a_1) \neq f(a_2)$.

[6] The function $f : X \to Y$ is surjective if for every $y \in Y$, there exists $x \in X$ such that $f(x) = y$.

Consider the integers $\{1,2,3,4,5,6\}$ (complete set of residue class modulo 7 except 0). Now, take an integer, say 3. Multiply the whole set with 3 and find the residues again:

$$\{3,6,9,12,15,18\} \equiv \{3,6,2,5,1,4\} \pmod 7$$

Does this look interesting? If not, take a look again. And try to understand what happened and why. Firstly, the products forms a residue class as well. Alternatively, it is a permutation of the residue class. Why? What if we multiplied by 5? Check it out yourself and see if the conclusion holds. Check for some more integers like 10, 13, 14 etc. You will see the same is true for all integers except $0, 7, 14, \cdots$ i.e. multiples of 7. Again, why? 7 is a prime. So we know if an integer is not divisible by 7, it is co-prime to 7. Take a such that $a \perp 7$. Now, what does it mean that the set of products is a permutation of the original? We could state it this way: no two products leave the same remainder when divided by 7. And you can see, if this is true, everything makes sense. If we can show that for $0 < i < j < 7$, ia and ja are not congruent modulo 7, we are done! That is indeed the case. For the sake of contradiction, assume that,

$$\begin{aligned} & ia \equiv ja \pmod 7 \\ \iff & 7 \mid ia - ja = a(i-j) \end{aligned}$$

Here $a \perp 7$, so we have $7 \mid i-j$. But remember that, $i < j < 7$ so $|i-j| < 7$. This yields the contradiction we were looking for. This claim was true mainly because $a \perp 7$. What if we did not take a prime 7? Well, we could still do something similar. And that is why Euler's totient function comes to the play. This is more valuable than you may realize.

Definition. Let m be a positive integer. The set A is called a reduced residue system modulo m if all elements of A are relatively prime to m, and also every integer which is relatively prime to m is congruent to a unique element of A modulo m.

Example. The set $A = \{1, 2, \cdots, p-1\}$ is a reduced residue system modulo a prime p. The set $\{7, 17\}$ is also a reduced residue system mod 6.

You can clearly sense how the Euler's phi function is related to reduced residue systems: the number of elements of A is $\phi(m)$. So we can express the above definition in a better way:

Proposition 2.3.4. *The set $A = \{a_1, a_2, \cdots, a_k\}$ is a reduced residue set (or system) modulo m if and only if*

- *$a_i \perp m$ for all i,*
- *$k = \varphi(m)$, and*
- *$a_i \not\equiv a_j \pmod m$ for $i \neq j$.*

An important aspect of the reduced systems is stated in the next proposition. It will help us prove the Euler's theorem later.

Proposition 2.3.5. *Let $A = \{a_1, a_2, \cdots, a_{\varphi(m)}\}$ be a reduced residue set modulo m and let a be an integer such that $a \perp m$. Then the set*

$$B = \{aa_1, aa_2, \cdots, aa_{\varphi(m)}\}$$

is also a reduced residue set modulo m.

The proof of this theorem is pretty easy, try it for yourself. Pay attention to the difference between this proposition and the similar Proposition 2.3.2 for complete systems.

The latest theorem says that there are infinitely many reduced residue systems for any m. So, it makes sense to define a set as the original reduced residue system for any positive integer m. We call this set $\mathbb{U}_m$.

Definition. Let m be a positive integer. The *set of units* modulo m, $\mathbb{U}_m$, is the set of positive integers $g_1, \cdots, g_{\varphi(m)}$ less than m which are relatively prime to m.

Example. $\mathbb{U}_8 = \{1, 3, 5, 7\}$, and $\mathbb{U}_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$. If p is a prime, then $\mathbb{U}_p = \{1, 2, \cdots, p-1\}$.

You might be wondering why we call $\mathbb{U}_m$ the set of *units*. In algebraic structures, a unit is an element a for which there exists some element b such that $ab = 1$. In our case, the number a is a unit if there exists some b such that $ab \equiv 1 \pmod{m}$. As proved before, a is a unit if and only if it is relatively prime to m, and this shows us why $\mathbb{U}_m$ is called the set of units.

§§2.4 Bézout's Lemma

In this section, we are going to explain the simple but useful Bézout's lemma and then introduce modular multiplicative inverses.

§§§2.4 Bézout's Identity and Its Generalization

Before representing this lemma, we would like you define the *linear combination* of two integers.

Definition. For two integers a and b, every number of the form

$$ax + by$$

is called a *linear combination of a and b, where x and y are integers.*

For example, $2a + 3b$ and $-4a$ are both linear combinations of a and b, but $a^2 - b$ is not. The *Bézout's lemma* (sometimes called *Bézout's identity* states that for every two integers a and b, there exists a linear combination of a and b which is equal to (a, b). For example if $a = 18$ and $b = 27$, then $18 \cdot (-1) + 27 \cdot 1 = 9 = (18, 27)$.

Theorem 2.4.1 (Bézout's Identity). *For two nonzero integers a and b, there exists $x, y \in \mathbb{Z}$ such that*

$$ax + by = (a, b)$$

You are probably familiar with this theorem. A simple proof uses Euclidean division, but it doesn't show you where exactly to use this identity. So, we prove a stronger theorem and the proof of Bézout's identity is immediately implied from it.

Theorem 2.4.2. *Let a, b, m be integers such that a, b are not zero at the same time. Then the equation*

$$ax + by = m$$

has solutions for x and y in positive integers if and only if $(a, b) \mid m$.

Proof. The first part is easy. Suppose that there exist integers x_0 and y_0 such that

$$ax_0 + by_0 = m$$

We know that $(a, b) \mid a$ and also $(a, b) \mid b$, thus $(a, b) \mid m$ and we are done.

Conversely, if $(a, b) = d$ and m is divisible by d, then we want to prove that there exist some positive integers x and y for which $ax + by = m$. First, we show that it's sufficient to show that there exist x and y such that

$$ax + by = d$$

The reason is simple: if there exist x and y such that $ax + by = d$, then

$$a\left(x\frac{m}{d}\right) + b\left(y\frac{m}{d}\right) = m$$

Assume that A is the set of all positive integer linear combinations of a and b. A is non-empty because if $a \neq 0$, then

$$0 < |a| = a\frac{|a|}{a} + b \cdot 0$$

and if $b \neq 0$, then

$$0 < |b| = a \cdot 0 + b\frac{|b|}{b}$$

Because of well-ordering principle[7], A contains a least element. Let this smallest element be t. So there exist integers x_0 and y_0 such that

$$ax_0 + by_0 = t$$

We claim that $t \mid a$ and $t \mid b$. Using division theorem, divide a by t:

$$a = tq + r$$

and thus

$$a\underbrace{(1 - qx_0)}_{=x_1} + b\underbrace{(-qy_0)}_{=y_1} = a - tq = r < t$$

[7]The well-ordering principle states that every non-empty set of positive integers contains a least element.

If $r \neq 0$, then r is a positive integer written in the form $ax_1 + by_1$, which is a positive integer linear combination of a and b, so $r \in A$. But $r < t$, which is in contradiction with minimality of t. Therefore $r = 0$ and $t \mid a$. We can prove that $t \mid b$ in a similar way. By Proposition 1.2.3, we find that $t \mid d$. Also, according to the first part of the proof, we have $d \mid t$. Following Proposition 1.1.3, $t = d$. This means that $d \in A$ and there exist integers x and y such that

$$ax + by = d$$

□

Bézout's Identity has many interesting applications. We will see one such application in Chapter 5, to prove *Chicken McNugget Theorem*.

We are now ready to represent a stronger version and also a generalization of Bézout's lemma.

Corollary 2.4.3 (Stronger Form of Bézout's Identity). *The smallest positive integer linear combination of a and b is (a, b).*

Corollary 2.4.4. *If $a \perp b$ for non-zero integers a and b, then there exist integers x and y such that*

$$ax + by = 1$$

Theorem 2.4.5 (Generalization of Bézout's Identity). *If $a_1, a_2, \cdots, a_n$ are integers with $(a_1, a_2, \cdots, a_n) = d$, then the equation*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = m$$

has a solution $(x_1, x_2, \cdots, x_n)$ in integers if and only if $d \mid m$.

Theorem 2.4.6. *Let m be a positive integer and let a and b be positive integers. Then the modular arithmetic equation*

$$ax \equiv b \pmod{m}$$

has a solution for x in integers if and only if $(m, a) \mid b$.

Proof. Rewrite the congruence equation as $ax - my = b$ for some integer y. Now it is the same as Theorem 2.4.2. The equation $ax - by = m$ has solutions if and only if $(m, a) \mid b$, which is what we want. □

Problem 2.4.7. Let a, b, and c be non-zero integers such that $(a, c) = (b, c) = 1$. Prove that $(ab, c) = 1$.

Solution. By Corollary 2.4.4, there exist integers x, y, z, and t such that

$$ax + cy = 1$$
$$bz + ct = 1$$

Multiply these two equations to get

$$\begin{aligned} 1 &= (ax + cy)(bz + ct) \\ &= ab(xz) + c(axt + byz + cyt) \end{aligned}$$

This means that we have found a linear combination of c and ab which is equal to 1. From Corollary 2.4.3 it follows that $(ab, c) = 1$ (why?).

Let's prove the second part of proposition (1.2.4) in section (1.2).

Problem 2.4.8. Let a, b, and c be integers. If $a \mid bc$ and $(a, b) = 1$, prove that $a \mid c$.

Solution. The problem is obvious for $c = 0$. Assume that $c \neq 0$. Since $(a, b) = 1$, there exist integers x and y such that $ax + by = 1$. Multiply both sides of this equation by c to obtain $acx + bcy = c$. Because a divides both acx and bcy, it must also divide their sum, which is equal to c.

§§§2.4 Modular Arithmetic Multiplicative Inverse

When speaking of real numbers, the multiplicative inverse of x – usually named reciprocal of x – is $\frac{1}{x}$. This is because $x \cdot \frac{1}{x} = 1$ for non-zero x.

The definition of a multiplicative inverse in modular arithmetic must be more clear for you now.

Definition. Let a be an integer and let m be a positive integer. The *modular multiplicative inverse* of a modulo m is an integer x such that

$$ax \equiv 1 \pmod{m}$$

Once defined, x may be denoted by a^{-1} and simply called *inverse of* a.

Note. Unlike real numbers which have a unique reciprocal, an integer a has either no inverse, or infinitely many inverses modulo m.

Example. An inverse for 3 modulo 7 is 5:

$$3 \cdot 5 \equiv 1 \pmod{7}$$

We can easily generate other inverses of 3 modulo 7 by adding various multiples of 7 to 5. Thus, the numbers in the set $\{\cdots, -2, 5, 12, 19, \cdots\}$ are all inverses of 3 modulo 7.

Example. An inverse for $2^{16} + 1$ modulo $2^{31} - 1$ is $2^{16} - 1$. In fact,

$$(2^{16} - 1)(2^{16} + 1) = 2^{32} - 1 = 2(2^{31} - 1) + 1 \equiv 1 \pmod{2^{31} - 1}$$

Theorem 2.4.9. *Let a be an integer and let m be a positive integer such that $a \perp m$. Then a has an inverse modulo m. Also, every two inverses of a are congruent modulo m.*

Proof. The proof is a straightforward result of corollary (2.4.4). Since $a \perp m$, the equation $ax + my = 1$ has solutions. Now take modulo m from both sides to complete the proof of the first part. For the second part, assume that x_1 and x_2 are inverses of a modulo m. Then,

$$\begin{aligned} & ax_1 \equiv ax_2 \equiv 1 \pmod{m} \\ \overset{(a,m)=1}{\implies} & x_1 \equiv x_2 \pmod{m} \end{aligned}$$

as desired. □

The uniqueness of inverse of an integer a modulo m gives us the following corollary.

Corollary 2.4.10. *For a positive integer m, let $\{a_1, a_2, \cdots, a_{\varphi(m)}\}$ be a reduced residue system modulo m. Then $\{a_1^{-1}, a_2^{-1}, \cdots, a_{\varphi(m)}^{-1}\}$ is also a reduced residue system modulo m.*

Problem 2.4.11. Find the unique odd integer t such that $0 < t < 23$ and $t + 2$ is the modular inverse of t modulo 23.

Solution. This means that $t(t+2) \equiv 1 \pmod{23}$. Add 1 to both sides of this congruence relation to get $(t+1)^2 \equiv 2 \equiv 25 \pmod{23}$. Therefore, $23 \mid (t+1)^2 - 25$ or $23 \mid (t-4)(t+6)$. By Euclid's lemma (Proposition 1.1.10), $23 \mid t-4$ or $23 \mid t+6$, which give $t = 4$ and $t = 17$ as solutions. Since we want t to be odd, the answer is $t = 17$.

We are going to prove a very simple fact which will be very useful later (for instance, in the next theorem or in the proof of Wolstenholme's theorem, where we re-state the same result as Lemma 2.9.6).

Proposition 2.4.12. *For a prime $p \geq 3$ and any positive integer a relatively prime to p,*

$$(a^{-1})^n \equiv (a^n)^{-1} \pmod{p}$$

for all positive integers n.

Proof. Since a is relatively prime to p, a^{-1} exists. Therefore,

$$\begin{aligned} & a \cdot a^{-1} \equiv 1 \pmod{p} \\ \implies & a^n \cdot (a^{-1})^n \equiv 1 \pmod{p} \\ \implies & (a^{-1})^n \equiv (a^n)^{-1} \pmod{p} \end{aligned}$$

as desired. □

Theorem 2.4.13. *Let a, b be integers and x, y, and n be positive integers such that $(a, n) = (b, n) = 1$, $a^x \equiv b^x \pmod{n}$, and $a^y \equiv b^y \pmod{n}$. Then,*

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

Proof. By Bézout's identity, we know there are integers u and v so that $ux+vy=(x,y)$. Therefore,

$$\begin{aligned} a^{(x,y)} &\equiv a^{ux+vy} \\ &\equiv (a^x)^u \cdot (a^y)^v \qquad (2.1) \\ &\equiv (b^x)^u \cdot (b^y)^v \qquad (2.2) \\ &\equiv b^{ux+vy} \qquad (2.3) \\ &\equiv b^{(x,y)} \pmod{n} \end{aligned}$$

□

Remark. Thanks to Professor Greg Martin, we should point out a very important detail here. In the computations above, we used the fact that there exist integers u and v such that $ux+by=1$. One must notice that these integers u and v need not be positive. In fact, if x and y are both positive, then u and v cannot be both positive (why?). But that doesn't make our calculations wrong, due to Proposition 2.4.12. If it's not clear to you yet, think of it in this way: suppose that, say, u is negative. For instance, consider the example when $x=3$ and $y=15$. Then, since $3\cdot(-4)+15\cdot 1=(3,15)$, we have $u=-4$ and $v=1$. Then, equation (2.2), would look like

$$(a^3)^{-4}\cdot(a^{15})^1 \equiv (b^3)^{-4}\cdot(b^{15})^1 \pmod{n}.$$

This might not seem normal because we have a -4 in the exponents. So, using Proposition 2.4.12, we can write the above congruence equation as

$$\left((a^{-1})^3\right)^4\cdot(a^{15})^1 \equiv \left((b^{-1})^3\right)^4\cdot(b^{15})^1 \pmod{n}.$$

Notice that we need $(a,n)=1$ and $(b,n)=1$ to imply a^{-1} and b^{-1} exist modulo n.

Problem 2.4.14. Prove that, $\frac{(m,n)}{m}\binom{m}{n}$ is an integer.

Since this problem is juxtaposed with this section, it is obvious we are going to use this theorem. But in a real contest, that may not be the case at all. Try solving it without seeing the solution first and you will know what we mean.

Solution. Since there are integers x,y with $(m,n)=mx+ny$, it is easy to deduce that:

$$\begin{aligned} \frac{\gcd(m,n)}{m}\binom{m}{n} &= \frac{mx+ny}{m}\binom{m}{n} \\ &= x\binom{m}{n}+\frac{ny}{m}\binom{m}{n} \\ &= x\binom{m}{n}+\frac{ny}{m}\cdot\frac{m}{n}\binom{m-1}{n-1} \\ &= x\binom{m}{n}+y\binom{m-1}{n-1} \end{aligned}$$

This is obviously an integer.

§§2.5 Chinese Remainder Theorem

Chinese Remainder Theorem –usually called *CRT*– is a very old principle in mathematics. It was first introduced by a Chinese mathematician Sun Tzu almost 1700 years ago. Consider the following example.

Problem 2.5.1. A positive integer n leaves remainder 2 when divided by 7 but has a remainder 4 when divided by 9. Find the smallest value of n.

You might have encountered similar problems when you were in 4th or 5th grade. May be even more basic ones. But the idea is essentially the same. If the problem was a bit different, like

Problem 2.5.2. A positive integer n leaves remainder 2 when divided by 7 or 9. Find the smallest value of n.

Then it would be easier. Because then we would have that $n-2$ is divisible by both 7 and 9. That means $n-2$ has to be divisible by their least common multiple, 63. Obviously, the minimum such n is $n=2$. Let's see what happens if we want $n>2$. Then all such positive integers would be $n=2+63k$. Now, as for this problem, we can't do this directly when the remainders are different. So we go back to the original problem and see how we can tackle the new one. Let's write them using congruence.

$$\begin{aligned} n &\equiv 2 \pmod 7 \\ n &\equiv 4 \pmod 9 \end{aligned}$$

In other words, using divisibility notation, $7 \mid n-2$ and $9 \mid n-4$. We can not do the same now. But *if* these two remainders were same, we could do that. Probably we should focus on that. That is, we want it to be something like

$$\begin{aligned} n &\equiv a \pmod 7 \\ n &\equiv a \pmod 9 \end{aligned}$$

The only thing we can do here is

$$\begin{aligned} n &\equiv 2+7k \pmod 7 \\ n &\equiv 4+9l \pmod 9 \end{aligned}$$

for some *suitable* integer k and l. Our aim is to find their values. Since both $2+7k$ and $4+9l$ must be the same modulo 7 and 9, if we can find a way to keep 9 in $2+7k$ and 7 is $4+9l$, that could work! One way around it is to do the following:

$$\begin{aligned} n &\equiv 2\cdot 1+7\cdot 4 \pmod 7 \\ n &\equiv 2\cdot 9\cdot 9^{-1}+7\cdot 4 \pmod 7 \end{aligned}$$

Let's do the same for the other congruence.

$$n \equiv 4 \cdot 1 + 9 \cdot 2 \pmod 9$$
$$n \equiv 4 \cdot 7 \cdot 7^{-1} + 2 \cdot 9 \pmod 9$$

Now you should understand what we can do to make those two equal. In the first congruence, no matter what we multiply with $7 \cdot 4$, the remainder won't change modulo 7. The same for 9 in the second congruence. We will exploit this fact. We need to rearrange it just a bit more. But here is a warning. We wouldn't be able to do it if 7 and 9 were not relatively prime, since then they would not have any multiplicative inverse. We could do that trick writing $1 = 7 \cdot 7^{-1}$ only because 7^{-1} modulo 9 exists. For simplicity, let's assume $7^{-1} \equiv u \pmod 9$ and $9^{-1} \equiv v \pmod 7$.

$$n \equiv 2 \cdot 9 \cdot v + 4 \cdot 7 \cdot u \pmod 7$$
$$n \equiv 4 \cdot 7 \cdot u + 2 \cdot 9 \cdot v \pmod 9$$

And now, we have what we want! We can say,

$$n \equiv 2 \cdot 9 \cdot v + 4 \cdot 7 \cdot u \pmod{7 \cdot 9}$$

since $7 \perp 9$. We have our solution! Think more on our approach and what led us to do this. Question is, is this n the smallest solution? If we take r with $0 \leq r \leq mn$ so that

$$n \equiv r \equiv 18v + 28u \pmod{63}$$

where $u \equiv 7^{-1} \equiv 4 \pmod 9$ and $v \equiv 9^{-1} \equiv 4 \pmod 7$. Therefore,

$$\begin{aligned} n &= (18 \cdot 4 + 28 \cdot 4) \pmod{63} \\ &= 184 \pmod{63} \\ &= 58 \end{aligned}$$

Since $58 < 63$, such a solution will be unique! Mathematically, we can write it this way. Let the inverse of a modulo n be a_n^{-1}.

Theorem 2.5.3 (Chinese Remainder Theorem for Two Integers). *For two positive integers $a \perp b$,*

$$x \equiv m \pmod a$$
$$x \equiv n \pmod b$$

has a solution

$$x_0 \equiv (mbb_a^{-1} + naa_b^{-1}) \pmod{ab}$$

and all the solutions are given by $x = x_0 + abk$.

But this form is not that convenient. We will give it a better shape. Let $M = ab$, then $\frac{M}{a} \perp b$ and $\frac{M}{b} \perp b$. Rewrite the theorem in the following form.

Theorem 2.5.4 (Refined CRT). *If $a_1 \perp a_2$ and $M = a_1 a_2$, then the congruences*

$$\begin{aligned} x &\equiv r_1 \pmod{a_1} \\ x &\equiv r_2 \pmod{a_2} \end{aligned}$$

has the smallest solution

$$x_0 \equiv \left(r_1 \left(\frac{M}{a_1}\right) \left(\frac{M}{a_1}\right)_{a_2}^{-1} + r_2 \left(\frac{M}{a_2}\right) \left(\frac{M}{a_2}\right)_{a_1}^{-1} \right) \pmod{M}$$

If we take n relatively prime integers instead of two, the same process will work! So we can generalize this for n variables.

Theorem 2.5.5 (CRT). *For n pairwise relatively prime integers $a_1, a_2, \cdots, a_n$ there exists a solution to the congruences*

$$\begin{aligned} x &\equiv r_1 \pmod{a_1} \\ x &\equiv r_2 \pmod{a_2} \\ &\vdots \\ x &\equiv r_n \pmod{a_n} \end{aligned}$$

If $M = a_1 a_2 \cdots a_n$ and $M_i = \dfrac{M}{a_i}$ and $M_i e_i \equiv 1 \pmod{a_i}$, then the smallest modulo M is given by

$$x_0 \equiv (r_1 M_1 e_i + \cdots + r_n M_n e_n) \equiv \left(\sum_{i=1}^{n} r_i M_i e_i \right) \pmod{M}$$

Proof. Note that, for a fixed i, M_j is divisible by a_i if $i \neq j$. Therefore,

$$\begin{aligned} x_0 &= \sum_{i=1}^{n} r_i M_i e_i \\ &\equiv r_i M_i e_i \\ &\equiv r_i \pmod{a_i} \end{aligned}$$

So x_0 is a solution to those congruences. Since $M_i \perp a_i$, there is a multiplicative inverse of M_i modulo a_i due to Bézout's identity. We leave it to the reader to prove that if x, y are two solutions, then $x \equiv y \pmod{M}$. That would prove its uniqueness modulo M. □

We want to mention a particular use of CRT. When you are facing some problems related to congruence equation, if you can not solve for some n, instead show a solution for $p_i^{e_i}$ where $n = p_1^{e_1} \cdots p_k^{e_k}$. Then you can say that such a solution modulo n exists as well. In short, we could reduce the congruences to prime powers because $p_1, \cdots, p_k$ are pairwise relatively prime integers. By the way, we could generalize CRT the following way.

Theorem 2.5.6 (General CRT). *For n integers $a_1, \cdots, a_n$ the system of congruences*

$$\begin{aligned} x &\equiv r_1 \pmod{a_1} \\ x &\equiv r_2 \pmod{a_2} \\ &\vdots \\ x &\equiv r_n \pmod{a_n} \end{aligned}$$

has a solution if and only if

$$r_i \equiv r_j \pmod{(a_i, a_j)}$$

for all i and j. Any two solutions x, y are congruent modulo the least common multiple of all a_i. That is, if $M = [a_1, \cdots, a_n]$ and x, y are two solutions, then $x \equiv y \pmod{M}$.

Problem 2.5.7. Prove that, for any n there are n consecutive integers such that all of them are composite.

Solution. We will use CRT here forcibly, even though it has a much easier solution. Consider the following congruences:

$$\begin{aligned} x &\equiv -1 \pmod{p_1 p_2} \\ x &\equiv -2 \pmod{p_3 p_4} \\ &\vdots \\ x &\equiv -n \pmod{p_{2n-1} p_{2n}} \end{aligned}$$

Here, $p_1, \cdots, p_{2n}$ are distinct primes. Therefore, $M_1 = p_1 p_2, \cdots, M_n = p_{2n-1} p_{2n}$ are pairwisely co-prime. So, by CRT, there is indeed such an x which satisfies all of the congruences above. And our problem is solved. Notice that, $x + 1$ is divisible by at least two primes p_1, p_2. Similarly, $x + i$ is divisible by $p_{2i-1} p_{2i}$.

Note. A common idea in such problems is to bring factorial into the play. Here, $(n + 1)! + 2, (n + 1)! + 3, \cdots, (n + 1)! + (n + 1)$ are such n consecutive integers. But the motivation behind the solution above is that, we making use of the fact: primes are co-prime to each other. And to make an integer composite, we can just use two or more primes instead of one.

Problem 2.5.8. Suppose that $\{s_1, s_2 \cdots, s_{\phi(m)}\}$ is a reduced residue set modulo m. Find all positive integers a for which $\{s_1 + a, s_2 + a \cdots, s_{\phi(m)} + a\}$ is also a reduced residue set modulo m.

Solution. We claim that the given set is a reduced residue system modulo m if and only if a is divisible by each prime factor of m.

First, suppose that m has a factor p and a is not divisible by p. Let $m = p^\alpha n$ for some positive integer n relatively prime to p. Since $n \perp p$, by CRT, there exists some integer k such that

$$\begin{aligned} k &\equiv -a \pmod{p} \\ k &\equiv \ \ 1 \pmod{n} \end{aligned}$$

Since $k \equiv -a \not\equiv 0 \pmod{p}$, we have $k \perp p$. Also, let $(k, n) = d$. Then $d \mid n \mid k-1$ and $d \mid k$, meaning $d \mid 1$ and so $d = 1$. It follows that $k \perp m$. So, $k \in \{s_1, s_2 \cdots, s_{\varphi(m)}\}$. But $k + a$ is divisible by p, and therefore not relatively prime to n, forcing $\{s_1 + a, s_2 + a \cdots, s_{\varphi(m)} + a\}$ not a reduced residue system.

For the converse, suppose that a is an integer which is divisible by all prime factors of m. Obviously, $s_1 + a, s_2 + a \cdots, s_{\varphi(m)} + a$ are all distinct modulo m. We just need to show that if s is relatively prime to m, then so is $s + a$. For any prime p which divides m, we have $s + a \equiv s \pmod{p}$ because as assumed, a is divisible by p. Since s is co-prime to p, so is $s + a$. Thus $s + a$ is co-prime to all prime factors of m, making it relatively prime to m as well.

Problem 2.5.9 (1997 Czech and Slovak Mathematical Olympiad). Show that there exists an increasing sequence $\{a_n\}_{n=1}^{\infty}$ of natural numbers such that for any $k \geq 0$, the sequence $\{k + a_n\}$ contains only finitely many primes.

It is a standard example of CRT because it is not obvious how CRT comes into the play here.

Solution. Let p_k be the kth prime number. Set $a_1 = 2$. For $n \geq 1$, let a_{n+1} be the least integer greater than a_n that is congruent to $-k$ modulo p_{k+1} for all $k \leq n$. Such an integer exists by the Chinese Remainder Theorem. Thus, for all $k \geq 0$, $k + a_n \equiv 0 \pmod{p_{k+1}}$ for $n \geq k + 1$. Then at most $k + 1$ values in the sequence $\{k + a_n\}$ can be prime since the ith term onward for $i \geq k+2$, the values are nontrivial multiples of p_{k+1} and must be composite. This completes the proof.

Note. We could deal with this using $a_n = (p_n - 1)!$ as well, combining with Wilson's theorem. Because if $k > 1$ then $p_n - 1 > k$ for sufficiently large n so it will be composite from that n. Otherwise $(p - 1)! + 1$ is divisible by p, so it is composite as well.

§§2.6 Wilson's Theorem

We have probably discussed that if $n > 4$ is a composite integer, then $(n-1)!$ is divisible by n. What if n is a prime? Take $n = 3$, then $(n - 1)! = 2$, not divisible by 3. Take $n = 5$. $(n - 1)! = 24$, which is not divisible by 5. Take $n = 7$, then $(n - 1)! = 120$ which is not divisible by 7. Take $n = 11$, $(n - 1)! = 3\,628\,800$ and this is not divisible by 11 either. Since they are not divisible by the primes (as expected), we should check for remainders. 2! leaves a remainder 2 when divided by 3. 4! leaves 4 when divided by 5, 6! leaves 6 when divided by 7. If you calculate further, you will see the pattern goes on. So it suggests us to conjecture that the remainder of $(p - 1)!$ when divided by the prime p is $p - 1$. In fact, this is what we call *Wilson's theorem*.

Theorem 2.6.1. *Let p be a prime number and a is a positive integer. Show that if the inverse of a modulo p is equal to a, then $a \equiv 1$ or $p - 1 \pmod{p}$.*

Proof. The proof for $p = 2$ is obvious, so assume that $p > 2$. The inverse of a is itself, so $a^2 \equiv 1 \pmod{p}$. This means that $p \mid a^2 - 1$. So, p divides $(a-1)(a+1)$. We know that $2 \mid (a-1, a+1)$, so p divides either $a+1$ or $a-1$, which results in $a \equiv 1$ or $p-1 \pmod{p}$. □

Now, why are we concerned about such a situation at all? The inverse of a being a is not something of interest, at least not obviously. In fact, there is a reason behind it. And you should have thought of it before reaching this point. Notice that, in the congruence

$$(p-1)! \equiv (p-1) \pmod{p}$$

$(p-1)$ is co-prime to p. So we can cancel it from both sides and get $(p-2)! \equiv 1 \pmod{p}$. Now, this is interesting and it asks us to reach 1 from a product. Notice the following rearrangement for $p = 11$.

$$\begin{aligned} 9! &= 1 \cdot 2 \cdots 9 \\ &= (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) \\ &= 12 \cdot 12 \cdot 45 \cdot 56 \\ &\equiv 1 \cdot 1 \cdot 1 \cdot 1 \pmod{15} \end{aligned}$$

Does it make sense now why the theorem above is necessary? If not, think a little bit more. Then proceed and you will realize we have actually found the crucial step to prove Wilson's theorem.

According to this theorem, the only two numbers in the set $\{1, 2, \ldots, p-1\}$ which have their inverse equal themselves are 1 and $p-1$. This will help us to prove the Wilson's theorem.

Theorem 2.6.2 (Wilson's Theorem). *The positive integer $p > 1$ is a prime if and only if* $(p-1)! \equiv -1 \pmod{p}$.

Proof. We divide the proof of this theorem into two parts. First, we show that if p is a prime, then $(p-1)! \equiv -1 \pmod{p}$. The result is obvious for $p = 2$ and 3. So we assume that $p \geq 5$. According to the Theorem 2.6.1, the only two numbers among $\{1, 2, \ldots, p-1\}$ which have their inverse equal themselves are 1 and $p-1$. Put them away and consider the set $A = \{2, 3 \ldots, p-2\}$. There are $p-3$ elements in this set, and each of them has an inverse modulo p, as proved in Theorem 2.4.9. Furthermore, inverse of each number is congruent to p. This means that the inverses of elements of A are distinct. So we can divide the elements of A into $(p-3)/2$ inverse pairs. Thus

$$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}$$

Multiply 1 and $p-1$ to both sides of the above equation and the proof is complete.

Now, we should show that if n is not a prime number, then $(n-1)! \not\equiv -1 \pmod{n}$. The theorem is obviously true for $n = 3$ and $n = 4$. So assume that $n \geq 5$ is a composite number. We can write $n = pq$ where p and q are integers greater than 1. If $p \neq q$, then both p and q appear in $(n-1)!$, which means $(n-1)! \equiv 0 \pmod{n}$. In case $p = q$, we have $n = p^2$. Note that $n > 2p$ and so both p and $2p$ appear in $(n-1)!$, which again yields to $(n-1)! \equiv 0 \pmod{n}$. □

Corollary 2.6.3. *For a prime p, $(p-2)! \equiv 1 \pmod{p}$.*

Problem 2.6.4. What is the remainder of 24! when divided by 29?

Solution. By Wilson's theorem, $28! \equiv -1 \pmod{29}$. Also,

$$\begin{aligned} -1 \equiv 28! &\equiv 24! \cdot 25 \cdot 26 \cdot 27 \cdot 28 \\ &\equiv 24! \cdot (-4) \cdot (-3) \cdot (-2) \cdot (-1) \\ &\equiv 24! \cdot 24 \\ &\equiv 24! \cdot (-5) \pmod{29} \end{aligned}$$

The last congruence equation can be written as $24! \cdot 5 \equiv 1 \pmod{29}$. In other words, 24! is the modular inverse of 5 modulo 29. The problem now reduces to finding the inverse of 5 modulo 29, which is 6.

Problem 2.6.5. Let n be a positive integer such that

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \ldots + \frac{1}{23} = \frac{n}{23!}$$

Find the remainder of n modulo 13.

Solution. Multiply both sides by 23!. The right side will be n and the left side includes 23 terms all of which are divisible by 13 except $\frac{23!}{13}$. Thus, we must find the remainder of this term modulo 13. Note that

$$\begin{aligned} \frac{23!}{13} &= 12! \cdot 14 \cdot 15 \cdots 23 \\ &\equiv -1 \cdot 1 \cdot 2 \cdots 10 \\ &\equiv -10! \pmod{13} \end{aligned}$$

This means that we only need to find the remainder of $-10!$ modulo 13. We will use the same trick as in the previous problem:

$$\begin{aligned} -1 \equiv 12! &\equiv 10! \cdot 11 \cdot 12 \\ &\equiv 10! \cdot (-2) \cdot (-1) \\ &\equiv 10! \cdot 2 \pmod{13} \end{aligned}$$

Rewriting the last equation, we find that 2 is the modular inverse of $-10!$ modulo 13. Therefore, the answer is the modular inverse of 2 mod 13, which is 7.

Try the next problem yourself!

Problem 2.6.6. Let p be a prime such that $p \equiv 1 \pmod{4}$. Prove that

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod{p}$$

§§2.7 Euler and Fermat's Theorem

Find the remainder of 2016^{2016} when divided by 2017. You might think we are joking but we are not. Without explicitly calculating this BIG integer, number theorists will tell you the remainder is 1. They will even consider this trivial. This demonstrates another important aspect of numbers. If you know how numbers dance, you know numbers. Anyway, as you may have already guessed, there is a theorem for it. But we want to focus on the intuition part. What could lead you to find this remainder without actually calculating it? If you have been attentive so far, you should already understand that you should focus on finding a 1 when you are multiplying (obviously, since we want to reduce the work we do!). We can try this in couple of ways, but let us start with the most obvious one. Even before that, have you noticed that 2017 is a prime? This may not be of much importance right now, but keep going. Instead of such big numbers, try a smaller example first. Find 6^6 modulo 7

$$\begin{aligned} 6^1 &\equiv -1 \pmod 7 \\ 6^2 &\equiv \ \ 1 \pmod 7 \end{aligned}$$

We already have 1. Is it clear to you that we will reach 1 in 6^4 and 6^6 as well? If not, just calculate them by hand and see if this is true or false. We will come back to this topic later. But it seems we have the result 1. Now, do this for $4^4 \pmod 5$ and $10^{10} \pmod{11}$. After you have done all the work, you should realize, like in Wilson's theorem, we are getting 1 again. This should encourage you to experiment with some further values such as $2^4 \pmod 5$, $3^6 \pmod 7$ etc. Surprisingly, the result is always 1 when the exponent is 1. *Pierre De Fermat* was the first one to observe and propose this.

Theorem 2.7.1 (Fermat's Little [8] Theorem). *If p is a prime and a is a positive integer such that $a \perp p$. Then*

$$a^{p-1} \equiv 1 \pmod p$$

Again, let's see an example. Take $a = 3$ and $p = 7$. And consider the numbers $3 \cdot 1, 3 \cdot 2, 3 \cdot 3, 3 \cdot 4, 3 \cdot 5, 3 \cdot 6$ modulo 7. They are respectively $3, 6, 2, 5, 1, 4$. Notice anything? It's just a rearrangement of $1, 2, \dots, 6$. In fact we already proved it before! Now we will just multiply them all to get

$$3 \cdot 1 \times 3 \cdot 2 \times 3 \cdot 3 \times 3 \cdot 4 \times 3 \cdot 5 \times 3 \cdot 6 \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \pmod 7$$

Collecting all 3's in the left-hand side, we will have

$$3^6 \times 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \pmod 7$$

[8] Fermat proposed (but did not prove) another theorem in number theory which is much more difficult than this one. So they call this theorem the "little" one. The other theorem is called Fermat's Last Theorem.

Since $1, 2, \dots, 6$ are all co-prime to 7, we can divide both sides of the above equation by $1 \cdot 2 \cdots 6$ to obtain

$$3^6 \equiv 1 \pmod 7$$

It is now clear that the same argument works for the general case.

Proof. From the Definition 2.3.0.1, it is clear that the set $A = \{0, 1, \dots, p-1\}$ is a complete residue system modulo p. We know that $a \perp p$, so from Proposition 2.3.2 the set $A' = \{0 \cdot a, 1 \cdot a, \dots, (p-1) \cdot a\}$ is also a complete residue system modulo p. Putting aside the first element, 0, it is clear that the product of the elements of A and A' are congruent modulo p:

$$1 \times a \cdot 2 \times a \cdots (p-1) \times a \equiv 1 \cdot 2 \cdots (p-1) \pmod p y$$

So, we find that

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod p. \tag{2.4}$$

In congruence equation (2.4), we can use the fact that $(p, (p-1)!) = 1$ to divide both sides by $(p-1)!$ and obtain $a^{p-1} \equiv 1 \pmod p$. □

You can find some other proofs for Fermat's Little Theorem that use either number theoretic techniques or even combinatorial approaches. For a very strange yet interesting proof of this theorem, read the proof by counting necklaces in Engel.[9]

Corollary 2.7.2. *If p is a prime and a is an arbitrary positive integer (not necessarily co-prime with p), then*

$$a^p \equiv a \pmod p$$

Fermat's little theorem comes in handy in so many situations, but it only handles prime numbers. So we present the Euler's theorem which is a more general form of Fermat's little theorem. The proof is similar as well. Let's take the following example.

Problem 2.7.3. Show that $4^{20} + 6^{40} + 12^{60}$ is divisible by 13.

Solution. Obviously, $12^{60} \equiv (-1)^{60} \equiv 1 \pmod{13}$. By Fermat's little theorem, $6^{12} \equiv 1 \pmod{13}$, hence

$$\begin{aligned} 6^{40} &\equiv 6^{36} \cdot 6^4 \\ &\equiv \left(6^{12}\right)^3 \cdot 6^4 \\ &\equiv 6^4 \\ &\equiv 9 \pmod{13} \end{aligned}$$

We can apply the same method to find $4^{20} \equiv 3 \pmod{13}$. Finally,

$$\begin{aligned} 4^{20} + 6^{40} + 12^{60} &\equiv 3 + 9 + 1 \\ &\equiv 0 \pmod{13} \end{aligned}$$

[9] Arthur Engel. *Problem-solving strategies*. Springer, 1997.

Here Andreescu, Andrica, and Feng[10] is an easy consequence of Fermat's little theorem.

Problem 2.7.4. For integers a, b, prove that $a^p b - ab^p$ is divisible by p.

Solution. This problem is kind of a direct consequence of Fermat's little theorem. Write $a^p b - ab^p = ab(a^{p-1} - b^{p-1})$. If one of a or b is divisible by p, we are done. If neither of them is divisible by p, then $a^{p-1} \equiv 1 \equiv b^{p-1} \pmod{p}$. So, p divides $a^{p-1} - b^{p-1}$.

The next problem is taken from Sierpiński.[11]

Problem 2.7.5. Prove that there exist infinitely many composite numbers of the form $(2^{2^n} + 1)^2 + 4$, where n is a positive integer.

Solution. A common approach for this kind of problems is to take different moduli (the first ones would be primes, obviously). Here, we will make use of modulo 29. We will show that for any n of the form $28k + 1$ (for $k \geq 1$), the number $(2^{2^n} + 1)^2 + 4$ will be divisible by 29. By Fermat's theorem, $2^{2 \cdot 28k} \equiv 1 \pmod{29}$. Therefore, for $n = 28k + 1$,

$$\begin{aligned}(2^{2^n} + 1)^2 + 4 &\equiv (2^{2\cdot(28k+1)} + 1)^2 + 4 \\ &\equiv (2^2 + 1)^2 + 4 \\ &\equiv 0 \pmod{29}\end{aligned}$$

Theorem 2.7.6 (Euler's [12] Theorem). *If a and n are positive integers such that $a \perp n$. Then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

where φ is the Euler's totient function.

Proof. Before we start the proof, remember Definition 2.3.0.2 where we defined Euler's totient function. The proof is very similar to the proof of Fermat's theorem and you only need to apply Proposition 2.3.5 once. Let $A = \{a_1, a_2, \cdots, a_{\varphi(m)}\}$ be a reduced residue set mod m. Then so is $B = \{aa_1, aa_2, \cdots, aa_{\varphi(m)}\}$. From the definition of reduced systems, any number which is relatively prime to m is congruent to exactly one element of A and exactly one element of B. Thus, the product of all elements of A must be congruent to that of B, modulo B. Therefore

$$\begin{aligned}&(aa_1)(aa_2)\cdots(aa_{\varphi(m)}) \equiv a_1 a_2 \cdots a_{\varphi(m)} \pmod{m} \\ \implies\ &a^{\varphi(m)} \cdot \left(a_1 a_2 \cdots a_{\varphi(m)}\right) \equiv a_1 a_2 \cdots a_{\varphi(m)} \pmod{m} \\ \implies\ &a^{\varphi(m)} \equiv 1 \pmod{m} \qquad (2.5)\end{aligned}$$

Note that in equation (2.5) we have used the fact that $a_i \perp m$ for $1 \leq i \leq \varphi(m)$, which results in $a_1 a_2 \cdots a_{\varphi(m)} \perp m$. □

[10] Titu Andreescu, D. Andrica, and Zuming Feng. *104 number theory problems: from the training of the USA IMO team*. Birkhäuser, 2007, Page 29, Example 1.29.

[11] Wacław Sierpiński. *Elementary theory of numbers*. eng. 1964. URL: http://eudml.org/doc/219306, Problem 124.

[12] Sometimes called Fermat-Euler theorem or Euler's totient theorem, proposed by Euler in 1763.

We can easily conclude the Fermat's little theorem from Euler's theorem: for a prime p, we have $\varphi(p) = p-1$ and so $a^{\varphi(p)} \equiv a^{p-1} \equiv 1 \pmod{p}$ for any integer a not divisible by p.

Problem 2.7.7. Let a and b be positive integers. Prove that in the arithmetic progression $ak+b$ (for $k \geq 0$ an integer), there exist infinitely many terms with the same prime divisors.

Solution. It's not obvious at all how we should approach this problem. First, let us discard the common factor between a and b so they do not have any common factor. Then we see that $ak + b = d(uk + v)$ for some relatively prime u, v. Since d is a fixed positive integer, we now have to worry about $uk + v$ only. We want to show that there are many k such that $uk+v$ has a fixed set of prime divisors. So, if we could show anyhow that $uk + v$ is the power of the same number for infinitely many k, that would give us a solution (note that the converse does not have to be true).

Let $d = (a, a + b)$. There exist positive integers a_1 and c such that

$$\begin{aligned} a &= da_1 \\ a + b &= dc \end{aligned}$$

Also, $(a_1, c) = 1$ and $c > 1$ (why?). Using Euler's theorem, one can write $c^{n\varphi(a_1)} \equiv 1 \pmod{a_1}$ for any positive integer n. This means that there exists a positive integer t_n such that $c^{n\varphi(a_1)} - 1 = t_n a_1$. Now,

$$\begin{aligned} a(ct_n + 1) + b &= da_1(ct_n + 1) + (dc - da_1) \\ &= dc(t_n a_1 + 1) \\ &= dc\left(c^{n\varphi(a_1)}\right) \\ &= dc^{n\varphi(a_1)+1} \end{aligned}$$

Therefore, the only prime divisors of the term $a(ct_n + 1) + b$ in the progression are prime divisors of dc, which are fixed (because d and c depend only on a and b, which are fixed). This means that there exist infinitely many terms in the sequence which have the same prime divisors and we are done.

Here is an exercise for you.

Problem 2.7.8. Find all primes p such that p^2 divides $5^{p^2} + 1$

§§2.8 Quadratic Residues

Let n be a fixed positive integer. There are many cases when we are interested in integers a relatively prime to n for which there exists another integer x such that $a \equiv x^2 \pmod{n}$. As an example, assume that we want to solve the quadratic congruence relation

$$ax^2 + bx + c \equiv 0 \pmod{n}$$

for x. Multiply both sides of the above relation by $4a$ to obtain

$$4a^2x^2 + 4abx + c \equiv 0 \pmod{n}$$

Rewriting the left side of the last relation as $(2ax+b)^2 - b^2 + c$, we have

$$(2ax+b)^2 \equiv b^2 - c \pmod{n}$$

which is of the form $y^2 \equiv z \pmod{n}$. Therefore, solving any quadratic congruence relation is equivalent to solving $x^2 \equiv a \pmod{n}$ for some a. We call such an a a quadratic residue modulo n. Quadratic residues play an important role in cryptography. They are even used in acoustical engineering.

In this section, we will discuss different aspects of quadratic residues in number theory.

Quadratic Residue. Let $m > 1$ be a positive integer and let a be an integer such that $(a, n) = 1$. Then a is a *quadratic residue* of n if there exists an integer x such that

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

If there is no such x, then a is a *quadratic non-residue* of n.

Example. 2 is a quadratic residue modulo 7 because $3^2 \equiv 2 \pmod{7}$. However, 3 is a non-residue modulo 7. In fact, modulo 7,

$$\begin{aligned} 1^2 &\equiv 1, & 2^2 &\equiv 4 \\ 3^2 &\equiv 2, & 4^2 &\equiv 2 \\ 5^2 &\equiv 4, & 6^2 &\equiv 1 \end{aligned}$$

This means that the only quadratic residues modulo 7 are 1, 2, and 4.

Corollary 2.8.1. *If $a \equiv b \pmod{n}$, then a is a quadratic residue (non-residue) modulo n, then so is b.*

Note. Whenever we say that an integer a is a quadratic residue (non-residue) modulo n, it is clear that $a + kn$ is also a quadratic residue(non-residue) modulo n. Therefore, in order to find which numbers are quadratic residues modulo n, we only need to check the numbers $1, 2, \dots, n-1$. Obviously, $a = 0$ is a quadratic residue modulo any n, and we omit this case in our calculations.

Theorem 2.8.2. *Let p be an odd prime number. There are exactly $\dfrac{p-1}{2}$ quadratic residues modulo p (excluding zero). Furthermore, the residues come from the numbers $1^2, 2^2, \dots, \left(\dfrac{p-1}{2}\right)^2$.*

Proof. Clearly, the quadratic residues modulo p are

$$1^2, 2^2, \dots, (p-1)^2 \pmod{p}$$

Note that $x^2 \equiv (p-x)^2 \pmod{p}$ for $x = 1, 2, \dots, p-1$. So we only need to go halfway, i.e., we should only consider the numbers

$$1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2 \pmod{p}$$

These numbers are distinct modulo p, because otherwise if $x^2 \equiv y^2 \pmod{p}$ for some $x, y \in \{1, 2, \dots, \frac{p-1}{2}\}$, then

$$\begin{aligned} & p \mid x^2 - y^2 \\ \implies & p \mid (x-y)(x+y) \end{aligned}$$

But note that $x+y < \frac{p-1}{2} + \frac{p-1}{2} = p-1$, and so $p \nmid x+y$, which means $p \mid x-y$. Finally, since x and y are less than p, we should have $x = y$. So we have proved that there are exactly $(p-1)/2$ quadratic residues and they are

$$1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$$

□

Theorem 2.8.3. *Let p be an odd prime. Then,*

(i) the product of two quadratic residues is also a quadratic residue,

(ii) the product of two quadratic non-residues is also a quadratic residue, and

(iii) the product of a quadratic residue and a quadratic non-residue is a quadratic non-residue.

Proof. The first one is obvious. If $a \equiv x^2 \pmod{p}$ and $b \equiv y^2 \pmod{p}$, then $ab \equiv (xy)^2 \pmod{p}$. Let's prove *(iii)* now. Assume that $a \equiv x^2$ is a residue and b is a non-residue modulo p and suppose to the contrary that ab is a residue and $ab \equiv y^2 \pmod{p}$. Then

$$\begin{aligned} ab &\equiv x^2 b \\ &\equiv y^2 \pmod{p} \end{aligned}$$

Note that since $(x^2, p) = (a, p) = 1$, the multiplicative inverse of x^2 exists. Therefore

$$\begin{aligned} b &\equiv (x^2)^{-1} \cdot y^2 \\ &\equiv (x^{-1})^2 \cdot y^2 \\ &\equiv (x^{-1} \cdot y)^2 \pmod{p} \end{aligned}$$

which contradicts the assumption that b is a non-residue. So ab is a non-residue. In order to prove *(ii)*, we use the fact that if a is an integer relatively prime to p, then

$$\{a, 2a, \dots, (p-1)a\} = \{1, 2, \dots, p-1\}$$

(The proof is easy, try it yourself). From Theorem 2.8.2, we see that there are exactly $(p-1)/2$ quadratic residues among $\{a, 2a, \dots, (p-1)a\}$. Assume that a is a fixed

quadratic non-residue modulo p. From the proof of (*iii*), we can say that whenever a is multiplied by one of $\frac{p-1}{2}$ quadratic residues of the set $\{1, 2, \dots, p-1\}$, the result is a non-residue. Therefore, each non-residue element of $\{a, 2a, \dots, (p-1)a\}$ is multiplication of a by a residue in the same set. This means that the multiplication of a by any non-residue element of the set $\{a, 2a, \dots, (p-1)a\}$ is a residue, and we are done. □

Theorem 2.8.3 gives us a nice result. Quadratic residues and quadratic non-residues act just like 1 and -1. How? Notice that $1 \times 1 = 1$, $(-1) \times 1 = -1$, and $(-1) \times (-1) = 1$, and this guides us to a point that quadratic residues behave like 1, and quadratic non-residues behave like -1. We can represent this result using Legendre's notation.

Legendre Symbol. We call $\left(\frac{a}{p}\right)$ the *Legendre symbol* for a prime p. It is defined by:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } a \text{ is a quadratic residue of } p \\ -1 & \text{otherwise} \end{cases}$$

Using this notation, Theorem 2.8.3 becomes

Theorem 2.8.4. *Let p be an odd prime and let a, b be two integers. Then*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Remark. Clearly, the same relation holds for the product of any n integers, that is,

$$\left(\frac{a_1 a_2 \cdots a_n}{p}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_n}{p}\right)$$

Example. Theorem (2.8.4) is helpful specially when dealing with big numbers. For instance, let's see if 18 is a quadratic residue modulo 73. According to the theorem,

$$\left(\frac{18}{73}\right) = \left(\frac{3}{73}\right)\left(\frac{3}{73}\right)\left(\frac{2}{73}\right)$$

Note that we don't need to calculate $\left(\frac{3}{73}\right)$ because whatever it is (-1 or 1), it has appeared twice and $1^2 = (-1)^2 = 1$. So

$$\left(\frac{18}{73}\right) = \left(\frac{2}{73}\right)$$

Now, how can we find $\left(\frac{2}{73}\right)$? It would be a pain to check all the values $1, 2, \dots, \frac{73-1}{2}$ to see if square of any of them is equal to 2 modulo 73. There are two ways to trick this. One is to use the general formula for $\left(\frac{2}{p}\right)$ which will be discussed next. The second (and better) idea is to *construct* the solution. Assume that you have a prime p and an integer a relatively prime to p. We know from Corollary 2.8.1 that if a is a residue (non-residue), then $a + kp$ is also a residue (non-residue). So we will add multiples of p to a and check if we have reached a perfect square. If yes, then a is a residue. Otherwise, we factorize

the new number into perfect squares times some other number b. Continue this process until you reach either a non-residue b (which means a was a non-residue) or a perfect square factorization (which means a was a residue). This whole process might seem a little confusing to you, but applying it to our case ($a = 2, p = 73$) will make it clear:

$$\begin{aligned} 2 &\equiv 75 \equiv 148 \equiv 2^2 \cdot 37 \\ &\equiv 2^2 \cdot (37 + 73) \equiv 2^2 \cdot 110 \\ &\equiv 2^2 \cdot (110 + 73) \equiv 2^2 \cdot 183 \\ &\equiv 2^2 \cdot (183 + 73) \equiv 2^2 \cdot 256 \\ &\equiv 2^2 \cdot 16^2 \\ &\equiv 32^2 \end{aligned}$$

So 2 is a quadratic residue modulo 73 and finally

$$\left(\frac{18}{73}\right) = \left(\frac{2}{73}\right) = 1$$

§§§2.8 Euler's Criterion

In the last example of previous section, we provided a method for computing $\left(\frac{a}{p}\right)$. However, this method only works when p and a are small enough to make the calculations. Fortunately, Euler developed a criteria to find out whether an integer is a quadratic residue or a quadratic non-residue. After we explain and prove Euler's criterion, we will explore some special cases, e.g., we will find the value of $\left(\frac{2}{p}\right)$ and $\left(\frac{-1}{p}\right)$ for all primes p.

Theorem 2.8.5 (Euler's Criterion). *Let p be an odd prime and let a be an integer relatively prime to p. Then*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

Proof. First notice that from Fermat's theorem, $a^{p-1} \equiv 1 \pmod{p}$. Since $p-1$ is even, we can write this as

$$\begin{aligned} a^{p-1} - 1 &= \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \\ &\equiv 0 \pmod{p} \end{aligned}$$

So either $a^{\frac{p-1}{2}} \equiv 1$ or $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Assume that a is a quadratic residue modulo p. That is, $\left(\frac{a}{p}\right) = 1$. We should prove that $a^{\frac{p-1}{2}} \equiv 1$. Since a is a residue, there exists some integer x for which $a \equiv x^2 \pmod{p}$. So, from Fermat's theorem,

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

Now assume the case where a is a quadratic non-residue modulo p. Then we should prove that $a^{\frac{p-1}{2}} \equiv -1$. We will use an interesting approach here. Let $b \in \{1, 2, \dots, p-1\}$.

Since $(b,p)=1$, the congruence equation $bx \equiv a$ has a unique solution $x \equiv a \cdot b^{-1} \pmod{p}$. Also, $x \not\equiv b \pmod{p}$ because otherwise $b^2 \equiv a \pmod{p}$ which is in contradiction with a being a non-residue. This means that the set $\{1,2,\dots,p-1\}$ can be divided into $\dfrac{p-1}{2}$ pairs (b,x) such that $bx \equiv a \pmod{p}$. So

$$\begin{aligned}(p-1)! &= 1 \times 2 \times \cdots \times (p-1) \\ &\equiv \underbrace{a \times a \times \cdots \times a}_{\frac{p-1}{2} \text{ times}} \\ &\equiv a^{\frac{p-1}{2}} \pmod{p}\end{aligned}$$

By Wilson's theorem, $(p-1)! \equiv -1 \pmod{p}$ and therefore $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, as desired. The proof is complete. □

Let's find $\left(\frac{a}{p}\right)$ for some small values of a.

Problem 2.8.6. What is $\left(\frac{-1}{p}\right)$ for a prime p?

Solution. This is a simple case. By Euler's criterion, we get

$$(-1)^{\frac{p-1}{2}} \equiv \left(\frac{-1}{p}\right) \pmod{p}$$

If $p \equiv 1 \pmod{4}$, that is, if $p = 4k+1$, then $\frac{p-1}{2}$ is even and so $(-1)^{\frac{p-1}{2}} = 1$. On the other side, we know that $\left(\frac{-1}{p}\right)$ is either 1 or -1. So in this case it must equal one. This means that

$$\begin{aligned} & p \equiv 1 \pmod{4} \\ \iff & \left(\frac{-1}{p}\right) = 1\end{aligned}$$

Note that the *only if* part of the above statement is true because if $(-1)^{\frac{p-1}{2}} = 1$, then $\frac{p-1}{2} = 2k$ for some integer k. So $p = 4k+1$, or $p \equiv 1 \pmod{4}$. You can easily check that the following statement is also true

$$\begin{aligned} & p \equiv 3 \pmod{4} \\ \iff & \left(\frac{-1}{p}\right) = -1\end{aligned}$$

Each prime has either the form $p \equiv 1 \pmod{4}$ or $p \equiv 3 \pmod{4}$, so these primes together make all primes. All in all,

Theorem 2.8.7. *For all primes p,*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{4} \text{ or } p = 2 \\ -1, & \text{if } p \equiv 3 \pmod{4} \end{cases}$$

This infers the following theorem and the next.

Theorem 2.8.8. *-1 is a quadratic residue of a prime p if and only if $p \equiv 1 \pmod 4$.*

Theorem 2.8.9. *Let a and b be relatively prime positive integers. Then every prime divisor of a^2+b^2 is either 2 or of the form $4k+1$.*

Proof. Let p be a prime divisor of a^2+b^2. If a and b both are odd then p can be 2. Now assume p is larger than 2. Then

$$\begin{aligned} & a^2 \equiv -b^2 \pmod p \\ \implies & (a^2)^{\frac{p-1}{2}} \equiv (-b^2)^{\frac{p-1}{2}} \pmod p \end{aligned}$$

If p is of the form $4k+3$, then $\frac{p-1}{2} = 2k+1$ is odd, hence,

$$\begin{aligned} & (a^2)^{\frac{p-1}{2}} \equiv (-b^2)^{\frac{p-1}{2}} \pmod p \\ \implies & a^{p-1} \equiv -b^{p-1} \pmod p \end{aligned}$$

Clearly, since $p \mid a^2+b^2$, if p divides one of a or b, it should divide the other one. But this is impossible because $a \perp b$. So $p \perp a$ and $p \perp b$. By Fermat's little theorem, $a^{p-1} \equiv b^{p-1} \equiv 1 \pmod p$, which is in contradiction with the above equation since p is odd. So, p cannot be of the form $4k+3$ and therefore every odd prime divisor of a^2+b^2 is of the form $4k+1$. □

Note. We could just say,

$$\begin{aligned} & a^2 \equiv -b^2 \pmod p \\ \implies & (ab^{-1})^2 \equiv -1 \pmod p \end{aligned}$$

which means that -1 is a quadratic residue of p, and therefore $p \equiv 1 \pmod 4$.

We get the following corollary, which can directly solve an IMO problem.

Corollary 2.8.10. *Let k be a positive integer. Every divisor of $4k^2+1$ is of the form $4n+1$ for some integer n.*

Proof. Thanks to the previous theorem, we know that all the prime divisors of $4k^2+1$ are of the form $4t+1$. Every divisor of $4k^2+1$ is a multiplication of its prime divisors. And if we multiply two numbers of the form $4t+1$, then the number is again of the same form (multiply $4x+1$ and $4y+1$ and see the result yourself). Hence, conclusion. □

Problem 2.8.11 (Iran, Third Round Olympiad, 2007). Can $4xy-x-y$ be a square for integers x and y?

Solution. Assume that $4xy-x-y=t^2$. We can rearrange it as $x(4y-1)=t^2+y$, so

$$\begin{aligned} & 4y-1 \mid t^2+y \\ \implies & 4y-1 \mid 4t^2+4y \\ \implies & 4y-1 \mid 4t^2+4y-(4y-1) \\ \implies & 4y-1 \mid 4t^2+1 \end{aligned}$$

Since $4y-1$ is of the form $4k+3$, it must have at least one prime factor of the form $4j+3$. Then we have a prime factor of $4t^2+1$ which is of this form, a contradiction. Thus, it can't be a square.

Back to quadratic residues, the next step is to determine if 2 is a quadratic residue modulo a prime. Unfortunately, we cannot apply Euler's criterion directly in this case because we do not know what $2^{\frac{p-1}{2}} \pmod p$ would be for different values of p. So our challenge is to find $2^{\frac{p-1}{2}}$ modulo p.

Problem 2.8.12. What is $\left(\frac{2}{p}\right)$ for a prime p?

Solution. As explained just above, we only need to find a way to calculate $2^{\frac{p-1}{2}} \pmod p$. The idea is similar to what we did in the proof of Fermat's little theorem. Remember that in Fermat's theorem, we needed to somehow construct a^{p-1} and we did that by multiplying elements of the set $\{a, 2a, \dots, (p-1)a\}$. Now how can we construct $2^{\frac{p-1}{2}}$? The idea is to find a set with $\frac{p-1}{2}$ elements such that the product of all elements has the factor $2^{\frac{p-1}{2}}$. One possibility is to consider the set $A = \{2, 4, \dots, p-1\}$. Then the product of elements of A is

$$\begin{aligned} 2 \times 4 \times \cdots \times (p-1) &= 2^{\frac{p-1}{2}} \times 1 \times 2 \times \cdots \times \frac{p-1}{2} \\ &= 2^{\frac{p-1}{2}} \times \left(\frac{p-1}{2}\right)! \end{aligned} \tag{2.6}$$

In order to get rid of the term $\left(\frac{p-1}{2}\right)!$, we have to compute the product of elements of A in some other way. Notice that we are looking for $2 \times 4 \times \cdots \times (p-1)$ and we want to make it as close as possible to $\left(\frac{p-1}{2}\right)!$ so that we can cancel out this term and find the value of $2^{\frac{p-1}{2}} \pmod p$. To construct this factorial, we need all the numbers in the set

$$B = \left\{1, 2, \dots, \frac{p-1}{2}\right\}$$

However, we only have even integers in A. For example, take $p = 11$. Then $A = \{2, 4, 6, 8, 10\}$ and $B = \{1, 2, 3, 4, 5\}$. Now, we want to construct $5!$ using the product of elements of A. Clearly, the elements 2 and 4 are directly chosen from A. Now it remains to somehow construct the product $1 \times 3 \times 5$ with the elements $6, 8, 10$. The trick is pretty simple: just notice that $10 \equiv -1, 8 \equiv -3$, and $6 \equiv -5 \pmod{11}$. This means that $6 \times 8 \times 10 \equiv (-1)^3 \cdot 1 \times 3 \times 5$, and so

$$2 \times 4 \times 6 \times 8 \times 10 \equiv (-1)^3 \cdot 5! \tag{2.7}$$

Comparing equations (2.6) (for $p = 11$) and (2.7), we find that

$$\begin{aligned} &2^5 \cdot 5! \equiv (-1)^3 \cdot 5! \pmod{11} \\ \implies &2^5 \equiv (-1)^3 \\ &\equiv -1 \pmod{11} \end{aligned}$$

Let's go back to the solution of the general problem. As in the example of $p = 11$, we are searching for the power of (-1) appeared in the congruence relation. In fact, this power equals the number of even elements bigger than $\frac{p-1}{2}$ and less than or equal to $p-1$. Depending on the remainder of p modulo 8, this power of (-1) can be even or

odd. Consider the case when $p \equiv 1 \pmod 8$. Then $p-1 = 8k$ for some positive integer k and so the even numbers less than or equal to $\frac{p-1}{2} = 4k$ in the set $A = \{2, 4, \dots, 8k\}$ are $2, 4, \dots, 4k$, which are $2k+1$ numbers. Therefore

$$\begin{aligned} 2 \times 4 \times \cdots \times (p-1) &= \overbrace{(2 \times 4 \times \cdots \times 4k)}^{2k+1 \text{ items}} \cdot \overbrace{((4k+2) \times (4k+4) \times \cdots \times 8k)}^{2k \text{ items}} \\ &\equiv (2 \times 4 \times \cdots \times 4k) \cdot ((-(4k-1)) \times (-(4k-3)) \times \cdots \times (-1)) \\ &\equiv (-1)^{2k} \cdot (4k)! \\ &\equiv (-1)^{2k} \cdot \left(\frac{p-1}{2}\right)! \pmod p \end{aligned}$$

Compare this result with (2.6), you see that

$$\begin{aligned} 2^{\frac{p-1}{2}} \times \left(\frac{p-1}{2}\right)! \equiv (-1)^{2k} \cdot \left(\frac{p-1}{2}\right)! \pmod p \\ \implies 2^{\frac{p-1}{2}} \equiv (-1)^{2k} \equiv 1 \pmod p \end{aligned}$$

So if $p \equiv 1 \pmod 8$, then $\left(\frac{2}{p}\right) = 1$.

The process is similar for $p \equiv 3, 5, 7 \pmod 8$ and we put it as an exercise for the reader.

After all this work, we are finally done computing $\left(\frac{2}{p}\right)$. The final result is stated in the following theorem.

Theorem 2.8.13.

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \text{ or } 7 \pmod 8 \\ -1, & \text{if } p \equiv 3 \text{ or } 5 \pmod 8 \end{cases}$$

We can generalize the method used in the solution of Problem 2.8.12 to find $\left(\frac{a}{p}\right)$ for all integers a and primes p.

Theorem 2.8.14 (Gauss' Criterion). *Let p be a prime number and let a be an integer relatively prime to p. Let $\mu(a, p)$ denote the number of integers x among*

$$a, 2a, \dots, \frac{p-1}{2}a$$

such that $x > p/2 \pmod p$. Then

$$\left(\frac{a}{p}\right) = (-1)^{\mu(a,p)}$$

The proof is left as an exercise for the reader.

Theorem 2.8.15. *The smallest quadratic non-residue of a prime p is a prime less than $\sqrt{p} + 1$.*

Proof. Let r be the smallest quadratic non-residue of prime p. Then, any $i < r$ is a quadratic residue of p. If $r = kl$ for $k, l > 1$, using Legendre's symbol, we have

$$\left(\frac{r}{p}\right) = \left(\frac{k}{p}\right) \cdot \left(\frac{l}{p}\right)$$

which gives $-1 = 1 \cdot 1$ (since r is a quadratic non-residue modulo p) and we get a contradiction. So, r can't be a prime. Let's move on to the next part of the theorem.

We have that $r, \cdots, (r-1)r$ are quadratic non-residues mosulo p. If any of them is greater than p, say ri, we have $r(i-1) < p < ri$ for some i. But then,

$$ri < p + r$$

so that $ri = p + s$ with $s < r$. Thus,

$$\begin{aligned} ri &= p + s \\ &\equiv s \pmod{p} \end{aligned}$$

Since $s < r$, s is a quadratic residue of p, which in turn means ri is a quadratic residue of p as well. Another contradiction, so $r(r-1) < p$. If $r \geq \sqrt{p} + 1$, we have $r(r-1) \geq \sqrt{p}(\sqrt{p}+1) = p + \sqrt{p} > p$, yet another contradiction. The claim is therefore true. □

§§§2.8 Quadratic Reciprocity

Assume we want to compute $\left(\frac{a}{p}\right)$ for some integer a and a prime p. The remark after Theorem 2.8.4 says that it's enough to find

$$\left(\frac{a_1}{p}\right), \left(\frac{a_2}{p}\right), \ldots, \left(\frac{a_n}{p}\right)$$

where $a_1, a_2, \ldots, a_n$ are divisors of a. This means that if we know the value of $\left(\frac{q}{p}\right)$ for a prime q, we can find the values of $\left(\frac{a}{p}\right)$ for any a.

So let's discuss on the value of $\left(\frac{q}{p}\right)$. If q is a big prime number, then by Corollary 2.8.1, we can reduce q modulo p until we reach some $c < p$ and find $\left(\frac{q}{p}\right)$ by some method (Euler's or Gauss's criteria). So we can handle the case when q is a big prime.

Now, what about the case when p is a big prime? In this case, finding $\left(\frac{q}{p}\right)$ would be very hard with theorems and methods stated by now. There is a very nice property of prime numbers which helps us to handle this case. This property is called the *Law of Quadratic Reciprocity* which relates $\left(\frac{q}{p}\right)$ and $\left(\frac{p}{q}\right)$. So, in case q is big, we can first calculate $\left(\frac{q}{p}\right)$ and then use this law to find $\left(\frac{p}{q}\right)$.

Theorem 2.8.16 (Law of Quadratic Reciprocity). *Let p and q be different odd primes. Then*

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

Example. Let's find $\left(\frac{11}{6661}\right)$. We have

$$\left(\frac{11}{6661}\right)\left(\frac{6661}{11}\right) = (-1)^{5\cdot 3330} = -1 \tag{2.8}$$

Now, since $6661 \equiv 6 \pmod{11}$, we obtain

$$\begin{aligned}\left(\frac{6661}{11}\right) &= \left(\frac{6}{11}\right)\\ &= \left(\frac{3}{11}\right)\left(\frac{2}{11}\right)\\ &= 1 \times (-1)\\ &= -1\end{aligned}$$

Replacing in equation (2.8), we finally find

$$\left(\frac{11}{6661}\right) = 1$$

The proof of this theorem is a bit complicated and it would make you lose the continuity of the context. For this reason, we will provide the proof in section (5.9).

§§§2.8 Jacobi Symbol

In previous sections, whenever we used the Legendre symbol $\left(\frac{p}{q}\right)$, we needed p to be a prime number. We are now interested in cases where p can be a composite number. In 1837, Jacobi generalized the symbol used by Legendre in this way:

Jacobi Symbol. Let a be an integer and $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$, where p_i are odd primes and α_i are non-negative integers ($1 \leq i \leq k$). The *Jacobi symbol* is defined as the product of the Legendre symbols corresponding to the prime factors of n:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1}\left(\frac{a}{p_2}\right)^{\alpha_2}\cdots\left(\frac{a}{p_k}\right)^{\alpha_k}$$

Also, we define $\left(\frac{a}{1}\right)$ to be 1.

Remark. The immediate result of the above definition is that if $\gcd(a, n) = 1$, then $\left(\frac{a}{n}\right)$ is either $+1$ or -1. Otherwise, it equals zero.

Example.

$$\begin{aligned}\left(\frac{14}{2535}\right) &= \left(\frac{14}{3}\right)\left(\frac{14}{5}\right)\left(\frac{14}{13}\right)^2\\ &= \left(\frac{2}{3}\right)\left(\frac{4}{5}\right)\left(\frac{1}{13}\right)^2\\ &= (-1)\cdot 1\cdot 1\\ &= -1\end{aligned}$$

Example.

$$\begin{aligned}\left(\frac{2}{15}\right) &= \left(\frac{2}{3}\right)\left(\frac{2}{5}\right)\\ &= (-1)\cdot(-1)\\ &= 1\end{aligned}$$

Note. If $\left(\frac{a}{n}\right) = -1$ for some a and n, then a is a quadratic non-residue modulo n. However, the converse is not necessarily true. The above example shows you a simple case when a is a quadratic non-residue modulo n but $\left(\frac{a}{n}\right) = 1$.

Theorem 2.8.17. *Let a be an integer and $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$, where p_i are odd primes and α_i are non-negative integers $(1 \le i \le k)$. Then a is a quadratic residue modulo n if and only if a is a quadratic residue modulo every $p_i^{\alpha_i}$ $(1 \le i \le k)$.*

Proof. The *if* part is easy to prove. Assume that a is a quadratic residue modulo n and $a \equiv x^2 \pmod{n}$ for some integer x. Then $a \equiv x^2 \pmod{p_i^{\alpha_i}}$ since p_is are relatively prime to each other. Now the *only if* part: assume that $a \equiv x_i^2 \pmod{p_i^{\alpha_i}}$ for all i, where x_i are integers. According to Chinese Remainder Theorem, since the numbers $p_i^{\alpha_i}$ are pairwise relatively prime, the system of congruence equations

$$\begin{aligned}x &\equiv x_1 \pmod{p_1^{\alpha_1}}\\ x &\equiv x_2 \pmod{p_2^{\alpha_2}}\\ &\vdots\\ x &\equiv x_k \pmod{p_k^{\alpha_k}}\end{aligned}$$

has a solution for x. Now $x^2 \equiv x_i^2 \equiv a \pmod{p_i^{\alpha_i}}$, and therefore $x^2 \equiv a \pmod{n}$, which means that a is a quadratic residue modulo n. □

The following theorem sums up almost everything explained in quadratic residues. The proofs are simple and straightforward, so we leave them as exercises for the reader.

Theorem 2.8.18. *Let a and b be any two integers. Then for every two odd integers m and n, we have*

i. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$

ii. $\left(\frac{a+bn}{n}\right) = \left(\frac{a}{n}\right)$

iii. $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$

iv. $\left(\frac{a}{mn}\right) = \left(\frac{a}{n}\right)\left(\frac{a}{m}\right)$

v. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$

vi. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$

Theorem 2.8.19. *If a positive integer is a quadratic residue modulo every prime, then it is a perfect square.*

This is a really cool theorem. However, proving this might be challenging![13] Give it a try.

Theorem 2.8.20. *Let $b, n > 1$ be integers. Suppose that for each $k > 1$ there exists an integer a_k such that $b - a_k^n$ is divisible by k. Prove that $b = A^n$ for some integer A.*

Proof. Assume that b has a prime factor, p, so that $p^{xn+r} \| b$ with $0 < r < n$. Then, we can let $k = p^{xn+n}$. It follows that $b \equiv a_k^n \bmod p^{xn+n}$. Since $p^{xn+r} \| b$, we see that $p^{xn+r} \| a_k^n$. Then, $p^{x+\frac{r}{n}} \| a_k^n$, which is a contradiction since $\frac{r}{n}$ is not an integer. Thus, we have a contradiction, so $r = 0$, which means that only nth powers of primes fully divide b, so b is an nth power. □

§§2.9 Wolstenholme's Theorem

The purpose of this section is to discuss the sum

$$\sum_{k=1}^{p-1} \frac{1}{k} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

Well, not exactly. We are more interested in this sum modulo p where p is a prime. But how do we calculate fractions modulo p? The answer should be obvious by now. $\frac{a}{b} \pmod p$ is actually $ab^{-1} \pmod p$ where $b^{-1} \pmod p$ is the inverse of b modulo p. So if $be \equiv 1 \pmod p$, then

$$\frac{a}{b} \equiv ae \pmod p$$

However, from modular cancellation property, we can take fractions modulo p if $p \nmid b$. Moreover, we can introduce some sort of divisibility here.

Let $\frac{a}{b}$ be a fraction and let n be an integer such that $(n, b) = 1$. If a is divisible by n, we say that $\frac{a}{b}$ is divisible by n. Following this convention, the congruence $\frac{a}{b} \equiv 0 \pmod n$ makes sense.

Example. Since $25 \mid 100$ and $(3, 25) = 1$, we have $\frac{100}{3} \equiv 0 \pmod 3$. We can also calculate it this way:

$$\begin{aligned} \frac{100}{3} &\equiv 100 \cdot (3)^{-1} \\ &\equiv 100 \cdot 17 \\ &\equiv 0 \pmod{25} \end{aligned}$$

[13] A popular proof for this uses Dirichlet's theorem: For two co-prime positive integers a and b, there are infinitely many primes in the sequence $\{an + b\}_{n \geq 1}$. This theorem is very famous for being difficult to prove and it is well beyond our scope.

Now, let's compute a non-zero fraction modulo 7:

$$\begin{aligned}\frac{840}{77} = \frac{120}{11} &\equiv 120 \cdot (11)^{-1} \\ &\equiv 120 \cdot 2 \\ &\equiv 2 \pmod 7\end{aligned}$$

Theorem 2.9.1 (Wolstenholme's Theorem). *Let $p > 3$ be a prime. Then*

$$\begin{aligned}S &= \sum_{k=1}^{p-1} \frac{1}{k} \\ &= 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \\ &\equiv 0 \pmod{p^2}\end{aligned}$$

Note. According to our assumption, the sum $\sum_{k=1}^{p-1} 1/k$ has been written in lowest terms, that is, as a fraction a/b such that $(a, b) = 1$.

Remark. Theorem (2.9.1) is not the original theorem stated by Wolstenholme. Actually the theorem was as stated below.

Theorem 2.9.2. *If p is a prime bigger than 3, then*

$$\begin{aligned}\binom{2p}{p} &\equiv 2 \pmod{p^3} \\ \binom{2p-1}{p-1} &\equiv 1 \pmod{p^3}\end{aligned}$$

This theorem is equivalent to Theorem 2.9.1.

This seems to be a very interesting theorem, however the proof is not straightforward. Let us tackle this theorem step by step (these steps are really intuitive and very useful in olympiad problems). But first we will show a weaker version of the Theorem 2.9.2.

Theorem 2.9.3. *For any prime p,*

$$\binom{2p}{p} \equiv 2 \pmod{p^2}$$

Proof. We make use of an identity in Binomial Identities to write

$$\begin{aligned}\binom{2p}{p} &= \binom{p}{0}^2 + \binom{p}{1}^2 + \cdots + \binom{p}{p-1}^2 + \binom{p}{p}^2 \\ &= 2 + \binom{p}{1}^2 + \cdots + \binom{p}{p-1}^2 \\ &\equiv 2 \pmod{p^2}\end{aligned}$$

The last line is true because from Theorem 1.5.27, for $0 < i < p$, we have

$$\binom{p}{i} \equiv 0 \pmod{p}$$
$$\binom{p}{i}^2 \equiv 0 \pmod{p^2}$$

□

Lemma 2.9.4. *Let $p > 3$ be a prime and S be defined as in Theorem 2.9.1. Then,*

$$S \equiv 0 \pmod{p}$$

Proof. The proof is straightforward. There are $p-1$ terms in the sum and since $p > 3$ is an odd prime, the number of terms is even. So we can write S as sum of pairs of the form $\frac{1}{k} + \frac{1}{p-k}$, for $k = 1, 2, \dots, \frac{p-1}{2}$. Thus

$$\begin{aligned}
S &= 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \\
&= \left(1 + \frac{1}{p-1}\right) + \left(\frac{1}{2} + \frac{1}{p-2}\right) + \cdots + \left(\frac{1}{\frac{p-1}{2}} + \frac{1}{\frac{p-1}{2}+1}\right) \\
&= \sum_{k=1}^{\frac{p-1}{2}} \left(\frac{1}{k} + \frac{1}{p-k}\right) \\
&= \sum_{k=1}^{\frac{p-1}{2}} \frac{(k) + (p-k)}{k(p-k)} \\
&= \sum_{k=1}^{\frac{p-1}{2}} \frac{p}{k(p-k)} \\
&= p \cdot \sum_{k=1}^{\frac{p-1}{2}} \frac{1}{k(p-k)} \\
&\equiv 0 \pmod{p}
\end{aligned}$$

In the last line of above equations, the sum can be written as $\frac{a}{(p-1)!}$, where a is some integer. Note that $(p, (p-1)!) = 1$ and that's why we can conclude

$$p \cdot \sum_{k=1}^{\frac{p-1}{2}} \frac{1}{k(p-k)} \equiv 0 \pmod{p}$$

□

Lemma 2.9.5. *For a prime $p > 3$,*

$$(1^{-1})^2 + (2^{-1})^2 + \cdots + ((p-1)^{-1})^2 \equiv 0 \pmod{p}$$

where i^{-1} is the multiplicative inverse of i modulo p for $i = 1, 2, \dots, p-1$.

Proof. We recommend you re-read section (2.4.2) if you have forgotten the definition of multiplicative inverse. We already know that

$$1^2 + 2^2 + \cdots + (p-1)^2 = \frac{(p-1)(p)(2p-1)}{6}$$

Clearly, the sum is an integer. Therefore $(p-1)(p)(2p-1)$ is divisible by 6. Now since $p > 3$, we have $(p, 6) = 1$ and thus p divides $(p-1)(p)(2p-1)/6$. Therefore,

$$1^2 + 2^2 + \cdots + (p-1)^2 \equiv 0 \pmod{p}$$

In order to prove the lemma we should show that

$$(1^{-1})^2 + (2^{-1})^2 + \cdots + ((p-1)^{-1})^2 \equiv 1^2 + 2^2 + \cdots + (p-1)^2 \pmod{p}$$

We shall show that the sets $A = \{1, 2, \ldots, p-1\}$ and $B = \{1^{-1}, 2^{-1}, \ldots, (p-1)^{-1}\}$ are equal. A proof is as follows: from Theorem 2.4.9, for any $x \in A$, there exists some $y \in B$ such that $xy \equiv 1 \pmod{p}$. This y is unique, because if there exists some other $z \in B$ for which $xz \equiv 1 \pmod{p}$, then $xy \equiv xz \pmod{p}$, and since $(x, p) = 1$, we have $y \equiv z \pmod{p}$ which means $y = z$ (why?). So there exists a unique $y \in B$ for each $x \in A$, and thus $A = B$ since A and B have equal number of elements. Finally,

$$\begin{aligned}(1^{-1})^2 + (2^{-1})^2 + \cdots + ((p-1)^{-1})^2 &\equiv 1^2 + 2^2 + \cdots + (p-1)^2 \\ &\equiv 0 \pmod{p}\end{aligned}$$

□

We are going to re-state Proposition 2.4.13 because, as we already mentioned, it is very useful:

Lemma 2.9.6. *For a prime $p \geq 3$ and any positive integer a relatively prime to p,*

$$(a^{-1})^n \equiv (a^n)^{-1} \pmod{p}$$

for all positive integers n.

Proof.

$$\begin{aligned}a \cdot a^{-1} &\equiv 1 \pmod{p} \\ \implies a^n \cdot (a^{-1})^n &\equiv 1 \pmod{p} \\ \implies (a^{-1})^n &\equiv (a^n)^{-1} \pmod{p}\end{aligned}$$

□

Lemma 2.9.7. *For a prime $p > 3$,*

$$\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i(p-i)} \equiv 0 \pmod{p}$$

Proof. Let's write the sum as

$$\begin{aligned}\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i(p-i)} &= \sum_{i=1}^{\frac{p-1}{2}} \frac{\frac{(p-1)!}{i(p-i)}}{(p-1)!} \\ &= \frac{1}{(p-1)!} \cdot \sum_{i=1}^{\frac{p-1}{2}} \frac{(p-1)!}{i(p-i)}\end{aligned}$$

Since $(p-1)!$ is relatively prime to p, we only need to show that

$$\sum_{i=1}^{\frac{p-1}{2}} \frac{(p-1)!}{i(p-i)} \equiv 0 \pmod{p}$$

Define

$$a_i = \frac{(p-1)!}{i(p-i)}$$

for $i = 1, 2, \dots, \frac{p-1}{2}$. From Wilson's theorem, we know that $(p-1)! \equiv -1 \pmod{p}$. Observe that

$$i \cdot (p-i) \cdot a_i = (p-1)! \equiv -1 \pmod{p}$$

Replacing $p - i \equiv -i \pmod{p}$ in the above equation, we have

$$-i^2 \cdot a_i = -1 \pmod{p} \tag{2.9}$$

$$\implies i^2 \cdot a_i \equiv 1 \pmod{p} \tag{2.10}$$

Notice that the above equations are true for $i = 1, 2, \dots, (p-1)/2$. Now, (2.9) means that a_i is the multiplicative inverse of i^2 modulo p. So we have proved that

$$a_i = \frac{(p-1)!}{i(p-i)} \tag{2.11}$$

$$\equiv (i^2)^{-1} \pmod{p} \tag{2.12}$$

for $i = 1, 2, \dots, \frac{p-1}{2}$ where $(i^2)^{-1}$ means the multiplicative inverse of i^2 modulo p. We should now prove that the sum of all a_is is divisible by p. Let $a = \sum_{i=1}^{(p-1)/2} a_i$. According to (2.11),

$$\begin{aligned}a &= \sum_{i=1}^{\frac{p-1}{2}} a_i \\ &= \sum_{i=1}^{\frac{p-1}{2}} (i^2)^{-1}\end{aligned}$$

From Lemma 2.9.6, $(i^2)^{-1} \equiv (i^{-1})^2 \pmod{p}$, and so

$$a \equiv \sum_{i=1}^{\frac{p-1}{2}} (i^{-1})^2 \pmod{p} \tag{2.13}$$

We want to show that $a \equiv 0 \pmod{p}$. The trick is to convert (2.13) to what we proved in Lemma 2.9.5, using the fact that $-(a^{-1}) \equiv (-a)^{-1} \pmod{p}$:

$$\begin{aligned}
2a \equiv a + a &\equiv \sum_{i=1}^{\frac{p-1}{2}} (i^{-1})^2 + \sum_{i=1}^{\frac{p-1}{2}} (i^{-1})^2 \\
&\equiv \sum_{i=1}^{\frac{p-1}{2}} (i^{-1})^2 + \sum_{i=1}^{\frac{p-1}{2}} (-(i)^{-1})^2 \\
&\equiv \sum_{i=1}^{\frac{p-1}{2}} (i^{-1})^2 + \sum_{i=1}^{\frac{p-1}{2}} ((-i)^{-1})^2 \\
&\equiv \sum_{i=1}^{\frac{p-1}{2}} (i^{-1})^2 + \sum_{i=1}^{\frac{p-1}{2}} ((p-i)^{-1})^2 \\
&\equiv \sum_{i=1}^{\frac{p-1}{2}} (i^{-1})^2 + \sum_{i=\frac{p+1}{2}}^{p-1} (i^{-1})^2 \\
&\equiv \sum_{i=1}^{p-1} (i^{-1})^2 \\
&\equiv 0 \pmod{p}
\end{aligned}$$

Thus $a \equiv 0 \pmod{p}$ and we are done. □

We are ready to prove Wolstenholme's theorem now.

Proof of Wolstenholme's Theorem. According to Lemma 2.9.4, we can write S as

$$S = p \cdot \sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i(p-i)}$$

From Lemma 2.9.7, we know that the above sum is divisible by p, so S is divisible by p^2. □

Problem 2.9.8. Let $p \geq 5$ be a prime number, and

$$1 + \frac{1}{2} + \ldots + \frac{1}{p} = \frac{a}{b}$$

where a and b are two relatively prime integers. Show that $p^4 \mid ap - b$.

Solution. From Wolstenholme's theorem, we have

$$1+\frac{1}{2}+\cdots+\frac{1}{p-1}=p^2\cdot\frac{x}{y}$$

for some integers x and y such that $y\perp p$. Replacing this in the given equation,

$$\begin{aligned}p^2\cdot\frac{x}{y}+\frac{1}{p}&=\frac{a}{b}\\ ap-b&=p^3b\cdot\frac{x}{y}\end{aligned}$$

Since b is divisible by p, we have $p^4\mid ap-b$.

Problem 2.9.9. Let $p\geq 5$ be a prime and

$$\frac{1}{p-1}+\frac{2}{p-2}+\ldots+\frac{p-1}{1}=\frac{a}{b}$$

where a and b are two relatively prime integers. Show that $p^3\mid a-b+bp$.

Solution. Note that

$$\begin{aligned}\frac{a}{b}&=\sum_{i=1}^{p-1}\frac{p-i}{i}\\ &=\sum_{i=1}^{p-1}\left(\frac{p}{i}-1\right)\\ &=\sum_{i=1}^{p-1}\frac{p}{i}-(p-1)\\ &=p\cdot\left(\sum_{i=1}^{p-1}\frac{1}{i}\right)-(p-1)\\ &=p\cdot p^2\frac{x}{y}-(p-1)\end{aligned}$$

where x and y are relatively prime integers with $y\perp p$ (we have used Wolstenholme's theorem in the last line). Now,

$$\begin{aligned}\frac{a}{b}+p-1&=p\cdot\frac{p^2x}{y}\\ \implies (a-b+bp)y&=p^3xb\end{aligned}$$

and since $y\perp p$, we have $p^3\mid a-b+bp$.

Problem 2.9.10. For any prime p and a positive integer k such that $1\leq k\leq p-1$, prove that

$$\binom{p-1}{k}\equiv(-1)^k\pmod p$$

Solution. We use the fact that $p-i \equiv -i \pmod{p}$ and that $(i,p)=1$ for $0<i<p$.

$$\begin{aligned}\binom{p-1}{k} &= \frac{(p-1)(p-2)\cdots(p-1-k+1)}{1\times 2\times\cdots\times k}\\ &\equiv \frac{(-1)\times(-2)\times\cdots\times(-k)}{1\times 2\times\cdots\times k}\\ &\equiv \frac{(-1)^k\cdot 1\times 2\times\cdots\times k}{1\times 2\times\cdots\times k}\\ &\equiv (-1)^k \pmod{p}\end{aligned}$$

Problem 2.9.11. For an odd prime p, show that

$$\frac{2^p-2}{p} \equiv 1-\frac{1}{2}+\cdots-\frac{1}{p-1} \pmod{p}$$

Solution. The approach is not obvious here unless one knows the above theorem. In problems like this, it is usually hard to pin down how to approach the problem. However, one should of course try to make use of the fact that

$$\begin{aligned}2^p=(1+1)^p &= 1+\binom{p}{1}+\cdots+\binom{p}{p-1}+1\\ &= 1+\frac{p}{1}\binom{p-1}{0}+\cdots+\frac{p}{p-1}\binom{p-1}{p-2}+1\end{aligned}$$

So,

$$2^p-2 = p\left(\frac{1}{1}\binom{p-1}{0}+\frac{1}{2}\binom{p-1}{1}+\cdots+\frac{1}{p-1}\binom{p-1}{p-2}\right)$$

Now, the problem is in a suitable shape and we can use the theorem above to write

$$\begin{aligned}\frac{2^p-2}{p} &= \frac{1}{1}\binom{p-1}{0}+\frac{1}{2}\binom{p-1}{1}+\cdots+\frac{1}{p-1}\binom{p-1}{p-2}\\ &\equiv (-1)^0+\frac{1}{2}(-1)^1+\cdots+\frac{1}{p-1}(-1)^{p-3}\\ &\equiv 1-\frac{1}{2}+\cdots-\frac{1}{p-1} \pmod{p}\end{aligned}$$

Corollary 2.9.12. *For an odd prime p,*

$$\frac{2^{p-1}-1}{p} \equiv 1-\frac{1}{2}+\cdots-\frac{1}{p-2} \pmod{p}$$

Problem 2.9.13. Let $p\geq 5$ be a prime. Prove that

$$\binom{p^2}{p} \equiv p \pmod{p^5}$$

Solution. Notice that

$$\begin{aligned}\binom{p^2}{p} - p &= \frac{p^2(p^2-1)(p^2-2)\cdots(p^2-(p-1))}{p!} - p \\ &= \frac{p}{(p-1)!}\Big((p^2-1)(p^2-2)\cdots(p^2-(p-1)) - (p-1)!\Big)\end{aligned}$$

Since $(p,(p-1)!)=1$, it suffices to show that

$$(p^2-1)(p^2-2)\cdots(p^2-(p-1)) \equiv (p-1)! \pmod{p^4}$$

Expand the left side to obtain

$$(p^2-1)(p^2-2)\cdots(p^2-(p-1)) = (p-1)! + p^2\Big(1+\frac{1}{2}+\cdots+\frac{1}{p-1}\Big)(p-1)! + p^4\cdot x$$

where x is some integer. By Wolstenholme's theorem, the second term in the above expansion is divisible by p^4 and we are done.

Corollary 2.9.14. *Let $p \geq 5$ be a prime and $n \geq 1$ be an integer. Then*

$$\binom{p^{n+1}}{p} \equiv p^n \pmod{p^{2n+3}}$$

A result from Carlitz.[14]

Problem 2.9.15. Let k be a non-negative integer and $p \geq 5$ be a prime. Prove that

$$\frac{1}{kp+1} + \frac{1}{kp+2} + \ldots + \frac{1}{kp+(p-1)} \equiv 0 \pmod{p^2}$$

Hint. Use the following:

$$\sum_{i=1}^{p-1} \frac{1}{kp+i} = \frac{1}{2}\sum_{i=1}^{p-1}\Big(\frac{1}{kp+i} + \frac{1}{kp+p-i}\Big)$$

Problem 2.9.16. For a prime $p \geq 5$, show that

$$\binom{p^3}{p^2} \equiv \binom{p^2}{p} \pmod{p^8}$$

The following problem appears in Vandendriessche and Lee.[15]

Problem 2.9.17. Let p be an odd prime of the form $p = 4n+1$.

- Show that n is a quadratic residue $\pmod{p}$.

[14] L. Carlitz. "A Note on Wolstenholme's Theorem". In: *The American Mathematical Monthly* 61.3 (1954), pp. 174–176. DOI: 10.2307/2307217.

[15] Peter Vandendriessche and Hojoo Lee. "Problems in Elementary Number Theory (PEN)". in: (2007), p. D23.

- Calculate the value $n^n \pmod p$.

Problem 2.9.18. Let $p \geq 7$ be a prime and let s be a positive integer such that $p-1 \nmid s$. Prove that

$$1+\frac{1}{2^s}+\frac{1}{3^s}+...+\frac{1}{(p-1)^s} \equiv 0 \pmod p$$

Problem 2.9.19. Let n be a positive integer not divisible by 6. Also, let S be a reduced residue system modulo n such that $1 \leq a < n$ for all $a \in S$. Prove that

$$\sum_{a \in S}{}' \frac{1}{a} \equiv 0 \pmod{n^2}$$

§§2.10 Lucas' Theorem

In 2010, the following problem was posed in Bangladesh national mathematical Olympiad:

Problem 2.10.1. Find the number of odd binomial coefficients in the expansion of $(a+b)^{2010}$.

Here is a hint: you need to find the value of $\binom{2010}{i} \pmod 2$ for $0 \leq i \leq 2010$. One idea for doing that is to count the exponent of 2 in $\binom{2010}{i}$ using Legendre's theorem. Then look for the condition when a coefficient can be odd.

Here, we will focus on a generalized version of such problems. In problems like this, it happens that we need to find the remainder of division of the binomial coefficient $\binom{m}{n}$ by a prime number p. *Édouard Lucas* found patterns in Pascal triangle which resulted in the following theorem. Lucas[16] proved the following theorem as part of his investigation into the Lucas sequences of first kind and second kind.

Theorem 2.10.2 (Lucas's Theorem). *Let p be a prime and let m and n be non-negative integers. Then*

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \pmod p$$

where

$$m = m_k p^k + m_{k-1} p^{k-1} + \cdots + m_1 p + m_0$$
$$n = n_k p^k + n_{k-1} p^{k-1} + \cdots + n_1 p + n_0$$

are the base p expansions of m and n respectively. This uses the convention that $\binom{m}{n} = 0$ if $m < n$.

[16] Edouard Lucas. "Théorie des Fonctions Numériques Simplement Périodiques. [Continued]". In: *American Journal of Mathematics* 1.3 (1878), pp. 197–240. ISSN: 00029327, 10806377. URL: `http://www.jstor.org/stable/2369311`, Page 230, § XXI.

Example. For $p = 7, m = 67$, and $n = 10$. Now

$$\begin{aligned} 67 &= 1 \cdot 7^2 + 2 \cdot 7 + 4 \\ 10 &= 0 \cdot 7^2 + 1 \cdot 7 + 3 \end{aligned}$$

and therefore

$$\begin{aligned} \binom{67}{10} &\equiv \binom{1}{0}\binom{2}{1}\binom{4}{3} \\ &\equiv 1 \cdot 2 \cdot 4 \\ &\equiv 1 \pmod 7 \end{aligned}$$

Note that $\binom{67}{10} = 247,994,680,648 \equiv 1 \pmod 7$, which is a huge number and it would be tedious to find the remainder modulo 7 without Lucas's theorem.

In order to prove Lucas's theorem, we need to prove the following first.

Lemma 2.10.3. *For a prime p, an integer x, and a positive integer r, we have*

$$(1+x)^{p^r} \equiv 1 + x^{p^r} \pmod p$$

Proof. We will use induction on r to prove them lemma. The base case $r = 1$ is easy: for any integer k such that $1 \le k \le p-1$, we know that $\binom{p}{k} \equiv 0 \pmod p$. Now

$$\begin{aligned} (1+x)^p &\equiv 1 + \binom{p}{1}x + \binom{p}{2}x^2 + \cdots + \binom{p}{p-1}x^{p-1} + x^p \\ &\equiv 1 + x^p \pmod p \end{aligned}$$

Now suppose that $(1+x)^{p^r} \equiv 1 + x^{p^r} \pmod p$ is true for some integer $r \ge 1$. Then

$$\begin{aligned} (1+x)^{p^{r+1}} &\equiv \left((1+x)^{p^r}\right)^p \\ &\equiv \left(1 + x^{p^r}\right)^p \\ &\equiv \binom{p}{0} + \binom{p}{1}x^{p^r} + \binom{p}{2}x^{2p^r} + \cdots + \binom{p}{p-1}x^{(p-1)p^r} + \binom{p}{p}x^{p^{r+1}} \\ &\equiv 1 + x^{p^{r+1}} \pmod p \end{aligned}$$

So the congruence relation holds for all $r \ge 1$. □

Proof of Lucas's Theorem. The idea is to find the coefficient of x^n in the expansion of $(1+x)^m$. We have

$$\begin{aligned} (1+x)^m &= (1+x)^{m_k p^k + m_{k-1}p^{k-1} + \cdots + m_1 p + m_0} \\ &= [(1+x)^{p^k}]^{m_k}[(1+x)^{p^{k-1}}]^{m_{k-1}} \cdots [(1+x)^p]^{m_1}(1+x)^{m_0} \\ &\equiv (1+x^{p^k})^{m_k}(1+x^{p^{k-1}})^{m_{k-1}} \cdots (1+x^p)^{m_1}(1+x)^{m_0} \pmod p \end{aligned}$$

We want the coefficient of x^n in $(1+x)^m$. Since $n = n_k p^k + n_{k-1}p^{k-1} + \cdots + n_1 p + n_0$, we want the coefficient of $(x^{p^k})^{n_k}(x^{p^{k-1}})^{n_{k-1}} \cdots (x^p)^{n_1}x^{n_0}$. The coefficient of each $(x^{p^i})^{n_i}$

comes from the binomial expansion of $(1+x^{p^i})^{m_i}$, which is $\binom{m_i}{n_i}$. Therefore we take the product of all such $\binom{m_i}{n_i}$, and thus we have

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \pmod{p}$$

□

Corollary 2.10.4. *The binomial coefficient $\binom{n}{k}$ is divisible by p if and only if at least one of the digits of k in base p is greater than the corresponding digit n in base p.*

Corollary 2.10.5. *Let s,t,q,r be non-negative integers and p p be a prime such that $0 \leq q,r \leq p-1$. Then*

$$\binom{sp+q}{tp+r} \equiv \binom{s}{t}\binom{q}{r} \pmod{p}$$

Problem 2.10.6. How many ordered triples (a,b,c) of positive integers satisfy $a+b+c = 94$ and 3 does not divide

$$\frac{94!}{a!b!c!}?$$

Solution. Write $c = 94-a-b$, and hence

$$\frac{94!}{a!b!(94-a-b)!} = \binom{94}{a} \cdot \binom{94-a}{b}$$

By Lucas' theorem, since $94 = (10111)_3$, 3 does not divide $\binom{94}{a}$ only when a is an element of the set

$$S = \{1,3,4,9,10,12,13,81,82,84,85,90,91,93,94\}$$

By symmetry, we only need to find a,b,c which are elements of S. There exist six such triples (a,b,c) which sum to 94:

$$(1,3,90),(1,9,84),(1,12,81),(3,9,82),(3,10,81),(4,9,81)$$

Problem 2.10.7. Let p be a prime. Prove that

$$\binom{p^n-1}{k} \equiv (-1)^{s_p(k)} \pmod{p}$$

where $s_p(k)$ is the sum of digits of k when represented in base p.

Hint. Use Problem 2.9.10 and apply Lucas' theorem.

Problem 2.10.8. Let p and q be distinct odd primes. Prove that

$$\binom{2pq-1}{pq-1} \equiv 1 \pmod{pq}$$

if and only if

$$\binom{2p-1}{p-1} \equiv 1 \pmod{q}$$
$$\binom{2q-1}{q-1} \equiv 1 \pmod{p}$$

Solution. Since $2pq-1 = (2q-1)p + p - 1$, the rightmost digit of $2pq-1$ when represented in base p is $p-1$ and the other digits form $2q-1$. Analogously, the rightmost digit of $pq-1$ when represented in base p is $p-1$ and the other digits form $q-1$. Applying corollary (2.10.5), we find

$$\binom{2pq-1}{pq-1} \equiv \binom{2q-1}{q-1}\binom{p-1}{p-1} \tag{2.14}$$

$$\equiv \binom{2q-1}{q-1} \pmod{p} \tag{2.15}$$

The if part is obvious since p and q are different primes. We will prove the only if part now.

Suppose that $\binom{2pq-1}{pq-1} \equiv 1 \pmod{pq}$. This means that $\binom{2pq-1}{pq-1} \equiv 1 \pmod{p}$. By equation (2.15), $\binom{2q-1}{q-1} \equiv 1 \pmod{p}$ as desired. Proving $\binom{2p-1}{p-1} \equiv 1 \pmod{q}$ is similar.

Problem 2.10.9. Let n and k be arbitrary positive integers and let p be an odd prime p. Prove that

$$p^2 \mid \binom{pk}{pm} - \binom{k}{m}$$

Hint. Induct on n and equate the coefficients of $a^{pm}b^{p(n-m)}$ in both sides of

$$(a+b)^{pn} = (a+b)^{p(n-1)}(a+b)^p$$

§§2.11 Lagrange's Theorem

Lagrange's theorem in polynomial congruence is a really influential result in number theory. It has many implications and applications. And it is so important that we decided to keep it in this book even though we are not discussing polynomials or polynomial congruence in the current book. We just need the following simple definition.

Definition. A polynomial is an expression consisting of variables and coefficients which only employs the operations of addition, subtraction, multiplication, and non-negative integer exponents.

Example. An example of a polynomial of a single variable x and with integer coefficients is $P(x) = x^4 + 3x^2 + x - 8$. An example in three variables and rational coefficients is

$$P(x,y,z) = 2x^3 + \frac{4}{5}xy - 7xyz + 3zy^2 - 6$$

Note. We only work with polynomials of a single variable and with integer coefficients in this book.

Definition. Consider a polynomial $P(x)$ with integer coefficients. The *degree* of $P(x)$ is the largest exponent of x in $P(x)$. That is, if

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

where a_i, $0 \leq i \leq n$ are integers and $a_n \neq 0$, then the degree of $P(x)$ is n. We show this by $\deg P(x) = n$.

Definition. Let

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

be a polynomial with integer coefficients. Assume that at least one coefficient of $P(x)$ is not divisible by p. For any prime p, the degree of $P(x)$ modulo p is the largest integer k, $0 \leq k \leq n$, for which $p \nmid a_k$. We denote this by $\deg_p P(x) = k$.

Example. The degree of $P(x) = 7x^4 + 14x^3 - 5x^2 + 5x + 3$ is 4. However, the degree of $P(x)$ is 2 modulo 7.

Theorem 2.11.1 (Lagrange's Theorem). *Let p be a prime and let $P(x)$ be a polynomial with integer coefficients not all divisible by p. Also, let $\deg_p P(x) = k$. The congruence equation $P(x) \equiv 0 \pmod{p}$ has at most k incongruent solutions modulo p.*

Note. Assume that

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

If $P(x) \equiv 0 \pmod{p}$ for some x, then since

$$\begin{aligned}(x + kp)^i &\equiv x^i + (kp)^i \\ &\equiv x^i \pmod{p}\end{aligned}$$

$\forall i, k \in \mathbb{N}$, we have $P(x + kp) \equiv 0 \pmod{p}$ as well. This means that we only need to search for solutions in the set $\{0, 1, \ldots, p-1\}$. The term *incongruent solutions* in the above theorem is there just for the same reason.

Example. Let $P(x) = 10x^3 + 3x^2 + 12x + 17$. The degree of $P(x)$ modulo 5 is 2. According to Lagrange's theorem, the equation $P(x) \equiv 0 \pmod{5}$ has at most 2 solutions modulo 5. To check this, note that

$$\begin{aligned}P(x) &= 10x^3 + 3x^2 + 12x + 17 \\ &\equiv 3x^2 + 12x + 12 \\ &\equiv 3(x+2)^2 \\ &\equiv 0 \pmod{5}\end{aligned}$$

has only one solution $x \equiv -2$ modulo 5.

We will prove Lagrange's theorem in the following.

Proof. We induct on k. Since $\deg_p P(x) = k$, we can write

$$P(x) \equiv a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$$

where $a_k, a_{k-1}, \ldots, a_0$ are coefficients of $P(x)$. It is clear that for $k = 0$, the equation $f(x) = a_0$ has no solutions modulo p because $p \nmid a_0$. Assume that the claim is true for all polynomials of degree up to $k-1$ modulo p. Assume that $P(x) \equiv 0 \pmod{p}$ has d solutions. If $d < k$, we are done. Otherwise, if $d \geq k$, take $x_1, x_2, \ldots, x_k$ to be k arbitrary incongruent solutions of $P(x) \equiv 0 \pmod{p}$. Define

$$Q(x) = P(x) - a_k(x - x_1)(x - x_2)\cdots(x - x_k)$$

Clearly, $\deg_p Q(x) < \deg_p P(x) = k$. However,

$$\begin{aligned} Q(x_1) &\equiv Q(x_2) \\ &\equiv \cdots \\ &\equiv Q(x_k) \\ &\equiv 0 \pmod{p} \end{aligned}$$

which means $Q(x) \equiv 0 \pmod{p}$ has at least k solutions. The induction hypothesis forces that $Q(x) \equiv 0 \pmod{p}$ for all x. It follows that

$$P(x) \equiv a_k(x - x_1)(x - x_2)\cdots(x - x_k) \pmod{p}$$

This means that $P(x) \equiv 0 \pmod{p}$ if and only if $x - x_i \equiv 0 \pmod{p}$ for some $i \in \{1, 2, \ldots, k\}$. So, $x_1, x_2, \ldots, x_k$ are the only solutions to $P(x) \equiv 0 \pmod{p}$. The induction is complete. □

In this section, we will discuss only the following result and see how to apply it to prove some other theorems.

Theorem 2.11.2 (Lagrange). *If p is a prime and*

$$(x+1)(x+2)\cdots(x+p-1) = x^{p-1} + a_1 x^{p-2} + \cdots + a_{p-2}x + (p-1)! \tag{2.16}$$

then the coefficients $a_1, a_2, \ldots, a_{p-2}$ are divisible by p where p is an odd prime.

The term x^{p-1} is produced by multiplying all x terms. Multiplying all the constant terms, we get $1 \cdot 2 \cdots (p-1) = (p-1)!$, which explains the reasoning behind the terms on the right side of the equation. The proof is an intuitive one. Though there maybe other proofs, we prefer this one.

Proof. Assume that $f(x) = (x+1)(x+2)\cdots(x+p-1)$. We start by noticing that $f(x+1) = (x+2)(x+3)\cdots(x+p)$. We can write

$$(x+p)f(x) = (x+1)f(x+1)$$

or equivalently,

$$pf(x) = (x+1)f(x+1) - xf(x) \tag{2.17}$$

Substituting the expressions for $f(x)$ and $f(x+1)$ in equation (2.16), we see that

$$\begin{aligned} pf(x) &= px^{p-1} + pa_1x^{p-2} + \cdots + pa_{p-2}x + p! \\ (x+1)f(x+1) &= (x+1)^p + a_1(x+1)^{p-1} \\ &\quad + \cdots + a_{p-2}(x+1)^2 + (x+1)(p-1)! \\ xf(x) &= x^p + a_1x^{p-1} + \cdots + a_{p-2}x^2 + x(p-1)! \end{aligned}$$

Replace these values into (2.17),

$$\begin{aligned} (x+1)f(x+1) - xf(x) &= (x+1)^p - x^p + a_1((x+1)^{p-1} - x^{p-1}) \\ &\quad + \cdots + a_{p-2}((x+1)^2 - x^2) + (x+1-x)(p-1)! \end{aligned} \tag{2.18}$$

We need to expand the terms $(x+1)^i - x^i$ (for $1 \leq i \leq p$) using binomial theorem so we can collect the terms with same degree (exponent).

$$\begin{aligned} (x+1)^i - x^i &= \left(x^i + \binom{i}{1}x^{i-1} + \binom{i}{2}x^{i-2} + \cdots + \binom{i}{i-1}x + 1\right) - x^i \\ &= \binom{i}{1}x^{i-1} + \binom{i}{2}x^{i-2} + \cdots + \binom{i}{i-1}x + 1 \end{aligned} \tag{2.19}$$

Since $pf(x) = (x+1)f(x+1) - xf(x)$, the coefficients of same exponents of x should be the same for both sides. The coefficient of x^{p-2} in $pf(x)$ is pa_1, while that of $(x+1)f(x+1) - xf(x)$ comes from the first two terms of (2.18) (that is, $(x+1)^p - x^p$ and $a_1((x+1)^{p-1} - x^{p-1})$). Using (2.19) to calculate these two terms, we get

$$pa_1 = \binom{p}{2} + \binom{p-1}{1}a_1$$

From Theorem 1.5.27, we know that p divides $\binom{p}{k}$ for any $0 < k < p$. So, p divides $\binom{p}{2}$, therefore p divides a_1.

Equating coefficient of x^{p-3}, we find

$$pa_2 = \binom{p}{3} + \binom{p-1}{2}a_1 + \binom{p-2}{1}a_2$$

Here, p divides $\binom{p}{3}$ and a_1, so p divides a_2. Continuing this process in a similar way, we find that $a_1, a_2, \ldots, a_{p-2}$ are divisible by p. To check correctness of this, we can equate the coefficient of x and find

$$pa_{p-2} = \binom{p}{p-1} + \binom{p-1}{p-2}a_1 + \cdots + \binom{2}{1}a_{p-2}$$

This equation implies p divides a_{p-2}, as claimed. The proof is complete. □

Before we describe some applications, let's try to understand the coefficients $a_1, a_2, \ldots, a_{p-2}$ in a better way. By investigating (2.16), one can easily obtain

$$\begin{aligned} a_1 &= 1 + 2 + \cdots + p - 1 \\ a_2 &= 1 \cdot 2 + \cdots + 1 \cdot (p-1) + 2 \cdot 3 + \cdots + 2 \cdot (p-1) + \cdots \\ &\vdots \end{aligned}$$

You should already guess what $a_1, \dots, a_{p-2}$ are. a_1 is the sum of all $1, \cdots, p-1$. a_2 is the sum of products of two numbers from $1, \cdots, p-1$ (all possible $\binom{p-1}{2}$ combinations). Similarly, a_{p-2} is the sum of products of $p-2$ numbers taken at a time. In general a_i the sum of all possible products of i numbers taken from $1, 2, \cdots, p-1$. Therefore, we can state Theorem 2.11.2 as

Theorem 2.11.3. *If p is an odd prime and $0 < k < p-1$, then the sum of all possible products of k numbers taken at a time from $1, 2, \dots, p-1$ is divisible by p.*

Let's see just how powerful this theorem can be, if used properly. We can take advantage of the fact that the theorem is actually an identity, so we can choose x freely as we wish.

Proof of Wilson's Theorem. The theorem is true when $p = 2$. Therefore, it is safe to assume that p is odd. Put $x = 1$ in Theorem 2.11.2 to obtain

$$2 \times 3 \times \cdots \times p = 1 + (a_1 + \cdots + a_{p-2}) + (p-1)!$$

and so,

$$p! = 1 + a_1 + \cdots + a_{p-2} + (p-1)!$$

Clearly, $p!$ is divisible by p, and so are $a_1, \cdots, a_{p-2}$. Thus, $1 + (p-1)!$ must be divisible by p too, which is exactly what we want. □

We will use this as an intermediary to prove Fermat's theorem. We want to prove $x^{p-1} - 1$ is divisible by p when $x \perp p$.

Proof of Fermat's Theorem. Since x is co-prime to p, one of $x+1, \cdots, x+p-1$ is divisible by p because they are $p-1$ consecutive integers. Therefore, their product is divisible by p too. Thus,

$$(x+1)\cdots(x+p-1) = x^{p-1} + a_1 x^{p-2} + \cdots + a_{p-2}x + (p-1)!$$

Here, left side is divisible by p so must be right side. Again, since $a_1, \dots, a_{p-2}$ are multiples of p, we have $x^{p-1} + (p-1)!$ is a multiple of p.

$$x^{p-1} \equiv -(p-1)! \pmod{p}$$

Hence, by Wilson's theorem, $x^{p-1} \equiv 1 \pmod{p}$, which finishes the proof. □

As for the last demonstration, we will use it to prove Wolstenholme's theorem, which we also proved before. The theorem requires us to show that for $p > 3$ a prime, the numerator of

$$1 + \frac{1}{2} + \cdots + \frac{1}{p-1}$$

is divisible by p^2 in its reduced form.

Proof of Wolstenholme's Theorem. The numerator is the sum of products of $p-2$ numbers taken from $1, 2, \dots, p-1$. So, it is a_{p-2}. Since the denominator of the fraction is $(p-1)!$, which is not divisible by p, we only need to show that $p^2 \mid a_{p-2}$.

Set $x = -p$ in Theorem 2.11.2 to obtain

$$(-p+1)\cdots(-p+p-1) = p^{p-1} - a_1 p^{p-2} + \cdots - a_{p-2}p + (p-1)!$$

The left hand side of the above equation equals $(p-1)!$. So

$$p^{p-1} - a_1 p^{p-2} + \cdots - a_{p-2}p = 0$$

which gives

$$a_{p-2} = p^{p-2} + a_1 p^{p-3} + \cdots + a_{p-3}p^2$$

If $p > 3$, then $p - 2 \geq 2$ and all the terms on the right side are divisible by p^2. □

Note. You should try to guess what motivates us to set exactly those values of x to get nice results.

§§2.12 Order, Primitive Roots

Recall the examples we took while discussing Fermat's little theorem. We were working with something like $2^6 \pmod 7$ or $6^6 \pmod 7$. While calculating, we found that $6^2 \equiv 1 \pmod 7$ or $2^3 \equiv 1 \pmod 7$ which eventually led to $6^6 \equiv 1 \pmod 7$ and $2^6 \pmod 7$. Along with the ideas we used there, did you conjecture anything else? We left a hint when we said that since $6^2 \equiv 1 \pmod 7$, $6^4 \equiv 1 \pmod 7$ and $6^6 \equiv 1 \pmod 7$ as well. We hope that this is sort of obvious by now. But it should also trigger you to think of something. If we can find the smallest exponent for which $2^x \equiv 1 \pmod 7$, then we can say $2^y \equiv 1 \pmod 7$ for all multiples of x (y here). We will shortly prove this formally. Moreover, it also encourages us to study these *smallest* values for which we get 1. The motivation is obvious. Whenever we get 1, we get a cycle of remainders from which point, the remainders repeat. Just finish the examples above if you did not entirely understand what we meant. We call this smallest integer order. And it should be clear to you why the study of order is important.

Order Modulo Integers. Let a and n be co-prime positive integers. If x is the smallest positive integer such that

$$a^x \equiv 1 \pmod n$$

then x is called the *order* of a modulo n. We denote this by $\operatorname{ord}_n(a) = x$.

Example. $\operatorname{ord}_8(3) = 2$ i.e. 2 is the smallest positive integer such that $3^2 \equiv 1 \pmod 8$.

Theorem 2.12.1. *Let a and n be positive integers. If $\operatorname{ord}_n(a) = d$ and $a^x \equiv 1 \pmod n$, then $d \mid x$.*

Proof. If $x < d$, it would contradict the fact that, d is such smallest positive integer that $a^d \equiv 1 \pmod{n}$. We are left with the case $x > d$. Assume that $x = dq + r$ with $0 \leq r < d$.

$$\begin{aligned} a^x &\equiv a^{dq} \cdot a^r \pmod{n} \\ &\equiv (a^d)^q \cdot a^r \pmod{n} \\ &\equiv 1 \cdot a^r \pmod{n} \\ &\equiv a^r \pmod{n} \end{aligned}$$

So $a^r \equiv a^x \equiv 1 \pmod{n}$. Since $0 \leq r < d$ and d is the order of a, this is impossible unless $r = 0$. Thus $x = dq$ and we are done. □

Corollary 2.12.2. *If $a \perp n$, then $\operatorname{ord}_n(a) \mid \varphi(n)$.*

Proof. If $d = \operatorname{ord}_n(a)$, then $a^d \equiv 1 \pmod{n}$. From Euler's theorem, $a^{\varphi(n)} \equiv 1 \pmod{n}$. Then using Theorem 2.12.1, we can say that $d \mid \varphi(n)$. □

We can use this result to find orders in practice. We only need to check for divisors of $\varphi(n)$ and find the smallest divisor for which the relation $a^d \equiv 1 \pmod{n}$ holds.

Corollary 2.12.3. *$a^k \equiv a^l \pmod{n}$ if and only if $k \equiv l \pmod{\operatorname{ord}_n(a)}$.*

Proof. $a^k \equiv a^l \pmod{n}$ implies $a^{k-l} \equiv 1 \pmod{n}$. By Theorem 2.12.1, we have $\operatorname{ord}_n(a) \mid k - l$. The reverse of this approach can be applied to prove the other part of the corollary. □

One could ask if we know the order of a modulo n, how do we find the order of other powers of a. Or, if we know order of a modulo two positive integers m and n, then what would be the order of a modulo mn?

Theorem 2.12.4. *If m and n are relatively prime positive integers such that $\operatorname{ord}_m(a) = d$ and $\operatorname{ord}_n(a) = e$, then $\operatorname{ord}_{mn}(a) = [d, e]$.*

Proof. Let $\operatorname{ord}_{mn}(a) = h$, so

$$a^h \equiv 1 \pmod{mn}$$

which gives $a^h \equiv 1 \pmod{m}$ and $a^h \equiv 1 \pmod{n}$ as well. By Theorem 2.12.1, since d and e are order of a modulo m and n, respectively, we have $d \mid h$ and $e \mid h$. Therefore, for the minimum h, we must have $h = [d, e]$ to satisfy the conditions. □

Theorem 2.12.5. *Let a, b, and n be positive integers such that $\operatorname{ord}_n(a) = k$ and $\operatorname{ord}_n(b) = l$, where $k \perp l$. Then $\operatorname{ord}_n(ab) = kl$.*

Proof. Let $\operatorname{ord}_n(ab) = h$. First, note that

$$\begin{aligned} a^{lh} &\equiv a^{lh} \cdot b^{lh} \pmod{n} \\ &\equiv (ab)^{lh} \pmod{n} \\ &\equiv \left((ab)^h\right)^l \pmod{n} \\ &\equiv 1 \pmod{n} \end{aligned}$$

So, by Theorem 2.12.1, we have $k \mid lh$ and since $(k,l) = 1$, it follows that $k \mid h$. We can similarly prove that $l \mid h$. So $kl \mid h$. On the other hand,

$$\begin{aligned}(ab)^{kl} &\equiv (a^k)^l \cdot (b^l)^k \pmod{n} \\ &\equiv 1 \pmod{n}\end{aligned}$$

Again, by Theorem (2.12.1), we have $h \mid kl$. This finishes the proof. □

Theorem 2.12.6. *If the order of a modulo n is d, then the order of a^k modulo n is $d/(d,k)$.*

Proof. Let the order of a^k modulo n be h. Then $\left(a^k\right)^h \equiv a^{kh} \equiv 1 \pmod{n}$. Theorem 2.12.1 says that d must divide kh. Assume that $(k,d) = g$, so there exist relatively prime positive integers l and e such that $k = gl$ and $d = ge$. Rewriting $d \mid kh$ implies

$$ge \mid glh \implies e \mid lh$$

and since $l \perp e$, e must divide h. Since $dl = ke = gel$,

$$\begin{aligned}\left(a^k\right)^e &\equiv \left(a^d\right)^l \\ &\equiv 1 \pmod{n}\end{aligned}$$

This means that the order of a^k modulo n must divide e. So, h divides e as well. We get that

$$h = e = \frac{d}{(d,k)}$$

must hold. □

The previous theorem also implies the following one.

Theorem 2.12.7. *The order of a modulo n is the same as the order of a^k modulo n if and only if $(k,n) = 1$.*

Here is a very useful theorem, often used to solve Diophantine equations.

Theorem 2.12.8. *Let q be a prime and x be a positive integer. Every prime divisor of the number*

$$1 + x + \cdots + x^{q-1}$$

is either q or congruent to 1 modulo q.

Proof. The sum can be written as

$$S = 1 + x + \cdots + x^{q-1} = \frac{x^q - 1}{x - 1}$$

Let p be any prime factor of S. Then

$$x^q \equiv 1 \pmod{p}$$

If the order of x modulo p is d, we have $d \mid q$. Since q is a prime, either $d = 1$ or $d = q$. If $d = 1$, then $x \equiv 1 \pmod{p}$. In that case,

$$S \equiv 1 + 1 + \cdots + 1 \pmod{p}$$

which gives $0 \equiv q \pmod{p}$. So, $p = q$. Now assume the case that $d = q$. Because of Fermat's little theorem,

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

This implies that $d = q$ divides $p - 1$. So $p \equiv 1 \pmod{q}$, as claimed. □

Primitive Root. Let n be a given positive integer. An integer g which is relatively prime to n is called a *primitive root* modulo n if $\text{ord}_n(g) = \varphi(n)$. That is, if $g^x \not\equiv 1 \pmod{n}$ for any positive integer $x < \varphi(n)$.

Note. Using this definition, we can say that:

1. Let g be a positive integer relatively prime to n. It is clear that g^m is also co-prime to n for any $m \in \mathbb{N}$.
2. If g is a primitive root modulo n and if $g^a \equiv g^b \pmod{n}$ for some positive integers a and b less than $\varphi(n)$, then $a = b$. The reason is simple: if $a \neq b$, then $g^{a-b} \equiv 1 \pmod{n}$, which is absurd since $a - b \leq \varphi(n)$ and g is a primitive root.

These two notes tell us that if g is a primitive root of n, then the set $\{g, g^2, \cdots, g^{\varphi(n)}\}$ is equal to $\mathbb{U}_n$, where $\mathbb{U}_n$ is the set of units modulo n (as defined in Definition 2.3.0.2). Notice that equality of these two sets is considered modulo n. Actually, the set $\{g, g^2, \cdots, g^{\varphi(n)}\}$ may contain some elements larger than n. We reduce those elements modulo n so that we have all elements less than n. This new set is now equal to $\mathbb{U}_n$. We may denote this by the notation $\{g, g^2, \cdots, g^{\varphi(n)}\} \equiv \mathbb{U}_n \pmod{n}$.

In algebraic words, g is a *generator* of $\mathbb{U}_n$. Moreover, the generators of $\mathbb{U}_n$ are exactly the primitive roots of n (if there is any). We will summarize this result in the following theorem.

Theorem 2.12.9. *A primitive root g modulo n (if existing) is a generator of $\mathbb{U}_n$. That is, for any $a \in \mathbb{U}$, there is a unique k with $0 < k \leq \varphi(n)$ such that $g^k \equiv a \pmod{n}$.*

Proof. Consider the powers $g, g^2, \ldots, g^{\varphi(n)}$ modulo n. Now assume $g^u \equiv g^v \pmod{n}$ for some $u, v \in \{1, 2, \ldots, \varphi(n)\}$, then since $(g, n) = 1$, we obtain

$$g^{u-v} \equiv 1 \pmod{n}$$

This is not possible unless $u = v$. The reason is simple: if $u \neq v$, then we have found some $x = u - v$ such that $0 < x \leq \varphi(n)$ and $g^x \equiv 1 \pmod{n}$, which is in contradiction with g being a primitive root modulo n. □

Example.

1. 3 is a primitive root modulo 7 since $\varphi(7) = 6$ and $3^i \not\equiv 1 \pmod 7$ for $i \in \{1, 2, 3, 4, 5\}$. Notice that powers of 3 create the whole set $\mathbb{U}_7$:

$$3^1 \equiv 3, \quad 3^2 \equiv 2, \quad 3^3 \equiv 6, 3^4 \equiv 4, \quad 3^5 \equiv 5, \quad 3^6 \equiv 1$$

where all the congruences are taken modulo 7.

2. Let's see if there exists a primitive root modulo 15. To show this, a possible way is to start from $a = 2$ and compute all the powers a^i for $i = 2, \dots, \varphi(15) - 1 = 7$ modulo 15 one by one:

$$2^2 \equiv 4, \quad 2^3 \equiv 8, \quad 2^4 \equiv 1$$

We stop at 2^4 because we got 1 mod 15, and this shows that 2 is not a primitive root modulo 15. Then, we should do the same process, but this time for $a = 4$ (we don't check 3 because it's not relatively prime to 15). Now you should be able to do the math much faster, and come up with $4^2 \equiv 1 \pmod{15}$, which shows $a = 4$ is not a primitive root modulo 15. Fortunately, we don't need to check $a = 5$ and $a = 6$. For $a = 7$, the computations are not as easy as $a = 2$ and $a = 4$, but still not hard

$$7^2 \equiv 4, \quad 7^3 \equiv 13, \quad 7^4 \equiv 1$$

So, 7 is not a primitive root mod 15 either. Now, we don't need to do the computations for $a = 8$ because in this case, a^{-1} is 2 and we showed that 2 is not a primitive root (why is that enough?). The next values for a to check are 11, 13, and 14. Since $13 = 7^{-1}$, we don't need to worry about 13. Check 11 and 14 for yourself and verify that neither of them are primitive roots mod 15 (we can't do the modular arithmetic invers trick here because 11 and 14 are the inverse of themselves modulo 15). This shows that there is no primitive root mod 15.

3. Let's assume that elements g_i of $\mathbb{U}_n$ are sorted in ascending order. That is, $g_1 < \cdots < g_{\varphi(n)}$. Then we have $g_1 = 1$ and $g_{\varphi(n)} = n - 1$.

Corollary 2.12.10. *If g is a primitive root of p then*

$$\mathbb{G} = \{g^1, g^2, \dots, g^{p-1}\}$$

forms a complete residue system modulo p.

Theorem 2.12.11. *Let n be a positive integer and let a be a quadratic non-residue modulo n such that $a \perp n$. Assume that $\mathbb{U}_n = \{g_1, g_2, \dots, g_{\varphi(n)}\}$. Then*

$$g_1 g_2 \cdots g_{\varphi(n)} \equiv a^{\frac{\varphi(n)}{2}} \pmod n$$

Proof. According to Theorem 2.4.6, for any g_i, there exists some x such that

$$g_i x \equiv a \pmod n \tag{2.20}$$

It is clear that $x \perp n$ because if $(x, n) = d$, then $d \mid n$ and $n \mid g_i x - a$, so $d \mid g_i x - a$ implies $d \mid a$. Since $\gcd(a, d) = 1$, we have $d = 1$. So $x = g_j$ for some j. We have $g_i \neq g_j$ since a is a quadratic non-residue. Moreover, g_j is unique because if $g_i g_k \equiv a \pmod{n}$ for some k, then $g_k \equiv g_j \pmod{n}$ and since g_k and g_j are both less than n, this forces $g_k = g_j$. Thus, we can pair up the $\varphi(n)$ elements of $\mathbb{U}_n$ into $\varphi(n)/2$ pairs (g_i, g_j), such that $g_i g_j \equiv a \pmod{n}$. Hence,

$$g_1 g_2 \cdots g_{\varphi(n)} \equiv a^{\frac{\varphi(n)}{2}} \pmod{n}$$

□

Here is a nice theorem which relates primitive roots and quadratic residues modulo a prime p.

Theorem 2.12.12. *If g is a primitive root modulo a prime p, then the quadratic residues of p are $g^2, g^4, \ldots, g^{p-1}$.*

Proof. By Euler's criterion, we know that if a is a quadratic residue modulo p, then

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Using Fermat's little theorem, it follows that $g^2, g^4, \ldots, g^{p-1}$ are all quadratic residues modulo p. Since the set $\{g^1, g^2, \ldots, g^{p-1}\}$ is a complete residue set modulo p and we know by Theorem 2.8.2 that there are exactly $\frac{p-1}{2}$ incongruent quadratic residues modulo p, we find that $g^2, g^4, \ldots, g^{p-1}$ are the only quadratic residues. □

It is a natural question whether there exists a primitive root g modulo an arbitrary positive integer n. If the answer is negative, one might ask for which n there exists a primitive root. We will answer these questions shortly.

Theorem 2.12.13. *A positive integer g is a primitive root modulo n if and only if*

$$g^{\frac{\varphi(n)}{p}} \not\equiv 1 \pmod{n}$$

for any prime p which divides $\varphi(n)$.

Proof. It is straightforward to check the truth of the "if" part. For the sake of contradiction, assume $\varphi(n) = pk$ and

$$g^k \equiv 1 \pmod{n}.$$

But this would contradict the minimality of $\varphi(n)$ since k is less than $\varphi(n)$, meaning that g is not a primitive root.

For the "only if" part, assume that for every prime divisor p of $\varphi(n)$, we have

$$g^{\frac{\varphi(n)}{p}} \not\equiv 1 \pmod{n}$$

We want to show that g is a primitive root modulo n. Let $d = \text{ord}_n(g)$, so that $d \mid \varphi(n)$. If $d < \varphi(n)$, then we must have $d \mid \varphi(n)/p$ for some prime p dividing $\varphi(n)$. Letting $\varphi(n) = pdl$,

$$\begin{aligned} g^{\frac{\varphi(n)}{p}} &\equiv g^{dl} \pmod{n} \\ &\equiv \left(g^d\right)^l \pmod{n} \\ &\equiv 1 \pmod{n} \end{aligned}$$

which is a contradiction. Hence, $d = \varphi(n)$ must hold. □

Note. In the proof above, we could just take p to be the smallest prime divisor of $\varphi(n)$. Then we must have that d is a divisor of $\varphi(n)/p$. This is because the greatest divisor of n less than n is n/p, where p is the smallest prime divisor of n (can you sense why?).

Corollary 2.12.14. *Let m be a positive integer. If g is a primitive root of n, then g^m is also a primitive root modulo n if and only if $m \perp \varphi(m)$.*

Proof. Let $(m, \varphi(n)) = d$, so that $m\varphi(n) = d \cdot [m, \varphi(n)]$. According to Theorem 2.12.13, g^m is a primitive root modulo n if and only if

$$g^{d\cdot[m,\varphi(n)]/p} \not\equiv 1 \pmod{n} \tag{2.21}$$

for all prime divisors p of $\varphi(n)$. Now, if $d \neq 1$, there exists a prime q which divides d. In that case, write $d = qk$ for some integer k. But then,

$$g^{d\cdot[m,\varphi(n)]/q} \equiv g^{k\cdot[m,\varphi(n)]} \pmod{n}$$

and since $[m, \varphi(n)]$ is divisible by $\varphi(n)$, we have $g^{[m,\varphi(n)]} \equiv 1 \pmod{n}$. Thus,

$$\begin{aligned} g^{d\cdot[m,\varphi(n)]/q} &\equiv \left(g^{[m,\varphi(n)]}\right)^k \\ &\equiv 1 \pmod{n} \end{aligned}$$

which is in contradiction with equation (2.21) since q is a prime divisor of $\varphi(n)$ (why?). So, we must have $d = 1$, and the proof is complete. □

Assume that some positive integer n has a primitive root. An interesting question is to find the number of primitive roots which are incongruent modulo n. The next theorem answers this question.

Theorem 2.12.15. *For any positive integer n, if there exists a primitive root modulo n, then there are exactly $\varphi(\varphi(n))$ incongruent primitive roots modulo n.*

Note. In case the word *incongruent* is somewhat unclear to you: two integers a and b are called *incongruent* modulo a natural number n if and only if $a \not\equiv b \pmod{n}$.

Proof. Assume that g is a primitive root modulo n. We aim to find all primitive roots of n. Since we are looking for incongruent primitive roots modulo n, it suffices to search in the set $\mathbb{U}_n$. Theorem 2.12.9 tells us that $\{g, g^2, \cdots, g^{\varphi(n)}\} \equiv \mathbb{U}_n \pmod{n}$ and so we should search for primitive roots in the set $\{g, g^2, \cdots, g^{\varphi(n)}\}$. On the other hand, Corollary 2.12.14 implies tha we should only investigate powers g^m of g for which $(m, \varphi(n)) = 1$. The number of such elements is $\varphi(\varphi(n))$. □

We are back to the first question: for which integers n do we have a primitive root? The process of finding such n is long, and we will break it into smaller parts. The first step is to see if there exist primitive roots modulo primes. We will soon prove that there always exists a primitive root modulo any prime. We need the following lemma to prove our claim.

Lemma 2.12.16. *Let p be a prime and d be a positive integer such that $d \mid p-1$. Then $x^d - 1 \equiv 0 \pmod{p}$ has exactly d incongruent solutions modulo p.*

Proof. Let $p - 1 = dk$ for some integer k. Consider the polynomial

$$P(x) = 1 + x^d + \left(x^d\right)^2 + \cdots + \left(x^d\right)^{k-1}$$

Then,

$$x^{p-1} - 1 = (x^d - 1)P(x) \tag{2.22}$$

By Fermat's theorem, all integers $1, 2, \ldots, p-1$ are solutions to $x^{p-1} - 1 \equiv 0 \pmod{p}$. So, this equation has exactly $p-1 = dk$ solutions. From (2.22), each of these dk solutions is either a solution of $P(x) \equiv 0 \pmod{p}$ or a solution of $x^d - 1 \equiv 0 \pmod{p}$. However, Lagrange's theorem says that $P(x) \equiv 0 \pmod{p}$ has at most $d(k-1)$ solutions and that $x^d - 1 \equiv 0 \pmod{p}$ has at most d solutions. Since $dk = d(k-1) + d$, this is only possible when $x^d - 1 \equiv 0 \pmod{p}$ has exactly d solutions and also $P(x) \equiv 0 \pmod{p}$ has exactly $d(k-1)$ solutions. □

Theorem 2.12.17. *Let p be a prime. There are exactly $\varphi(p-1)$ incongruent primitive roots modulo p.*

Proof. The case $p = 2$ is obvious. If there exists one primitive root of p, then by Theorem 2.12.15 there are exactly $\varphi(\varphi(p)) = \varphi(p-1)$ incongruent primitive roots of p.

So we just need to construct a primitive root for p. The trick is to factorize $\varphi(p) = p-1$ into product of prime powers. Let q be a prime such that $q^k \mid p-1$ for some integer $k \geq 1$. We want to show that there exists some integer a for which $\operatorname{ord}_p(a) = q^k$. By previous lemma, the equation $x^{q^k} - 1 \equiv 0 \pmod{p}$ has exactly q^k solutions. Take a to be one of these solutions. Then $a^{q^k} \equiv 1 \pmod{p}$, and so by Theorem 2.12.1, it follows that $\operatorname{ord}_p(a) \mid q^k$. So $\operatorname{ord}_p(a) = q^j$ for some integer $0 \leq j \leq k$. This means that a is a solution to the equation $x^{q^j} - 1 \equiv 0 \pmod{p}$. If $j = k$, we have found such an a. Otherwise, suppose that $j < k$. Let $i = k - j \geq 1$. Note that if $x^{q^j} \equiv 1 \pmod{p}$, then,

$$\begin{aligned} x^{q^{k-1}} &\equiv \left(x^{q^j}\right)^{k-j-1} \pmod{p} \\ &\equiv \left(x^{q^j}\right)^{i-1} \pmod{p} \\ &\equiv 1 \pmod{p} \end{aligned}$$

That is, every solution to $x^{q^j} \equiv 1 \pmod{p}$ is also a solution to $x^{q^{k-1}} \equiv 1 \pmod{p}$. According to the preceding lemma, number of solutions of $x^{q^{k-1}} \equiv 1 \pmod{p}$ is exactly q^{k-1}. So there are exactly $q^k - q^{k-1}$ integers x which satisfy $x^{q^k} \equiv 1 \pmod{p}$ but not $x^{q^{k-1}} \equiv 1 \pmod{p}$. If we select a from these solutions, we will have $\operatorname{ord}_p(a) = q^k$.

To finish the proof, let

$$p-1=q_1^{\alpha_1}q_2^{\alpha_2}\cdots q_t^{\alpha_t},$$

be the prime factorization of $p-1$. From what we have just proved, there exists some integer a_i for each q_i such that $\operatorname{ord}_p(a_i)=q_i^{\alpha_i}$. According to Theorem (2.12.5), since q_i are relatively prime,

$$\begin{aligned}\deg_p\left(\prod_{i=1}^{t}a_i\right)&=\deg_p(a_1)\deg_p(a_2)\cdots\deg_p(a_t)\\&=q_1^{\alpha_1}q_2^{\alpha_2}\cdots q_t^{\alpha_t}\\&=p-1\\&=\varphi(p)\end{aligned}$$

and so $\prod_{i=1}^{t}a_i$ is a primitive root modulo p. □

The next step is to find what other numbers have a primitive root. We will show, by the help of the following lemma, that all powers of an odd prime number have a primitive root.

Lemma 2.12.18. *Let p be an odd prime and let g be a primitive root modulo p such that $g^{p-1}\not\equiv 1 \pmod{p^2}$. Then,*

$$g^{\varphi(p^k)}\not\equiv 1 \pmod{p^{k+1}}$$

for any integer $k\geq 1$.

Proof. We will induct on k. The base case $k=1$ is immediately followed from the assumption that $g^{p-1}\not\equiv 1 \pmod{p^2}$. As the induction hypothesis, consider that $g^{\varphi(p^k)}\not\equiv 1 \pmod{p^{k+1}}$ for some $k\geq 1$. From Euler's theorem, $g^{\varphi(p^k)}\equiv 1 \pmod{p^k}$, which means

$$g^{\varphi(p^k)}=1+mp^k$$

for some m. The induction hypothesis implies that $p\nmid m$. By Proposition 2.3.3, we know that

$$\begin{aligned}\varphi(p^{k+1})&=p^{k+1}-p^k\\&=p\left(p^k-p^{k-1}\right)\\&=p\cdot\varphi(p^k)\end{aligned}$$

Hence,

$$\begin{aligned}g^{\varphi(p^{k+1})}&=(1+mp^k)^p\\&=1+\binom{p}{1}mp^k+\underbrace{\binom{p}{2}(mp^k)^2+\cdots+\binom{p}{p-1}(mp^k)^{p-1}+(mp^k)^p}_{\text{divisible by } p^{k+2}}\\&\equiv 1+mp^{k+1} \pmod{p^{k+2}}\end{aligned}$$

As m is not divisible by p, mp^{k+1} is not divisible by p^{k+2}. So,

$$g^{\varphi(p^{k+1})}\not\equiv 1 \pmod{p^{k+2}}$$

as desired. □

Theorem 2.12.19. *Let p be an odd prime and let g be a primitive root modulo p (as we know exists from Theorem 2.12.17). Then, either g or $g+p$ is a primitive root modulo p^k for any integer $k \geq 1$.*

Proof. We break the proof into two parts:

1. If $g^{p-1} \not\equiv 1 \pmod{p^2}$, then we will show that g is a primitive root of p^k. That is, we will prove that

$$\operatorname{ord}_{p^k}(g) = \varphi(p^k) \tag{2.23}$$
$$= p^{k-1}(p-1) \tag{2.24}$$

This is obviously true for $k = 1$. Suppose that equation (2.23) holds for some $k \geq 1$. We will prove that it also holds for $k+1$. Let $\operatorname{ord}_{p^{k+1}}(g) = m$. Then

$$\begin{aligned} & g^m \equiv 1 \pmod{p^{k+1}} \\ \implies & g^m \equiv 1 \pmod{p^k} \end{aligned}$$

Since we know that order of g modulo p^k is $\varphi(p^k)$, we should have $\varphi(p^k) = p^{k-1}(p-1) \mid m$. On the other hand, since m is the order of g modulo p^{k+1}, by corollary (2.12.2), we get $m \mid \varphi(p^{k+1}) = p^k(p-1)$. Therefore, m equals either $\varphi(p^k) = p^{k-1}(p-1)$ or $\varphi(p^{k+1}) = p^k(p-1)$. Previous lemma states that it is impossible to have $m = \operatorname{ord}_{p^{k+1}}(g) = \varphi(p^k)$. So, $m = \varphi(p^{k+1})$ and we are done.

2. If $g^{p-1} \equiv 1 \pmod{p^2}$, then we will show that $g+p$ is a primitive root modulo p^k for any integer $k \geq 1$. Note that

$$(g+p)^{p-1} = g^{p-1} + \binom{p-1}{1} g^{p-2}p + \underbrace{\binom{p-1}{2} g^{p-3}p^2 + \cdots + \binom{p-1}{p-2} gp^{p-2} + p^{p-1}}_{\text{divisible by } p^2}$$

Taking modulo p^2,

$$\begin{aligned} (g+p)^{p-1} &\equiv g^{p-1} + (p-1)g^{p-2}p \\ &\equiv 1 - g^{p-2}p \\ &\not\equiv 1 \pmod{p^2} \end{aligned}$$

because $p \nmid g$. We can now apply the same approach we followed in the first case, but now with $g+p$ instead of g. So $g+p$ is a primitive root modulo all powers of p and the proof is complete.

□

Finally, we are ready to answer our question.

Theorem 2.12.20 (Primitive Root Theorem). *Let $n > 1$ be a positive integer. There exists a primitive root modulo n if and only if $n \in \{2, 4, p^k, 2p^k\}$ for some odd prime p and a positive integer k.*

Proof. Obviously, $g = 1$ and $g = 3$ are primitive roots modulo 2 and 4, respectively. So, $n = 2$ and $n = 4$ are off the list. Let's consider the "if" part first. If n has a primitive root, we will prove n must be of the form p^k or $2p^k$, where p is an odd prime. First, let us show that 2^k does not have a primitive root for $k > 2$. It is obvious that if a is a primitive root modulo 2^k, then a is odd. We leave it as an exercise for the reader to prove by induction that for any odd a and $k > 2$,

$$2^k \mid a^{2^{k-2}} - 1$$

Since $\varphi(2^k) = 2^{k-1}$, a is never a primitive root modulo 2^k.

Now, if n is not of the form p^k or $2p^k$, we can write $n = ab$ with $\gcd(a, b) = 1$ and $a > b > 2$. So, $\varphi(b)$ and $\varphi(a)$ are larger than 1, and by Proposition 2.3.3, they are both even. Let g be a primitive root modulo n. This means that $\operatorname{ord}_n(g) = \varphi(ab)$. We will show that this cannot happen. Let $\operatorname{ord}_a(g) = d$ and $\operatorname{ord}_b(g) = e$. Since

$$\begin{aligned} g^{\varphi(a)} &\equiv 1 \pmod{a} \\ g^{\varphi(b)} &\equiv 1 \pmod{b} \end{aligned}$$

by Corollary (2.12.2), we find that $d \mid \varphi(a)$ and $e \mid \varphi(b)$. Hence, by Theorem (2.12.4),

$$\begin{aligned} \operatorname{ord}_{ab}(g) &= [d, e] \\ &\leq [\varphi(a), \varphi(b)] \\ &= \frac{\varphi(a)\varphi(b)}{(\varphi(a), \varphi(b))} \\ &= \frac{\varphi(ab)}{(\varphi(a), \varphi(b))} \\ &\leq \frac{\varphi(ab)}{2} \end{aligned}$$

where we have used the fact that $(\varphi(a), \varphi(b))$ is at least 2. This gives us the contradiction we were looking for. So, n must be of the form p^k or $2p^k$.

The only remaining part is to prove that for an odd prime p and $k \geq 1$, there exist primitive roots modulo the numbers p^k and $2p^k$. According to Theorem 2.12.17, p has a primitive root, say g. It now follows from Theorem 2.12.19 that either g or $g + p$ is a primitive root modulo p^k. Since Euler's totient function is multiplicative, we have

$$\begin{aligned} \varphi(2p^k) &= \varphi(2) \cdot \varphi(p^k) \\ &= \varphi(p^k) \end{aligned}$$

Let g be a primitive root modulo p^k.

1. If g is odd, then

$$\begin{aligned} & g^a \equiv 1 \pmod{p^k} \\ \iff\ & g^a \equiv 1 \pmod{2p^k} \end{aligned}$$

Let $m = \text{ord}_{2p^k}(g)$. If $m < \varphi(2p^k) = \varphi(p^k)$, then $g^m \equiv 1 \pmod{2p^k}$ implies $g^m \equiv 1 \pmod{p^k}$, which contradicts the fact that g is a primitive root modulo p^k. Therefore, g is also a primitive root modulo $2p^k$.

2. If g is even, then $g' = g + p^k$ is an odd number and it is also a primitive root modulo p^k. Applying the same approach used in the first case, we find that g' is a primitive root modulo $2p^k$.

We have shown that $2p^k$ always has a primitive root and the proof is complete. □

Here is a generalization of Wilson's theorem, though it can be generalized even further. We refer the reader to section (5.11) of the book to see another generalization of Wilson's theorem.

Problem 2.12.21. Let n be a positive integer and let $\mathbb{U}_n = \{g_1, g_2, \dots, g_{\varphi(n)}\}$. Prove that if there exists a primitive root modulo n, then

$$g_1 g_2 \cdots g_{\varphi(n)} \equiv -1 \pmod{n}$$

Otherwise,

$$g_1 g_2 \cdots g_{\varphi(n)} \equiv 1 \pmod{n}$$

Hint. Combine Theorems 2.12.20 and 2.12.13 along with the fact that if p is an odd prime and k is a positive integer, then $p^k \mid a^2 - 1$ implies $p^k \mid a + 1$ or $p^k \mid a - 1$.

Theorem 2.12.22. *Let g be a primitive root modulo n. Then $n - g$ is a primitive root modulo n as well if 4 divides $\varphi(n)$.*

Proof. We have a criteria to see if x is a primitive root modulo n. We need to check if $x^{\varphi(n)/p} \not\equiv 1 \pmod{n}$ for any prime p which divides $\varphi(n)$. Therefore, to check if $n - g$ is a primitive root of n, we just need to prove the following holds

$$(n-g)^{\varphi(n)/p} \not\equiv 1 \pmod{n}$$

for any prime divisor p of $\varphi(n)$. Now, since $4 \mid \varphi(n)$, we have $2 \mid \varphi(n)/2$. So, $\varphi(n)/p$ is even for any proper p. Using the fact that $g^2 \equiv (n-g)^2 \pmod{n}$, we get

$$\begin{aligned}(n-g)^{\frac{\varphi(n)}{p}} &\equiv \left((n-g)^2\right)^{\frac{\varphi(n)}{2p}} \\ &\equiv \left(g^2\right)^{\frac{\varphi(n)}{2p}} \\ &\equiv g^{\frac{\varphi(n)}{p}} \\ &\not\equiv 1 \pmod{n}\end{aligned}$$

Thus, $(n-g)$ is a primitive root modulo n as well. □

The use of primitive roots is usually not obvious in problems. There is hardly any hint on why you should use it. Best if you see its use through problems.

Problem 2.12.23. Let p be odd prime number. Prove that equation $x^{p-1} \equiv 1 \pmod{p^n}$ has exactly $p - 1$ different solution modulo p^n.

Solution (1). Let g be a primitive root modulo p^n (which exists by Theorem 2.12.20). Now, take $x = g^k$, so every solution x maps to a certain k. The number of different k is the number of solutions of this congruence equation. Since

$$\begin{aligned} \operatorname{ord}_{p^n}(g) &= p^{n-1}(p-1) \\ g^{k(p-1)} &\equiv 1 \pmod{p^n} \end{aligned}$$

we either have

$$p^{n-1}(p-1) \mid k(p-1)$$

or $p^{n-1} \mid k$ for any such k. Take $k = p^{n-1}\ell$. If $\ell = sp + r$ with $1 \leq r < p$, then we have that

$$\begin{aligned} g^k &= g^{p^{n-1}(p-1)(sp+r)} \pmod{p^n} \\ &\equiv g^{p^{n-1}(p-1)r} \pmod{p^n} \end{aligned}$$

Therefore, for two incongruent solutions, we must have $1 \leq r \leq p-1$, giving us exactly $p-1$ solutions.

Solution (2). This is a special case of Lemma 2.12.16, where $d = p - 1$.

Problem 2.12.24. Prove that 3 is a primitive root modulo p, where p is any prime of the form $2^n + 1$ for some integer $n > 1$.

Solution (1). $p = 2^n + 1$ in particular means $p \equiv 1 \pmod 4$. According to Problem 1.6.17, we find that p is of the form $2^{2^r} + 1$ for some positive integer r. Therefore

$$\begin{aligned} p &= 2^{2^r} + 1 \\ &\equiv (-1)^{2^r} + 1 \\ &\equiv 2 \pmod 3 \end{aligned}$$

which is not a quadratic residue modulo 3. Using the law of quadratic reciprocity and the fact that $p \equiv 1 \pmod 4$,

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{(p-1)/2} = 1.$$

From the above discussion, we know that $\left(\frac{p}{3}\right) = -1$. Therefore, $\left(\frac{3}{p}\right) = -1$ and 3 is a quadratic non-residue modulo p.

We will now prove that for a prime of the form $p = 2^{2^r} + 1$ every quadratic non-residue modulo p is a primitive root modulo p. Since p is a prime, we know that there exists a primitive root modulo p, say g. By Theorem 2.12.12, we know that $g^2, g^4, \cdots, g^{p-1}$ are $p - 1/2$ different nonzero residues modulo p and they are all quadratic residues. Therefore, all the quadratic non-residues are given by

$$g, g^3, g^5, \cdots, g^{p-2}.$$

We will now take one of these residues, say g^{2k+1}, and show that it is a primitive root mod p. This means we want to show that

$$g^{2k+1}, g^{2(2k+1)}, g^{3(2k+1)}, \ldots, g^{(p-1)(2k+1)}$$

are incongruent modulo p, which happens if and only if

$$2k+1, 2(2k+1), 3(2k+1), \dots, (p-1)(2k+1)$$

are all different modulo $p-1$. This happens if and only if $(2k+1, p-1) = 1$, or $(2k+1, 2^{2^r}) = 1$, which is clearly true since $2k+1$ is odd and 2^{2^r} is a power of 2.

Therefore, all quadratic-non residues are primitive roots modulo p, and as we have shown 3 is among them, we are done.

Solution (2). Just like the previous solution, we will use the fact that 3 is not a quadratic residue modulo p. Therefore, by Euler's criterion,

$$3^{\frac{p-1}{2}} \equiv \left(\frac{3}{p}\right) = -1 \pmod{p} \implies 3^{2^{m-1}} \equiv -1 \pmod{p}. \tag{2.25}$$

Let d be the order of 3 modulo p. Since $d \mid p-1 = 2^n$, we must have $d = 2^\alpha$ for some integer α. If $\alpha < n$ then

$$\begin{aligned} 3^{2^\alpha} &\equiv 1 \pmod{p} \\ \implies 3^{2^{n-1}} &\equiv 1 \pmod{p} \end{aligned}$$

which is in contradiction with equation (2.25). So, $d = 2^n$, and this means that 3 is primitive root modulo $p = 2^n + 1$.

Problem 2.12.25. Let p and q be prime numbers such that $p = 2q+1$. Let a be an integer relatively prime to p and incongruent to -1, 0, and 1 modulo p. Show that $-a^2$ is primitive root modulo p.

Solution. Check $q = 2$ for yourself. Assume $q \geq 3$ is an odd prime, say $q = 2k+1$. Hence, $p = 4k+3$, or $p \equiv 3 \pmod{4}$. According to Theorem 2.8.9, $-a^2$ is not a quadratic residue modulo p. Suppose that $-a^2$ is not a primitive root modulo p. Let g be a primitive root modulo p. Theorem 2.12.12 states that there exists an $l \geq 1$ such that

$$g^{2l+1} \equiv -a^2 \pmod{p}.$$

Since $-a^2$ is not a primitive root, there exists an integer k with $k < p-1$ such that

$$g^{(2l+1)k} \equiv (-a^2)^k \equiv 1 \pmod{p}.$$

This, together with Fermat's little theorem, implies $(2l+1)k \mid p-1 = 2q$ and hence $k = 2$. Therefore, $a^4 \equiv 1 \pmod{p}$ and by Fermat's little theorem $4 \mid 2q$, which leads to a contradiction as q is prime. Hence, $-a^2$ is a primitive root modulo p.

Problem 2.12.26. Let q be a prime such that $q \equiv 1 \pmod{4}$ and that $p = 2q+1$ is also prime. Prove that 2 is a primitive root mod p.

Solution. By Euler's criterion, we have

$$2^q \equiv 2^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$

We analyze both cases now:

- Assume that $2^q \equiv -1 \pmod{p}$. Let $\text{ord}_p(2) = d$. Then, $d \mid \varphi(p) = p - 1 = 2q$. Since q is a prime, we must have

$$d \in \{1, 2, q, 2q\}.$$

  Since $q \equiv 1 \pmod{4}$, we have $q \geq 5$ and the cases $d = 1$ and $d = 2$ cannot happen. Also, if $d = q$, then $2^q \equiv 1 \pmod{p}$, which is in contradiction with $2^q \equiv -1 \pmod{p}$. Thus $d = 2q = p - 1$ and 2 is a primitive root modulo p.

- Assume that $2^q \equiv 1 \pmod{p}$. Multiply both sides of this equation by 2 to get $2^{q+1} \equiv 2 \pmod{p}$. Since $q + 1$ is even, the latter equation means that 2 is a quadratic residue modulo p. Therefore, by Theorem 2.8.13, p must be congruent to either 1 or 7 modulo 8. However, problem says that $q \equiv 1 \pmod{4}$ which results in $q \equiv 1$ or $5 \pmod{8}$. Now,

$$p \equiv 2q + 1 \equiv 3 \text{ or } 5 \pmod{8}$$

  which is a quick contradiction. Hence, $2^q \equiv 1 \pmod{p}$ is not possible.

Problem 2.12.27. Suppose that p is an odd prime number. Prove that there exists a positive integer x such that x and $4x$ are both primitive roots modulo p.

Solution. We will prove a stronger claim: there exists some x such that both x and d^2x are primitive roots mod p for any integer d. Let g be a primitive root modulo p. Since d^2 is a quadratic residue mod p, it follows by Theorem 2.12.12 that

$$d^2 \equiv g^{2k} \pmod{p}$$

for some integer k. We then find by Corollary 2.12.14 that any power g^n of g is a primitive root modulo p if and only if $(n, p - 1) = 1$.

Now, it suffices to show there exist two integers a and b such that

$$\begin{aligned} b - a &= 2k \\ \gcd(b, p - 1) & \\ &= \gcd(a, p - 1) = 1 \end{aligned}$$

because then $x = g^a$ would be a solution. This is luckily easy. Let $2, q_1, q_2, \ldots, q_z$ be the prime divisors of $p - 1$. Suppose that $a_1, a_2, \ldots, a_z$ are integers such that $2k \equiv a_i \pmod{q_i}$ for each $1 \leq i \leq z$. By CRT, there exists an a such that

$$\begin{aligned} a &\equiv 1 \pmod{2} \\ a &\equiv -a_i + p_i \pmod{q_i} \end{aligned}$$

where p_i is some prime, not equal to q_i, and $a_i \not\equiv p_i \pmod{q_i}$. It is easy to see $\gcd(a, p - 1) = 1$ and $\gcd(a + 2k, p - 1) = 1$. Thus, g^a and g^{a+2k} are primitive roots modulo p and $g^{a+2k} \equiv d^2 g^a \pmod{p}$, done.

§§2.13 Carmichael Function, Primitive λ-roots

§§§2.13 Carmichael λ Function

In this section, we discuss a very important function in number theory. Carmichael[17] first introduced it for generalizing Euler's totient function. Consider that two relatively prime positive integers a, n are given, and $\text{ord}_n(a) = d$. Now, fix n. Consider the case when $a^d \equiv 1 \pmod{n}$ holds for any positive integer a relatively prime to n. This brings up some questions.

Problem 2.13.1. Does there exists an a such that $\text{ord}_n(a) = d$?

Problem 2.13.2. How do we find the minimum d such that $a^d \equiv 1 \pmod{n}$ holds for any a relatively prime to n?

Let's proceed slowly. We will develop the theories that can solve these problems. For doing that, we have to use properties of order and primitive roots we discussed in previous sections.

Carmichael Function. For a positive integer n, $\lambda(n)$ is the smallest positive integer for which $a^{\lambda(n)} \equiv 1 \pmod{n}$ holds for any positive integer a relatively prime to n. This number $\lambda(n)$ is called the *Carmichael function* of n. Sometimes, it is also called the *lambda function* of n or the *minimum universal exponent* $\pmod{m}$ Sierpiński and Schinzel.[18] Note that Theorem (2.12.1) implies the following theorem.

Theorem 2.13.3. *If $a^d \equiv 1 \pmod{n}$ holds for all a relatively prime to n, then $\lambda(n) \mid d$.*

Corollary 2.13.4. *For any positive integer n, $\lambda(n) \mid \varphi(n)$.*

The following theorem is self-implicating and solves the first problem, if we can prove that $\lambda(n)$ exists. For now, let's assume it does.

Theorem 2.13.5. *Let n be a positive integer. There exists a positive integer a relatively prime to n such that $\text{ord}_n(a) = \lambda(n)$.*

Let's focus on finding $\lambda(n)$. First, consider the case $n = 2^k$.

Theorem 2.13.6. *If $k > 2$ then $\lambda(2^k) = 2^{k-2}$.*

[17] Robert Daniel Carmichael. "Note on a new number theory function". In: *Bulletin of the American Mathematical Society* 16.5 (1910), pp. 232–239. DOI: 10.1090/s0002-9904-1910-01892-9.

[18] Wacław Sierpiński and Andrzej Schinzel. *Elementary theory of numbers*. Polish Scientific Publishers, 1988, Chapter §VI, Section 4, Page 265.

Proof. The integers relatively prime to 2^k are all odd numbers. We will prove by induction that $x^{2^{k-2}} \equiv 1 \pmod{2^k}$ holds for all odd positive integers x. The base case $k = 3$ is obvious. Assume that for some $k \geq 3$, we have

$$x^{2^{k-2}} \equiv 1 \pmod{2^k}$$

or equivalently, $x^{2^{k-2}} - 1 = 2^k t$ for some t. Using the identity $a^2 - b^2 = (a-b)(a+b)$, we can write

$$x^{2^{k-1}} - 1 = \left(x^{2^{k-2}} - 1\right)\left(x^{2^{k-2}} + 1\right) \tag{2.26}$$

$$= 2^k t\left(2^k t + 2\right) \tag{2.27}$$

$$= 2^{k+1} t\left(2^{k-1} t + 1\right) \tag{2.28}$$

This gives $x^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}$, and the induction is complete.

Now, we should prove that 2^{k-2} indeed is the smallest such integer. Again, by induction, the base case is to find an x for which $\operatorname{ord}_8(x) = 2$. Obviously, any $x = 8j \pm 3$ satisfies this condition. Assume that for all numbers t from 1 up to k, we have $\lambda(2^l) = 2^{l-2}$. Let $\lambda(2^{k+1}) = \lambda$. Since we proved that $x^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}$ for all odd x, it follows from Theorem 2.13.3 that $\lambda \mid 2^{k-1}$. So λ is a power of 2. If $\lambda = 2^{k-1}$, we are done. Otherwise, let $\lambda = 2^\alpha$, where $1 \leq \alpha < k-1$. Then for every x, one can write

$$x^{2^\alpha} \equiv 1 \pmod{2^{k+1}} \tag{2.29}$$

However, similarly as in (2.28), for some t,

$$x^{2^\alpha} - 1 = 2^{\alpha+2} t\left(2^\alpha t + 1\right) \tag{2.30}$$

In (2.30), the highest power of 2 which divides $x^{2^\alpha} - 1$ is $2^{\alpha+2}$ (since $2^\alpha t + 1$ is odd). But

$$\alpha + 2 < (k-1) + 2 = k + 1$$

, which contradicts (2.29). The induction is complete. □

Theorem 2.13.7. *For any prime p and any positive integer k,*

$$\begin{aligned}\lambda(p^k) &= \lambda(2p^k) \\ &= \varphi(p^k)\end{aligned}$$

Proof. Consider the congruence equation $x^d \equiv 1 \pmod{p^k}$ and let $d = \lambda(p^k)$. By Corollary 2.13.4, $d \mid \varphi(p^k)$. Take $x = g$ where g is a primitive root modulo p^k. Then, $\operatorname{ord}_{p^k}(g) = \varphi(p^k)$ and we immediately have $\varphi(p^k) | d$. Thus, $d = \varphi(p^k)$. A very similar proof can be stated to show that $\lambda(2p^k) = \varphi(2p^k) = \varphi(p^k)$. □

Theorem 2.13.8. *Let a and b be relatively prime positive integers. Then*

$$\lambda(ab) = \operatorname{lcm}(\lambda(a), \lambda(b))$$

Proof. Suppose that

$$\lambda(a) = d$$
$$\lambda(b) = e$$
$$\lambda(ab) = h$$

Then

$$x^d \equiv 1 \pmod{a}$$
$$x^e \equiv 1 \pmod{b}$$
$$x^h \equiv 1 \pmod{ab}$$

We also have $x^h \equiv 1 \pmod{a}$ and $x^h \equiv 1 \pmod{b}$ as well. Hence, $d \mid h$ and $e \mid h$. This means that $[d, e] = h$ since $[d, e]$ is the smallest positive integer that is divisible by both d and e. □

Generalization of this theorem is as follows.

Theorem 2.13.9. *For any two positive integers a and b,*

$$\operatorname{lcm}(\lambda(a), \lambda(b)) = \lambda(\operatorname{lcm}(a, b))$$

The next theorem combines the above results and finds $\lambda(n)$ for all n.

Theorem 2.13.10. *Let n be a positive integer with prime factorization $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$. Also, let p be a prime and k be a positive integer. Then*

$$\lambda(n) = \begin{cases} \varphi(n) & \text{if } n \in \{2, 4, p^k, 2p^k\} \\ \dfrac{\varphi(n)}{2} & \text{if } n = 2^k \text{ with } k > 2 \\ \operatorname{lcm}(\lambda(p_1^{e_1}), \cdots, \lambda(p_r^{e_r})) & \text{otherwise} \end{cases}$$

Theorem 2.13.11. *For positive integers a and b, if $a \mid b$, then $\lambda(a) \mid \lambda(b)$.*

The proof is left as an exercise for the reader. We are now ready to fully solve Problem 2.13.1.

Theorem 2.13.12. *For fixed positive integers n and d, there exists a positive integer a relatively prime to n so that $\operatorname{ord}_n(a) = d$ if and only if $d \mid \lambda(n)$.*

Proof. The "if" part is true by Theorem 2.12.1. For the "only if" part, assume that g is an integer with $\operatorname{ord}_n(g) = \lambda(n)$ and $\lambda(n) = de$. Then $\operatorname{ord}_n(g^e) = d$, as desired. □

We finish this section by proposing a theorem. We will leave the proof for the reader as an exercise.

Theorem 2.13.13. *If $\lambda(n)$ is relatively prime to n, then n is square-free.*

Recall that n is square-free if it is not divisible by any perfect square other than 1.

§§§2.13 Primitive λ-roots

Carmichael[19] defined a generalization of primitive roots as follows using his function. As you will see, this section generalizes everything related to primitive roots.

Primitive λ-root. Let a and n be relatively prime positive integers. If $\text{ord}_n(a) = \lambda(n)$, then a is a primitive λ-root modulo n. That is, $a^{\lambda(n)}$ is the smallest power of a which is congruent to 1 modulo n. Cameron and Preece[20] shows the following theorem.

Definition. Let n be a positive integer. Define $\xi(n) = \frac{\varphi(n)}{\lambda(n)}$ (read ξ as "ksi"). According to Corollary 2.13.4, $\xi(n)$ is an integer.

Proposition 2.13.14. *There is a primitive root (defined in the previous section) modulo n if and only if $\xi(n) = 1$. Carmichael calls a primitive root a φ-primitive root, and they are, in fact, a special case of λ-primitive roots.*

Now, the existence of a primitive root is generalized to the following theorem from Carmichael's original paper.

Theorem 2.13.15 (Carmicahel). *For any positive integer n, the congruence equation*

$$x^{\lambda(n)} \equiv 1 \pmod{n}$$

has a solution a which is a primitive λ-root, and for any such a, there are $\varphi(\lambda(n))$ primitive roots congruent to powers of a.

We can show that this theorem is true in a similar fashion to what we did in last section, and we leave it as an exercise.

As we mentioned earlier in Proposition 2.3.3, $\varphi(n)$ is always even for $n > 2$. As it turns out, λ and φ share some common properties.

Problem 2.13.16. For any integer $n \geq 1$, either $\xi(n) = 1$ or $\xi(n)$ is even.

Hint. Use the formula for $\lambda(n)$ in Theorem 2.13.10.

Problem 2.13.17. If $\lambda(n) > 2$, the number of primitive λ-roots modulo n is even.

The next theorem generalizes Theorem 2.12.21, which itself was a generalization to Wilson's theorem.

Theorem 2.13.18. *Let n be a positive integer such that $\lambda(n) > 2$. Also, suppose that g is a primitive λ-root modulo n. The product of primitive λ-roots of n is congruent to 1 modulo n.*

[19] Carmichael, "Note on a new number theory function", Page 232 – 233, Result II.

[20] Peter J. Cameron and D. A. Preece. "Primitive Lambda-Roots". In: (Jan. 2014). URL: `https://cameroncounts.files.wordpress.com/2014/01/plr1.pdf`.

Proof. Since $\lambda(n) > 2$, we can easily argue that it must be even. If g is a primitive λ-root modulo n, all the primitive λ-roots are

$$\{g^{e_1}, g^{e_2}, \cdots, g^{e_k}\}$$

where e_i (for $1 \leq i \leq k$) are all (distinct) positive integers with $(e_i, \lambda(n)) = 1$. Also, note that we can pair them up since $\lambda(n)$ is even if $n > 2$. In fact, we can pair g^{e_i} with $g^{\lambda(n)-e_i}$ for all i. Then,

$$\begin{aligned} g^{e_1} \cdot g^{e_2} \cdots g^{e_k} &\equiv g^{\lambda(n)} \cdots g^{\lambda(n)} \\ &\equiv 1 \pmod{n} \end{aligned}$$

□

Corollary 2.13.19. *For any n, there are $\varphi(\lambda(n))$ primitive λ-roots modulo n.*

§§2.14 Pseudoprimes

In general, a *Pseudoprime* is an integer which shares a common property with all prime numbers but is not actually a prime. Pseudoprimes are classified according to which property of primes they satisfy. We will investigate a few types of pseudoprimes in this section.

§§§2.14 Fermat Pseudoprimes, Carmichael Numbers

The most important class of pseudoprimes are Fermat pseudoprimes which come from Fermat's little theorem.

Fermat Pseudoprime to Base a. For an integer $a > 1$, if a composite integer n satisfies $a^{n-1} \equiv 1 \pmod{n}$, then n is said to be a *Fermat pseudoprime to base a* and is denoted by $\text{psp}(a)$. Suppose $a > 1$ is an integer. It can be shown that the number of Fermat pseudoprimes to base a is small compared to the number of primes. Therefore, any number n that passes Fermat's little theorem (i.e., $a^{n-1} \equiv 1 \pmod{n}$) could be considered to be probably a prime and that is why it is called pseudoprime.

Example. Fermat pseudoprime to base 2 are called *Poulet numbers*. $341 = 11 \times 31$ is the smallest Poulet number. The reason is that

$$\begin{aligned} 2^{340} &\equiv \left(2^5\right)^{68} \\ &\equiv (32)^{68} \\ &\equiv 1^{68} \\ &\equiv 1 \pmod{31} \end{aligned}$$

and

$$\begin{aligned} 2^{340} &\equiv \left(2^{10}\right)^{34} \\ &\equiv (1024)^{34} \\ &\equiv (1)^{34} \\ &\equiv 1 \pmod{11} \end{aligned}$$

which yields $2^{340} \equiv 1 \pmod{341}$.

Theorem 2.14.1. *For any integer $a > 1$, there are infinitely many Fermat pseudoprime to base a.*

Proof. Let $p \geq 3$ be any prime number such that $p \nmid a^2 - 1$. We show that

$$n = \frac{a^{2p} - 1}{a^2 - 1}$$

is a Fermat pseudoprime to base a. First, n is composite because

$$n = \frac{a^p - 1}{a - 1} \cdot \frac{a^p + 1}{a + 1}$$

By Fermat's little theorem, $a^{2p} \equiv a^2 \pmod{p}$ and therefore $p \mid a^{2p} - a^2$. Since p does not divide $a^2 - 1$, it divides

$$\begin{aligned} n - 1 &= \frac{a^{2p} - a^2}{a^2 - 1} \\ &= a^{2p-2} + a^{2p-4} + \cdots + a^4 + a^2 \end{aligned}$$

which is an even integer. We can now deduce that $2p \mid n - 1$ because p is odd. Now, $a^{2p} - 1 = n\left(a^2 - 1\right)$ which means $a^{2p} \equiv 1 \pmod{n}$. Thus $a^{n-1} \equiv 1 \pmod{n}$ and n is a Fermat pseudoprime to base a. □

When you first encountered Fermat's little theorem, you may have wondered if the reverse is true. That is, if $a^{n-1} \equiv 1 \pmod{n}$ for all integers a relatively prime to n, then n is prime or not. If you try some examples by hand, you may convince yourself that n must be a prime in order to hold the condition true. Unfortunately, that is not the case. There are infinitely many composite integers n with the given property and the are called *Carmichael numbers*.

Note. Do not be mistaken by this simple statement. It took a long time for number theorists to prove that there indeed exist infinitely many Carmichael numbers.

With the above definition of Fermat pseudoprimes, we may provide another definition for Carmichael numbers.

Carmichael Number. Let n be a positive integer. If n is a Fermat pseudoprime for all values of a that are relatively prime to n, then it is a *Carmichael number* or *Fermat pseudoprime* (and sometimes *absolute Fermat pseudoprime*).

The first few Carmichael numbers are $561, 1105, 1729, \ldots$.

The following theorem shows us a way to determine if an integer is a Carmichael number.

Theorem 2.14.2 (Korselt's Criterion). *A positive integer n is a Carmichael number if and only if all of the following conditions meet.*

i. *n is composite.*

ii. *n is squarefree.*

iii. *For any prime $p|n$, we also have $p-1 \mid n-1$.*

Proof. Let's prove the second proposition first. For the sake of contradiction, let p be a prime factor of n such that p^2 divides n. Then for all a, $p^2 \mid n \mid a^n - a$. Choose $a = p$ and we have $p^2 \mid p^n - p$ or $p^2 \mid p$, which is impossible. So, n is square-free.

Now we will prove the third one. To prove this, we will use a classical technique. Let p be a prime divisor of n. Since $a^n \equiv a \pmod{n}$, we can say $a^n \equiv a \pmod{p}$ for all a. Choose a so that $a \perp p$. Then p divides $a^n - a = a(a^{n-1} - 1)$, thus $p \mid a^{n-1} - 1$. Also from Fermat's little theorem, $p \mid a^{p-1} - 1$.

Here is the crucial part. From Theorem 2.12.17, we know that *there is a primitive root for all primes p*, i.e., there is a positive integer g with $\operatorname{ord}_p(g) = p - 1$. For that g,

$$\begin{aligned} g^{n-1} &\equiv 1 \pmod{p} \\ g^{p-1} &\equiv 1 \pmod{p} \end{aligned}$$

Since $p-1$ is the order, by Theorem 2.12.1, $p - 1 \mid n - 1$ must hold. □

Note. The connection of Carmichael numbers with Carmichael function is obvious. We could just do it in the following way:

It is evident that we need $\lambda(n) \mid n - 1$. For $n > 2$, $\lambda(n)$ is even so $n - 1$ is even too. This means n is odd. Next, $\lambda(n)$ is co-prime to n, so n is square-free.

Euler Pseudoprime to Base a. For an integer $a > 1$, if an odd composite integer n which is relatively prime to a satisfies the congruence relation

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

where $\left(\frac{a}{n}\right)$ is the Jacobi symbol, then n is called an *Euler pseudoprime to base a* and denoted by $\operatorname{epsp}(a)$.

Corollary 2.14.3. *Let $a > 1$ be an odd integer. Then every Euler pseudoprime to base a is also a Fermat pseudoprime to base a.*

There are infinitely many $\operatorname{epsp}(a)$ for any integer $a > 1$. Actually, even more is true: there exist infinitely many Euler pseudoprimes to base a which are product of k distinct primes and are congruent to 1 modulo d, where $k, d \geq 2$ are arbitrary integers.

You may wonder if there exist *absolute Euler pseudoprimes*, numbers which are Euler pseudoprimes to every base relatively prime to themselves. The answer is negative. In fact, it can be shown that an odd composite integer n can be Euler pseudoprime for at most $\frac{1}{2}\varphi(n)$ bases a, where $1 < a < n$ and $(a, n) = 1$. The proof needs some algebraic background and we do not include it in this book.

Example. 121 is an epsp(3). To see why, note that

$$\left(\frac{3}{121}\right) = \left(\frac{3}{11}\right)^2 = 1$$

by the definition of Jacobi symbol (Definition 2.8.3). Now,

$$\begin{aligned} 3^{60} &= \left(3^5\right)^{12} \\ &= (243)^{12} \\ &\equiv 1^{12} \equiv 1 \pmod{121} \end{aligned}$$

As the last class of pseudoprimes, we mention strong pseudoprimes.

Strong Pseudoprime to Base a. Let $n = 2^s d + 1$ where s and d are positive integers and d is odd. Also, let $a > 1$ be a positive integer relatively prime to n such that one of the following conditions holds:

$$\begin{aligned} a^d &\equiv 1 \pmod{n} \\ a^{2^r d} &\equiv -1 \pmod{n} \end{aligned}$$

for some integer $0 \leq r < s$. Then n is called a *strong pseudoprime to base a* and is denoted by spsp(a). It can be proved that every spsp(a) is also a epsp(a) (and hence a psp(a)).

There exist infinitely many strong pseudoprimes to base a for every integer $a \geq 1$. We show a special case of this where $a = 2$ in the following proposition.

Proposition 2.14.4. *There are infinitely many strong pseudoprimes to base 2.*

Proof. If n is a Fermat pseudoprime to base 2, then $2^{n-1} \equiv 1 \pmod{n}$ and so $2^{n-1} - 1 = nk$ for some integer k. Choose $m = 2^n - 1$. We will show that m is a strong pseudoprime to base 2. To proceed, notice that $m - 1 = 2^n - 2 = 2\left(2^{n-1} - 1\right)$ and $2^{n-1} - 1$ is an odd integer. So it suffices to show that $2^{2^{n-1}-1} \equiv 1 \pmod{m}$. Now,

$$\begin{aligned} 2^{2^{n-1}-1} &= 2^{nk} \\ &= \left(2^n\right)^k \\ &\equiv 1^k \equiv 1 \pmod{m} \end{aligned}$$

The proof is complete. □

§§2.15 Using Congruence in Diophantine Equations

Diophantine equations are an especial kind of equations which allow solutions only in integers. They have been studied for a really long time. The name is taken after the

mathematician *Diophantus of Alexandria*. We have avoided discussing such equations in this book because this area is too huge for us to include right now, and for the same reason we had to ax a lot of topics. However, it is compulsory that we discuss how to use modular arithmetic to solve some particular Diophantine equations. And even if the whole equation can not be solved, we can say a lot about the solutions using modular properties.

§§§2.15 Some Useful Properties

There are some modular arithmetic properties that usually come handy. But before showing them, we intend to pose a question.

Question 2.15.1. Find two positive integer whose sum of squares is 123.

Since there does not exist many squares below 123, you may try to do it by hand. And after exhausting all possible cases, you must conclude there are no such integers. But if you are clever, you don't have to go through trial and error. Let's write $a^2+b^2=123$ and notice the following. Exactly one of a or b must be odd since 123 is odd. Without loss of generality, assume a is even (you can take b if you want). Then b is odd, and we know $b^2\equiv 1 \pmod 4$. Thus, $a^2+b^2\equiv 1 \pmod 4$, whereas $123\equiv 3 \pmod 4$. This is a straight contradiction implying there are no such positive integers a and b. The idea seems simple enough, yet powerful to be of great use.

For reaching such a contradiction (it is often the case, Diophantine equations usually do not have any solutions), we use some common facts. The main idea is the same: find a proper n so that the two sides of the equation leave different remainders modulo n.

You might ask what happens if the equation actually *does* have a solution in integers? Let us explain this with an example. Suppose that you are given the simple linear Diophantine equation $6x+5y=82$ and you want to solve it over non-negative integers. Let's solve this problem by trial and error. First, notice that $x\leq 13$ (otherwise $6x$ would exceed 82). We can draw a table to find the solutions.

x	0	1	2	3	4	5	6
y	none	none	14	none	none	none	none
x	7	8	9	10	11	12	13
y	8	none	none	none	none	2	none

Table 2.3: Solving $6x+5y=82$ by trial and error.

As seen in Table 2.3, we need to do 13 calculations to find the solutions

$$(x,y)=(2,14),(7,8),(12,2)$$

Now, consider the same linear equation $6x+5y=82$ again. We are going to solve it using modular arithmetic this time. Take modulo 5 from both sides of the equation.

The left side would be x while the right side is 2, giving us the relation $x \equiv 2 \pmod 5$. Although this does not give us the solution directly, it helps us find the solutions much faster. Just notice that we already know x must be less than or equal to 13, and it must have a remainder of 2 when divided by 5. The only choices for x then are 2, 7, and 12. We can now plug these values of x into the equation and find the solutions with only three calculations (instead of thirteen).

Sometimes we need to use some theorems such as Fermat's little theorem or Wilson's theorem and pair them up with some modular arithmetic. Here are some highly useful congruences:

Theorem 2.15.2. *Let x be an integer (not necessarily positive). Then*

$$\begin{aligned}
x^2 &\equiv 0, 1 \pmod 3 \\
x^2 &\equiv 0, 1 \pmod 4 \\
x^2 &\equiv 0, 1, 4 \pmod 8 \\
x^2 &\equiv 0, 1, 4, 9 \pmod{16} \\
x^3 &\equiv 0, \pm 1 \pmod 7 \\
x^3 &\equiv 0, \pm 1 \pmod 9 \\
x^4 &\equiv 0, 1 \pmod{16} \\
x^4 &\equiv 0, \pm 1, \pm 4 \pmod{17} \\
x^5 &\equiv 0, \pm 1 \pmod{11} \\
x^6 &\equiv 0, 1, 4 \pmod{13}
\end{aligned}$$

Most of congruences above can be proved easily. Some are direct consequence of Fermat's or Euler's theorem. Or you can just consider the complete set of residue of the modulus and then investigate their powers. Whatever the case, we will leave the proofs as exercises. Sometimes you may notice that Fermat's little theorem or Euler's theorem is disguised in the equation.

Problem 2.15.3. The sum of two squares is divisible by 3. Prove that both of them are divisible by 3.

Solution. Assume that $a^2 + b^2$ is divisible by 3. If a is divisible by 3, so must be b. So, take a not divisible by 3. Then, from the properties above, we have $a^2 \equiv 1 \pmod 3$ and $b^2 \equiv 1 \pmod 3$. And this immediately gives us a contradiction that $a^2 + b^2 \equiv 1 + 1 \equiv 2 \pmod 3$.

Remark. We could just use Theorem 2.8.9 which shows that every prime factor of $a^2 + b^2$ is of the form $4k + 1$ if a and b are coprime.

Problem 2.15.4. Show that there are no integers a, b, c for which $a^2 + b^2 - 8c = 6$.

Solution. The term $-8c$ guides us to choose the right modulo. Consider the equation modulo 8. We have $a^2 + b^2 \equiv 6 \pmod 8$. By Theorem 2.15.2, $a^2 \equiv 0, 1, \text{or } 4 \pmod 8$. Now you may check the possible combinations to see that $a^2 + b^2 \equiv 6 \pmod 8$ is impossible.

Problem 2.15.5. Solve the Diophantine equation $x^4 - 6x^2 + 1 = 7 \cdot 2^y$ in integers.

Solution. There are no solutions for $y < 0$. So assume $y \geq 0$. Add 8 to both sides of the equation to get

$$(x^2 - 3)^2 = 7 \cdot 2^y + 8$$

Note that if $y \geq 3$, the right hand side of above equation is divisible by 8. So taking modulo 8 may seem reasonable. However, it leads to $(x^2 - 3)^2 \equiv 0 \pmod 8$ and no further results are included. We should look for another modulo. If $y \geq 4$, then the right hand side is congruent to 8 modulo 16. However, the left hand side, $(x^2 - 3)^2$ is a square and so it's $0, 1, 4$, or 9 modulo 16. The only left cases are $y = 0, 1, 2$, and 3 which imply no solutions. Hence, no solutions at all.

Let's see another problem in which we will also see an application of *Fermat's method of infinite descent*. This is a technique for solving Diophantine equations but we briefly use the idea here.

Problem 2.15.6. Find all integer solutions to the equation

$$x^2 + y^2 = 7(z^2 + t^2)$$

Solution. First of all, using the same approach as in previous problem, we can prove that 7 divides both x and y. Let $x = 7a$ and $y = 7b$ and substitute them in the equation. After dividing by 7,

$$z^2 + t^2 = 7(a^2 + b^2)$$

Note that this equation looks like the original one. However, z and t in the latter equation are strictly smaller than x and y in the original equation. We can continue this process by noting the fact that z and t are divisible by 7. So, assume that $z = 7u$ and $t = 7v$ and rewrite the equation as

$$u^2 + v^2 = 7(a^2 + b^2)$$

This process can be done infinitely many times. Thus, we get that x and y are divisible by 7^i for all positive integers i, which is not possible. So, the equation does not have any solutions. The process of finding new equations similar to the original one is called the method of *infinite descent*.

Problem 2.15.7. Show that the following equation does not have any solutions in positive integers:

$$5^n - 7^m = 1374$$

Solution. The most important thing in solving a Diophantine equation is to take the right modulo. In this case, it's obvious that the easiest mods to take are 5 and 7. Let's take modulo 5 from both sides of the equation. Since $7^m \equiv 2^m \pmod 5$,

$$\begin{aligned} -2^m &\equiv -1 \pmod 5 \\ \implies 2^m &\equiv 1 \pmod 5 \end{aligned}$$

Since $\text{ord}_5(2) = 4$, we have $4 \mid m$. Let $m = 4k$ for some integer k. So $7^m = 7^{4k} = \left(7^k\right)^4$. This reminds us of the fact that x^2 (and thus x^4) is either 0 or 1 modulo 4. So, $7^m \equiv 1 \pmod 4$. Taking modulo 4 from the original equation, we get

$$\begin{aligned} 5^n - 7^{4k} &\equiv 2 \pmod 4 \\ \implies 1 - 1 &\equiv 2 \pmod 4 \end{aligned}$$

which is a contradiction. Thus, there are no solutions.

Problem 2.15.8 (Kazakhstan 2016). Solve in positive integers the equation

$$n! + 10^{2014} = m^4$$

Solution. You can usually use modular arithmetic to solve the problem when there is a factorial term in the given equation. The interesting property of $n!$ is that it is divisible by all integers less than or equal to n. In this problem, if we find the right modulo k, we can assume $n \geq k$ and take modulo k from the equation (we will check the cases when $n < k$ later). It will be $10^{2014} \equiv m^4 \pmod k$. As said before, we guess the equation does not have any solutions. So, we are searching for a modulo k for which m^4 cannot be congruent to 10^{2014}. We should first try the simplest values for k, i.e., values of k for which m^4 can have a few values. For $k = 16$, we have $m^4 \equiv 0 \pmod{16}$, no contradiction. For $k = 17$, we have $m^4 \equiv 8 \pmod{17}$, which is impossible because m^4 can only have the values $0, \pm 1$, or ± 4 modulo 17. We have found our desired contradiction, and we just have to check the values of $n < 17$. This is easy. Obviously, $n! + 10^{2014}$ is bigger than 10^{2014}. However, the smallest perfect square bigger than 10^{2014} is

$$\left(10^{1007} + 1\right)^2 = 10^{2014} + 2 \cdot 10^{1007} + 1$$

which is way bigger than $10^{2014} + 16!$. So, no solutions in this case as well.

Problem 2.15.9. Prove that the equation $x^2 + 5 = y^3$ has no integer solutions.

Solution. Taking modulo 4, since $x^2 + 5$ is congruent to either 1 or 2 modulo 5, but y^3 is never congruent to 2 modulo 4, we have $x^2 + 5 \equiv y^3 \equiv 1 \pmod 4$, and so x is even, $y \equiv 1 \pmod 4$. Rewrite the equation as

$$x^2 + 4 = (y - 1)(y^2 + y + 1)$$

Note that since $y \equiv 1 \pmod 4$, we have $y^2 + y + 1 \equiv 3 \pmod 4$. According to theorem (1.5.14), we know that every number congruent to 3 modulo 4 has a prime divisor also congruent to 3 modulo 4. Let $p \equiv 3 \pmod 4$ be that prime divisor of $y^2 + y + 1$. Then

$$x^2 + 4 \equiv 0 \pmod p$$

If we raise both sides of the congruence equation $x^2 \equiv -4 \pmod p$ to the power of $\frac{p-1}{2}$ (which is an odd integer since $p \equiv 3 \pmod 4$), we have

$$\left(x^2\right)^{\frac{p-1}{2}} \equiv -(4)^{\frac{p-1}{2}} \pmod p$$

or, by Fermat's little theorem,

$$\begin{aligned} 1 &\equiv x^{p-1} \\ &\equiv -4^{p-1} \\ &\equiv -1 \pmod{p} \end{aligned}$$

This is the contradiction we were looking for and the equation does not have integer solutions.

Note. The idea of taking a prime $p \equiv 3 \pmod 4$ of a number $n \equiv 3 \pmod 4$ comes handy in solving Diophantine equations pretty a lot. Keep it in mind.

Problem 2.15.10 (Romania JBMO TST 2015). Solve in nonnegative integers the equation

$$21^x + 4^y = z^2$$

Solution. First, let us consider the case $x = 0$. Then $z^2 - 1 = (z-1)(z+1) = 4^y$. If $z - 1 = 1$ and $z + 1 = 4^y$, we have no solutions. Otherwise, both $z - 1$ and $z + 1$ should be perfect powers of 4, which is impossible.

We can show, in a similar way, that the case $y = 0$ gives no solutions as well. So, suppose that x and y are positive integers.

Rewrite the original equation as

$$3^x \cdot 7^x = (z - 2^y)(z + 2^y)$$

There are a few cases to check:

- If $z - 2^y = 1$, then $z + 2^y = z - 2^y + 2^{y+1} = 1 + 2^{y+1} = 21^x$. This implies $2^{y+1} = 21^x - 1$. But the right hand side of the latter equation is divisible by 20, contradiction. So no solutions in this case.

- If both $z-2^y$ and $z+2^y$ are divisible by 21, then $21 | (z-2^y, z+2^y)$. This is impossible because if $d = (z - 2^y, z + 2^y)$, then $d \mid (z + 2^y) - (z - 2^y) = 2^{y+1}$, which means d is a power of 2.

- If $z - 2^y = 3^x$ and $z + 2^y = 7^x$, then

  $$7^x - 3^x = 2^{y+1} \tag{2.31}$$

  $y = 1$ gives the solution $(x, y, z) = (1, 1, 5)$. Assume $y \geq 2$. Take modulo 8 from equation (2.31). 2^{y+1} is divisible by 8 and so $7^x - 3^x \equiv 0 \pmod 8$. But this does not happen for any x (just consider two cases when x is even or odd). So the only solution in this case is $(x, y, z) = (1, 1, 5)$.

Note that we have used the fact that $z + 2^y > z - 2^y$ to omit some cases (like when $z - 2^y = 21^x$ and $z + 2^y = 1$). So, $(x, y, z) = (1, 1, 5)$ is the only solution to the given equation.

§§2.16 Exercises

Problem 2.16.1. Consider the following progression:

$$u_0 = \frac{1}{2}$$
$$u_{n+1} = \frac{u_n}{3 - 2u_n}$$

for $n \in \mathbb{N}$. Let a be a real number. We define the series $\{w_n\}$ as

$$w_n = \frac{u_n}{u_n + a}$$

Find all values of a such that w_n is a geometric progression.

Problem 2.16.2. Let p be an odd prime number and consider the following sequence of integers: $a_1, a_2 \ldots a_{p-1}, a_p$. Prove that this sequence is an arithmetic progression if and only if there exists a partition of the set of natural numbers $\mathbb{N}$ into p disjoint sets A_1, $A_2 \ldots, A_{p-1}, A_p$ such that the sets $\{a_i + n \mid n \in A_i\}$ (for $i = 1, 2, \cdots, p$) are identical.

Problem 2.16.3. Assume we have 15 prime numbers which are elements of some arithmetic sequence with common difference d. Prove that $d > 30000$.

Problem 2.16.4 (Vietnam Pre-Olympiad 2012). Determine all values of n for which there exists a permutation $(a_1, a_2, a_3, \cdots, a_n)$ of $(1, 2, 3, \cdots, n)$ such that

$$\{a_1, a_1a_2, a_1a_2a_3, \cdots, a_1a_2 \cdots a_n\}$$

is a complete residue system modulo n.

Problem 2.16.5. Prove that for any two positive integers m and n, there exists a positive integer x, such that

$$2^x \equiv 1999 \pmod{3^m}$$
$$2^x \equiv 2009 \pmod{5^n}$$

Problem 2.16.6. Let $f(x) = 5x^{13} + 13x^5 + 9ax$. Find the least positive integer a such that 65 divides $f(x)$ for every integer x.

Problem 2.16.7 (Romanian Mathematical Olympiad 1994). Find the remainder when 2^{1990} is divided by 1990.

Problem 2.16.8. Prove that $a^2 + b^5 = 2015^{17}$ has no solutions in $\mathbb{Z}$.

Problem 2.16.9 (Middle European Mathematical Olympiad 2009). Determine all integers $k \geq 2$ such that for all pairs (m, n) of different positive integers not greater than k, the number $n^{n-1} - m^{m-1}$ is not divisible by k.

Problem 2.16.10 (ELMO 2000). Let a be a positive integer and let p be a prime. Prove that there exists an integer m such that

$$m^{m^m} \equiv a \pmod{p}$$

Problem 2.16.11. Find all pairs of prime numbers (p, q) for which

$$7pq^2 + p = q^3 + 43p^3 + 1$$

Problem 2.16.12 (IMO 1996). The positive integers a and b are such that the numbers $15a + 16b$ and $16a - 15b$ are both squares of positive integers. What is the least possible value that can be taken on by the smaller of these two squares?

Problem 2.16.13. 2017 prime numbers $p_1, \ldots, p_{2017}$ are given. Prove that

$$\prod_{i<j} (p_i^{p_j} - p_j^{p_i})$$

is divisible by 5777.

Problem 2.16.14 (Ukraine 2014). Find all pairs of prime numbers (p, q) that satisfy the equation

$$3p^q - 2q^{p-1} = 19$$

Problem 2.16.15. Let p be an odd prime and let ω be the p^{th} root of unity (that is, ω is some complex number such that $\omega^p = 1$). Let

$$X = \sum \omega^i$$
$$Y = \sum \omega^j$$

where i in the first sum runs through quadratic residues and j in the second sum runs over quadratic non-residues modulo p and $0 < i, j < p$. Prove that XY is an integer.

Problem 2.16.16. Let $p > 2$ be a prime number. Prove that in the set

$$\{1, 2, \cdots, \lfloor \sqrt{p} \rfloor + 1\}$$

there exists an element which is not a quadratic residue mod p.

Problem 2.16.17 (APMO 2014). Find all positive integers n such that for any integer k there exists an integer a for which $a^3 + a - k$ is divisible by n.

Problem 2.16.18. Let $b, n > 1$ be integers. Suppose that for each $k > 1$ there exists an integer a_k such that $b - a_k^n$ is divisible by k. Prove that $b = A^n$ for some integer A.

Problem 2.16.19. 16 is an eighth power modulo every prime.

Problem 2.16.20. Let m and n be integers greater than 1 with n odd. Suppose that n is a quadratic residue modulo p for any sufficiently large prime number $p \equiv -1 \pmod{2^m}$. Prove that n is a perfect square.

Problem 2.16.21. Form the infinite graph A by taking the set of primes p congruent to $1 \pmod 4$, and connecting p and q if they are quadratic residues modulo each other. Do the same for a graph B with the primes $1 \pmod 8$. Show A and B are isomorphic to each other.

Problem 2.16.22. Find all positive integers n that are quadratic residues modulo all primes greater than n.

Problem 2.16.23. Let k be an even positive integer and $k \geq 3$. Define

$$n = \frac{2^k - 1}{3}$$

Find all k such that (-1) is a quadratic residue modulo n.

Problem 2.16.24. Let n and k be given positive integers. Then prove that

- there are infinitely many prime numbers p such that $\pm 1, \pm 2, \pm 3, \ldots, \pm n$ are quadratic residue of p, and
- there infinitely many prime numbers $p > n$ such that $\pm i/j$ are k^{th}-power residue of p, where i and j are integers between 1 and n (inclusive).

Problem 2.16.25. Let $p > 5$ be a prime number and

$$A = \{b_1, b_2, \cdots, b_{\frac{p-1}{2}}\}$$

be the set of all quadratic residues modulo p, excluding zero. Prove that there doesn't exist positive integers a and c satisfying $(ac, p) = 1$ such that set

$$B = \{ab_1 + c, ab_2 + c, \cdots, ab_{\frac{p-1}{2}} + c\}$$

and A are disjoint modulo p.

Problem 2.16.26. Let p be a prime number such that $p = a^2 + 5b^2$, where a and b are positive integers and a is odd. Prove that a is a quadratic residue modulo p if and only if $p \equiv 1 \pmod 5$.

Problem 2.16.27. Find all primes p such that $5, 7$, and -7 are quadratic residues modulo p.

Problem 2.16.28. Prove that there are no positive integers k such that for the first k odd prime numbers $p_1, p_2, \cdots, p_k$, there are $a, n \in \mathbb{Z}^+$ $(n > 1)$ satisfying

$$p_1 p_2 \cdots p_k = a^n + 1$$

Problem 2.16.29. Find all the pairs of positive integers (x, p) such that p is a prime, $x \leq 2p$, and x^{p-1} is a divisor of $(p-1)^x + 1$.

Problem 2.16.30. Determine all positive integers n such that $3^n + 1$ is divisible by n^2.

Problem 2.16.31. Find a condition for $a \in \mathbb{N}$ such that there are infinitely many natural x such that $a^{2x} \equiv a^{2a} \pmod{p}$ implies $a^x \equiv -a^a \pmod{p}$, where p is any positive integer.

Problem 2.16.32. Show that n does not divide $2^n - 1$ for $n > 1$.

Problem 2.16.33 (China 2006). Find all positive integer pairs (a, n) such that

$$\frac{(a+1)^n - a^n}{n}$$

is an integer.

Problem 2.16.34. Prove that for any integer $n \geq 2$ the number

$$\frac{3^n - 2^n}{n}$$

is not an integer.

Problem 2.16.35 (China 2009). Find all the pairs of prime numbers (p, q) such that

$$pq \mid 5^p + 5^q$$

Problem 2.16.36. Prove that any two different Fermat numbers are relatively prime with each other.

Note. The n^{th} Fermat number is $F_n = 2^{2^n} + 1$.

Problem 2.16.37. Prove that for all positive integers n, $\gcd(n, F_n) = 1$, where F_n is the n^{th} Fermat number.

Problem 2.16.38. Let a and b be relatively prime integers and let d be an odd prime that divides $a^{2^k} + b^{2^k}$. Prove that $d - 1$ is divisible by 2^{k+1}.

Problem 2.16.39. Prove that if p is a prime, then $p^p - 1$ has a prime factor greater than p.

Problem 2.16.40.

1. Show that if p is a prime and $\text{ord}_p(a) = 3$, then

$$\left(\sum_{j=0}^{2} a^{j^2}\right)^2 \equiv -3 \pmod{p}$$

2. Show that if p is a prime and $\text{ord}_p(a) = 4$, then

$$\left(\sum_{j=0}^{3} a^{j^2}\right)^2 \equiv 8a \pmod{p}$$

3. Show that if p is a prime and $\text{ord}_p(a) = 6$, then

$$\sum_{j=0}^{5} a^{j^2} \equiv 0 \pmod{p}$$

Problem 2.16.41 (Poland 2016). Let k and n be odd positive integers greater than 1. Prove that if there a exists positive integer a such that $k \mid 2^a + 1$ and $n \mid 2^a - 1$, then there is no positive integer b satisfying $k \mid 2^b - 1$ and $n \mid 2^b + 1$.

Problem 2.16.42. Let $n > 9$ be a positive integer such that $\gcd(n, 2014) = 1$. Show that if $n \mid 2^n + 1$, then $27 \mid n$.

Problem 2.16.43. Find all primes p and q that satisfy

$$p^2 + 1 \mid 2003^q + 1$$
$$q^2 + 1 \mid 2003^p + 1$$

Problem 2.16.44. Prove that there do not exist non-negative integers a, b, and c such that

$$(2^a - 1)(2^b - 1) = 2^{2^c} + 1$$

Problem 2.16.45. Find all triples (x, y, z) of positive integers which satisfy the equation

$$2^x + 1 = z(2^y - 1)$$

Problem 2.16.46. Let p be a prime number of the form $3k + 2$ that divides $a^2 + ab + b^2$ for two positive integers a and b. Prove that p divides both a and b.

Problem 2.16.47. Prove Wilson's theorem using primitive roots.

Problem 2.16.48. If p is a prime, show that the product of the primitive roots of p is congruent to to $(-1)^{\varphi(p-1)}$ modulo p.

Problem 2.16.49. Let g be a primitive root modulo a prime p. Find $\text{ord}_{p^r}(g)$.

Problem 2.16.50. Prove that if r is a primitive root modulo m, then so is the multiplicative inverse of r modulo m.

Problem 2.16.51. Prove that 3 is a primitive root modulo p for any prime p of the form $2^n + 1$.

Problem 2.16.52. Suppose $q \equiv 1 \pmod 4$ is a prime, and that $p = 2q + 1$ is also prime. Prove that 2 is a primitive root modulo p.

Problem 2.16.53. Find all Fermat primes F_n such that 7 is a primitive root modulo F_n.

Problem 2.16.54. Prove that if $F_m = 2^{2^m} + 1$ is a prime with $m \geq 1$, then 3 is a primitive root of F_m.

Problem 2.16.55. For a given prime $p > 2$ and a positive integer k, let

$$S_k = 1^k + 2^k + \cdots + (p-1)^k$$

Find those values of k for which $p \mid S_k$.

Problem 2.16.56. Show that for each odd prime p, there is an integer g such that $1 < g < p$ and g is a primitive root modulo p^n for every positive integer n.

Problem 2.16.57. Show that if $p = 8k + 1$ is a prime for some positive integer k, then $p \mid x^4 + 1$ for some integer x.

Problem 2.16.58. Let n be a positive integer. Prove that

$$n \leq 4\lambda(n)\left(2^{\lambda(n)} - 1\right)$$

where $\lambda(n)$ denotes the Carmichael function of n.

Problem 2.16.59. Find $\lambda(1080)$.

Problem 2.16.60 (RMO 1990). Find the remainder when 2^{1990} is divided by 1990.

Hint. Use Carmichael's function.

Problem 2.16.61. Given three integers a, b, c satisfying $a \cdot b \cdot c = 2015^{2016}$. Find the remainder when we divide A by 24, knowing that

$$A = 19a^2 + 5b^2 + 1890c^2$$

Problem 2.16.62 (APMO 2006). Let $p \geq 5$ be a prime and let r be the number of ways of placing p checkers on a $p \times p$ checkerboard so that not all checkers are in the same row (but they may all be in the same column). Show that r is divisible by p^5. Here, we assume that all the checkers are identical.

Problem 2.16.63 (Putnam 1996). Let p be a prime greater than 3. Prove that

$$p^2 \mid \sum_{i=1}^{\left\lfloor \frac{2p}{3} \right\rfloor} \binom{p}{i}$$

Problem 2.16.64. Let a and b be two positive integers satisfying $0 < b \leq a$. Let p be any prime number. Show that

$$\binom{pa}{pb} \equiv \binom{a}{b} \pmod{p^3}$$

Problem 2.16.65. The sequence a_n is defined as follows: $a_1 = 0$ and

$$a_{n+1} = \frac{(4n+2).n^3}{(n+1)^4} a_n + \frac{3n+1}{(n+1)^4}$$

for $n \geq 1$. Prove that there are infinitely many positive integers n such that a_n is an integer.

Hint. Find an explicit formula for a_n and then try Wolstenholme's theorem.

Problem 2.16.66. Let p be an odd prime. Define

$$H_n = 1 + \frac{1}{2} + \ldots + \frac{1}{n}$$

to be the n^{th} *harmonic number* for any positive integer n. Prove that p divides the numerator of both $H_{p(p-1)}$ and H_{p^2-1}.

Problem 2.16.67. Let p be an odd prime number. Define $q = \frac{3p-5}{2}$ and

$$S_q = \frac{1}{2 \cdot 3 \cdot 4} + \frac{1}{5 \cdot 6 \cdot 7} + \cdots + \frac{1}{q(q+1)(q+2)}$$

If we write $\frac{1}{p} - 2S_q$ as an irreducible fraction, prove that p divides the difference between numerator and denominator of this fraction.

Problem 2.16.68. Find the largest power of a prime p which divides

$$S_p = \binom{p^{n+1}}{p^n} - \binom{p^n}{p^{n-1}}$$

Problem 2.16.69. Let $p \geq 5$ be a prime. Prove that

$$\sum_{k=1}^{p-1} \frac{2^k}{k^2} \equiv -\frac{(2^{p-1}-1)^2}{p^2} \pmod{p}$$

Problem 2.16.70. Let $p \geq 3$ be a prime number and let

$$\sum_{j=1}^{p-1} \frac{(-1)^j}{j} \binom{p-1}{j} = \frac{a}{b}$$

where a and b are relatively prime integers. Prove that $p^2 \mid a$.

Problem 2.16.71. Prove that $\binom{2^n-k}{k-1}$ is even for all positive integers n and k such that $2 \leq k \leq 2^{n-1}$.

Problem 2.16.72. How many of the following numbers are divisible by 3?

$$\binom{200}{0}, \binom{200}{1}, \binom{200}{2}, \cdots, \binom{200}{200}$$

Problem 2.16.73. Find all pairs (p, q) prime numbers such that

$$7p^3 - q^3 = 64$$

Problem 2.16.74 (BMO 2009). Solve the equation

$$3^x - 5^y = z^2$$

in positive integers.

Problem 2.16.75. Solve the equation $7^x = 3^y + 4$ in integers.

Problem 2.16.76. Solve the equation $2^x + 3 = 11^y$ in positive integers.

Problem 2.16.77. Solve the Diophantine equation

$$2^x(1 + 2^y) = 5^z - 1$$

in positive integers.

Hint. Take modulo 16.

Problem 2.16.78 (Putnam 2001). Prove that there are unique positive integers a and n such that

$$a^{n+1} - (a+1)^n = 2001$$

§§3 Arithmetic Functions

In chapter Chapter 1, we encountered cases where we had to iterate through the divisors of a number. For example, in problem 1.6.5, we were looking for divisors of 17 that satisfied a certain condition. In the next problem, we checked for divisors of 8. This is a pattern which encourages us to study the number of divisors in details. One can go a step further and ask the sum of these divisors. It is natural that we would encounter more of these functions repeatedly. Therefore, we are interested in similar functions that involve natural numbers. .

§§3.1 Definitions

Arithmetic Function. An *arithmetic function* f is a function $f : \mathbb{N} \to \mathbb{C}$ with *domain* $\mathbb{N} = \{1, 2, \cdots, n, \cdots\}$ and *co-domain* $\mathbb{C} = \{a + bi : (a, b) \in \mathbb{R}^2\}$, where i is the imaginary unit defined by $i = \sqrt{-1}$. Here, we are primarily interested in $f : \mathbb{N} \to \mathbb{N}$ only.

Remark. The original definition of arithmetic functions states that the output of an arithmetic function can be any complex number. For example, consider the function $f : \mathbb{N} \to \mathbb{C}$ with

$$f(n) = \frac{n^e e^{-n}}{e^n + n + 1 + \ln n}$$

With the above definition, $f(n)$ is an arithmetic function even though it does not represent any specific property of n. In this chapter, we want to study functions that present some *number theoric* properties. One example of such a function would be $\varphi(n)$. As you already know, the Euler's totient function takes a positive integer n as its input and gives the number of positive integers less than n and relatively prime to n as its output.

Here are some examples of arithmetic functions.

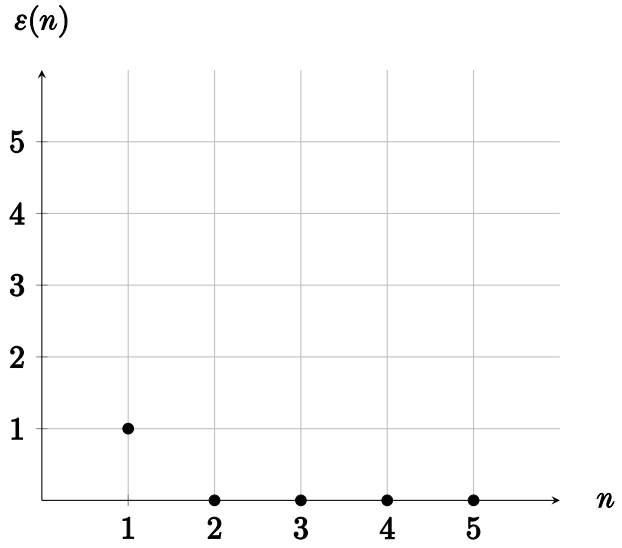


Figure 3.1: The unit function $\varepsilon(n)$ for $n = 1, 2, \cdots, 5$.

Unit Function. The *unit function* is defined as below for all positive integers n:

$$\varepsilon(n) = \left[\frac{1}{n}\right] = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

The first values of $\varepsilon(n)$ are illustrated in Figure 3.1.

Note. Here, we call $\varepsilon(n)$ the unit function because it acts like 1 when multiplying arithmetic functions. That is, ε is the multiplicative identity of arithmetic functions. In section 3.3, we will discuss the process of finding the result of multiplication of two arithmetic functions (called the Dirichlet product) and explain why $\varepsilon(n)$ has this property.

Identity Function. The *identity function*, id, maps every positive integer to itself so $\mathrm{id}(n) = n$ for all positive integers n.

Constant Function. Let c be a fixed positive integer.Consider the function f with the property that $f(n) = c$ for all positive integers n. We call f the *constant c function*. A plot for constant 4 function can be seen in Figure 3.3.

Additive Function. An arithmetic function f is called an *additive function* if and only if

$$f(mn) = f(m) + f(n) \tag{3.1}$$

for all $m, n \in \mathbb{N}$ such that $m \perp n$. The condition $m \perp n$ is particularly significant for a lot of arithmetic functions as we will see later. The case where equation 3.1 is true for all $m, n \in \mathbb{N}$, f is called a *completely additive function*.

Multiplicative Function. An arithmetic function f is called a *multiplicative function* if and only if

$$f(mn) = f(m)f(n) \tag{3.2}$$

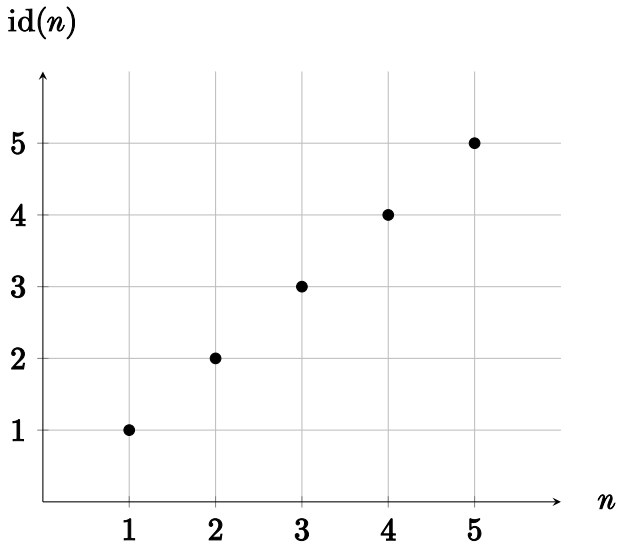


Figure 3.2: The identity function $\mathrm{id}(n)$ for $n = 1, 2, \cdots, 5$.

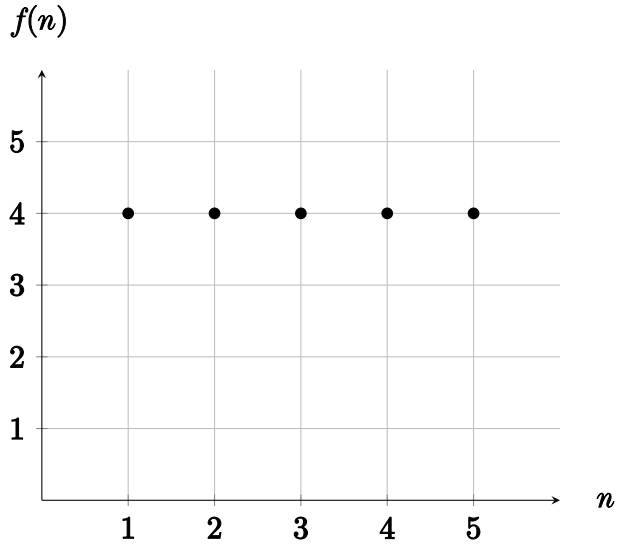


Figure 3.3: The constant 4 function ($f(n) = 4$) for $n = 1, 2, \cdots, 5$.

for all $m, n \in \mathbb{N}$ such that $m \perp n$. In the case where equation 3.2 is true for all $m, n \in \mathbb{N}$, f is called a *completely multiplicative function*.

Example. The identity function and the constant 1 function $g(n) = 1$ are completely multiplicative because for any two positive integers m and n,

$$\begin{aligned} \mathrm{id}(mn) &= mn \\ &= m \cdot n \\ &= \mathrm{id}(m)\mathrm{id}(n) \end{aligned}$$

$$\begin{aligned} g(mn) &= 1 \\ &= 1 \cdot 1 \\ &= g(m)g(n) \end{aligned}$$

§§3.2 Common Arithmetic Functions

§§§3.2 Number of Divisors

We first introduced $\tau(n)$ in chapter Chapter 1. To be precise, in Theorem 1.5.15, we explained that there are $\tau(n)$ positive integer solutions (a, b) to the equation $ab = n$. For example, $ab = 12$ has $\tau(12) = 6$ solutions $(1, 12), (2, 6), (3, 4), (4, 3), (6, 2), (12, 1)$ in positive integers.

Number-of-divisors Function. Let n be a positive integer. The number of positive divisors of n is denoted by $\tau(n)$. In other words, the *number-of-divisors* function is defined as

$$\tau(n) = \sum_{d|n} 1$$

What if the number is so huge that we can not compute all the divisors by hand? Or what if we need to tell a computer how to compute the number of divisors in general?[1] If you need more motivation to find a way to compute number of divisors easily, consider the following nice problem!

Problem 3.2.1 (Bangladesh National Mathematical Olympiad, 2010). You have a regular 2016-gon. You have to choose some points from that polygon so that the resulting polygon you get from those points is a regular polygon. How many distinct regular

[1] Well, you can use a brute force method if you are familiar with programming. But certainly iterating through integers from 1 to n or a solution of that complexity is not a good idea.

polygons can you construct this way? Order of vertex is not important. And the polygon will be constructed joining a point with the next one in an order that does not result in a self intersecting polygon or a polygon which has an angle larger than 180 (convex simple polygon in other words).

Solution. First, try to make sense of what this problem is asking. This is one of those problems that make you think in a nice way while also teaching that theorems are not everything to solve problems. A very important point to keep in mind here is that, the order in which we pick the points does not matter.

The next step should be finding out how we should pick those points if we want to make a regular polygon and how many points are necessary to make such a polygon. Let us label the points of the 2016-gon as $P_1, P_2, \dots, P_{2016}$. So, the regular polygon would be $P_1P_2 \dots P_{2016}$. Here, P_1 is connected to P_2, P_2 to P_3, and so on. However, P_{2016} would be connected to P_1 to complete the cycle of the polygon.

An important observation: we can always let P_1 be the first vertex of the regular polygon we want to construct. Because no matter where we start from, if we rotate, it would be identical to the one that can be created starting from P_1. So, P_1 is the first vertex of our regular polygon. Also, we fix the number of points in the new regular polygon we want to create. If it has k points, all k sides must be equal.

Assume that we want to construct a regular quadrilateral $P_1P_iP_jP_k$. What can we say about i, j or k? The length P_1P_i must be equal to P_iP_j, and P_jP_k. This implies that j must be $i + i$. Because if $j < i$ then P_iP_j would be less than P_1P_i (if you are confused about it, just rotate P_iP_j back to P_1P_i). Then we also must have $k = 3i$. This in turn implies that if there are m points we must have $2016 = mq$ for some integer q. That is, m must be a divisor of 2016. Therefore, the number of distinct polygons is the number of distinct divisors of 2016. But we must consider divisors greater than 2 only. Because we can not create a polygon with one or two points. We have found the solution, but it would be a lot nicer if we actually knew the value of that.

We will see how to compute number of divisors for a positive integer n. Take $n = 12$. If d is a divisor of n, then it is evident that d can not have any prime factor that is not in n. But the opposite might be true. n might have some prime factor that is not in d. In this case, a divisor of 12 must have prime factor of 2 and 3 only. Second observation is: we have $n = 2^2 \cdot 3^1$. Thus, d can not have the exponent of 2 greater than 2 or the exponent of 3 greater than 1. If $d = 2^a3^b$ then $a \leq 2$ and $b \leq 1$. The most interesting part is that, we can actually generate all the divisors this way. Set $a = 0, 1, 2$ and $b = 0, 1$. Consider the sets $A = \{2^0, 2^1, 2^2\}$ and $B = \{3^0, 3^1\}$. If we multiply an element of A with an element of B, we get a divisor of 12. And for each multiplication, we get a distinct divisor each time. And certainly, this can be generalized. If the prime factorization of n is $p_1^{e_1}p_2^{e_2} \cdots p_k^{e_k}$, then the divisors can be generated multiplying elements from sets $A_1 = \{p_1^0, \dots, p_1^{e_1}\}, A_2 = \{p_2^0, \dots, p_2^{e_2}\}, A_k = \{p_k^0, \dots, p_k^{e_k}\}$. A_i has $e_i + 1$ elements because the exponent ranges from 0 to e_1. Then clearly, the number of divisors of n would be the product of number of elements in all A_i, that is, $(e_1 + 1) \cdots (e_k + 1)$. However, we will have to prove something even though it is clear from the example. That is, we will not get a duplicate divisor in this process. This will be left as an exercise for the readers.

Theorem 3.2.2. *Let n be a positive integer with prime factorization $n = p_1^{e_1}p_2^{e_2} \cdots p_k^{e_k}$.*

Then,

$$\tau(n) = \prod_{i=1}^{k}(1+e_i) \tag{3.3}$$

Proof. Every positive divisor of n must be of the form

$$d = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$$

where $0 \leq alpha_i \leq e_i$ for $i = 1, 2, \cdots, k$. There are $e_i + 1$ possible values $\{0, 1, 2, \cdots, e_i\}$ for the power of prime p_i in d. The number of divisors of n, $\tau(n)$, is therefore the product of $e_1 + 1, e_2 + 1, \cdots,$ and $e_k + 1$. We are done. □

Theorem 3.2.3. *Let n be a positive integer. Prove that $\tau(n) \leq 2\sqrt{n}$.*

Proof. We can find two positive integers a and b such that $n = ab$. At least one of a and b is less than or equal to $\sqrt{n}$ (otherwise their product will be larger than n). This means that $\frac{\tau(n)}{2}$ can take at most $\lfloor\sqrt{n}\rfloor$ values. So,

$$\tau(n) \leq 2\lfloor\sqrt{n}\rfloor \leq 2\sqrt{n}$$

□

Theorem 3.2.4. *$\tau(n)$ is odd if and only if n is a perfect square.*

Proof. Let n be a positive integer with factorization $n = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ and suppose that $\tau(n)$ is odd. This means that all terms in the right hand side of equation 3.3 must be odd. Therefore, e_i is even for $i = 1, 2, \cdots, k$. Take $e_i = 2f_i$ for some integer f_i. Then,

$$\begin{aligned} n &= p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k} \\ &= p_1^{2f_1}p_2^{2f_2}\cdots p_k^{2f_k} \\ &= \left(p_1^{f_1}p_2^{f_2}\cdots p_k^{f_k}\right)^2 \end{aligned}$$

which is a perfect square. The proof for the converse is easy. □

Problem 3.2.5. Show that for any integer $n > 1$, in the infinite sequence

$$n, \tau(n), \tau(\tau(n)), \tau(\tau(\tau(n))), \cdots$$

all the terms after a certain point onwards are equal to 2.

Solution. For $n = 2$ the statement is obvious, so assume $n > 2$. Note that $\tau(n)$ counts the number of positive integers in the set $\{1, 2, \ldots, n\}$ that divide n. So, it is at most n. For $n > 2$, we know that $n - 1$ does not divide n, hence $\tau(n) < n$ for all $n > 2$. This means that the sequence is strictly decreasing as far as its terms are greater than 2. The proof is complete.

Remark. Thanks to Professor Greg Martin for his suggestion about proving $\tau(n) < n$.

§§§3.2 Sum of Divisors

The sum of divisors of a number is another important property of each positive integer.

Sum-of-divisors Function. Let n be a positive integer. The sum of positive divisors of n is denoted by $\sigma(n)$.[2] In other words, the *sum-of-divisors* function is defined as

$$\sigma(n) = \sum_{d|n} d$$

Note. One might rephrase this definition as: the sum-of-divisors is the summatory function of id.

Example.

- $\sigma(p^2) = p^2 + p + 1$ for any prime p.
- $\sigma(pq) = pq + p + q + 1 = (p+1)(q+1)$, for any two primes p and q.

Note. Just like the number-of-divisors function, σ is not completely multiplicative. Can you think of an example which shows this?

Theorem 3.2.6. *For any positive integer n,*

$$\frac{\sigma(n)}{n} = \sum_{d|n} \frac{1}{d}$$

Proof. Beginning from $\sigma(n) = \sum_{d|n} d$, you can simply realize that the equation can be written in the form

$$\sigma(n) = \sum_{d|n} \frac{n}{d}$$

because when for every divisor d of n, the number n/d also divides n. We can now take n out of the sum in the right side of above equation and finish the proof. □

Note. The idea of employing n/d instead of d, where d is a divisor of n, is a good trick for solving such problems.

As for the case of $\tau(n)$, one can express $\sigma(n)$ explicitly as well.

Theorem 3.2.7. *Let n be a positive integer with prime factorization $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Then,*

$$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{e_i+1} - 1}{p - 1}$$

[2] Read "sigma of n".

Proof. Later in proposition 3.4.10, we will show that σ is multiplicative. Just accept it for now. So, it suffices to prove the assertion for the case when n is a power of a prime. Let $n = p^\alpha$, where p is a prime and α is a positive integer. In this case, the only divisors of n are $1, p, p^2, \cdots, p^\alpha$. Therefore, their sum, $\sigma(n)$, is

$$\sigma(p^\alpha) = 1 + p + p^2 + \cdots + p^\alpha$$

Now, by theorem Theorem 1.5.19, we can write the above equation as

$$\sigma(p^\alpha) = \frac{p^{\alpha+1} - 1}{p - 1}$$

To finish the proof, consider any positive integer n with factorization $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Then,

$$\begin{aligned}\sigma(n) &= \sigma(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) \\ &= \sigma(p_1^{e_1})\sigma(p_2^{e_2}) \cdots \sigma(p_k^{e_k}) \\ &= \prod_{i=1}^{k} \frac{p_i^{e_i+1} - 1}{p - 1}\end{aligned}$$

□

We are going to define amicable numbers as an application of the sum of divisors function.

Definition. Two positive integers are called *amicable numbers*[3] if the sum of proper divisors of each of them is equal to the other. Recall that a proper divisor of n is a divisor of n which is not equal to n. In other words, (m, n) is a pair of amicable numbers if $m = \sigma(n) - n$ and $n = \sigma(m) - m$.

Example. The smallest pair of amicable numbers is $(220, 284)$. One can easily check this:

$$\begin{aligned}220 &= 1 + 2 + 4 + 71 + 142 \\ 284 &= 1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 4 + 55 + 110\end{aligned}$$

Amicable numbers have been studied since a very long time ago, and there is evidence that they were known to Pythagoreans (followers of Pythagoras) which originated in the sixth century BC. According to Dickson[4] Thābit ibn Qurra (826–901) found a formula that generates amicable numbers (which we will state in the following). The Iranian mathematician Muhammad Baqir Yazdi, who lived in 16th century, found the pair $(9363584, 9437056)$ of amicable numbers. You can imagaine how difficult it is to find such numbers without using computers. Over a billion pairs of amicable numbers have been found so far (July 2018).

[3] Amicable: having a spirit of friendliness.

[4] Leonard E. Dickson. *History of the theory of numbers*. Chelsea Pub. Co., 1952, Chapter I, Page 39.

Theorem 3.2.8 (Thābit ibn Qurra's Rule). *Let $n \geq 2$ be a positive integer such that*

$$\begin{aligned} p &= 3 \cdot 2^{n-1} - 1 \\ q &= 3 \cdot 2^n - 1 \\ r &= 9 \cdot 2^{2n-1} - 1 \end{aligned}$$

are all primes. Then, $(2^n \cdot p \cdot q, 2^n \cdot r)$ is a pair of amicable numbers.

Proof. Let $a = 2^n \cdot p \cdot q$ and $b = 2^n \cdot r$. Since p, q, and r are all odd primes, the divisors of a are of the form $2^\alpha \cdot p^\beta \cdot q^\gamma$, where α, β, γ are integers with $0 \leq \alpha \leq n$ and $\beta, \gamma \in \{0, 1\}$. Similarly, the divisors of b are of the form $2^\delta \cdot r^\epsilon$, where δ and ϵ are integers with $0 \leq \delta \leq n$ and $\epsilon \in \{0, 1\}$. Hence,

$$\begin{aligned} \sigma(a) &= \sum_{\alpha=0}^{n} \sum_{\beta=0}^{1} \sum_{\gamma=0}^{1} 2^\alpha p^\beta q^\gamma \\ &= \sum_{\alpha=0}^{n} \sum_{\beta=0}^{1} 2^\alpha p^\beta \sum_{\gamma=0}^{1} q^\gamma \\ &= \sum_{\alpha=0}^{n} \sum_{\beta=0}^{1} 2^\alpha p^\beta (q+1) \\ &= \sum_{\alpha=0}^{n} 2^\alpha (q+1) \sum_{\beta=0}^{1} p^\beta \\ &= \sum_{\alpha=0}^{n} 2^\alpha (p+1)(q+1) \\ &= (p+1)(q+1) \sum_{\alpha=0}^{n} 2^\alpha \\ &= (p+1)(q+1)\left(2^{n+1} - 1\right) \\ &= 9 \cdot 2^{2n-1}\left(2^{n+1} - 1\right) \end{aligned}$$

and so,

$$\begin{aligned} \sigma(a) - a &= 9 \cdot 2^{2n-1}\left(2^{n+1} - 1\right) - 2^n\left(3 \cdot 2^{n-1} - 1\right)\left(3 \cdot 2^n - 1\right) \\ &= 2^n\left(9 \cdot 2^{2n-1} - 1\right) = b \end{aligned}$$

We expect the reader to be able to prove $\sigma(b) - b = a$ in a similar way on their own. This shows that (a, b) is a pair of amicable numbers. □

The above theorem is pretty interesting, but you might wonder if it gives us all the amicable numbers. The answer is negative. You can compute the values of p, q, r, and a, b to see how large they get even when n is as small as 10. For the above theorem to work, we require p, q, r to be primes, and determining whether those numbers are prime is a difficult task for large n.

The mighty Euler Dickson[5] found a more general formula for amicable numbers and discovered 61 pairs of amicable numbers at his time. We state Euler's generalization of Thābit ibn Qurra's rule below, usually called Euler's rule, and leave the proof to the interested reader.

Theorem 3.2.9 (Euler's Rule). *Let m and n be positive integers with $m < n$ such that*

$$\begin{aligned} p &= 2^m \cdot (2^{n-m} + 1) - 1 \\ q &= 2^n \cdot (2^{n-m} + 1) - 1 \\ r &= 2^{n+m} \cdot (2^{n-m} + 1)^2 - 1 \end{aligned}$$

are all primes. Then, $(2^n \cdot p \cdot q, 2^n \cdot r)$ is a pair of amicable numbers.

§§§3.2 Euler's and Jordan's Totient Functions

We have already defined Euler's totient function and used some of its properties to solve problems. In this section, we will prove those properties and provide some more features of φ. We already know that $\varphi(n)$ is the number of positive integers less than n which are equal to n. Suppose that $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ is the prime factorization of n. Then

$$\varphi(n) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdots p_k^{\alpha_k - 1} (p_1 - 1) \cdots (p_k - 1) \tag{3.4}$$

In order to find $\varphi(n)$, we will first find the number of positive integers less than or equal to n which are *not* co-prime to n. Then, $\varphi(n)$ would be the difference of this number and n. Let us consider the simple case $n = pq$, where p and q are primes. A positive integer less than or equal to n is not co-prime to n if it is divisible by either p or q. Let $\psi(n)$ be the number of such positive integers. There are n/p and n/q numbers less than or equal to n which are divisible by p and q, respectively. So, we might guess that $\psi(n) = n/p + n/q$. However, notice that we are counting the number pq in both the numbers divisible by p and divisible by q. So, the true value for $\psi(n)$ is $n/p + n/q - 1$. Thus,

$$\begin{aligned} \varphi(n) &= n - k(n) \\ &= n - n/p - n/q + 1 \\ &= pq - q - p + 1 \\ &= (p-1)(q-1) \end{aligned}$$

which is in agreement with equation 3.4. Take another example when $n = p_1, p_2, \cdots, p_k$, where $p_1, p_2, \cdots, p_k$ are different primes. Our first guess for $\psi(n)$ would be $n/p_1 + n/p_2 + \cdots + n/p_k$. However, we are counting the numbers divisible by $p_i p_j$ (for $1 \le i < j \le k$) twice. So, our next guess for $\psi(n)$ is

$$\psi(n) = \sum_{1 \le i \le k} \frac{n}{p_i} - \sum_{1 \le i < j \le k} \frac{n}{p_i p_j}$$

[5] Dickson, *History of the theory of numbers*, Chapter I, Page 42.

But this is still not true. For instance, the number $p_1p_2p_3$ is counted in the first sum and we remove it by subtracting the second sum. So, we would have to add another sum

$$\sum_{1\le i<j<t\le k}\frac{n}{p_ip_jp_t}$$

to include all products[6] such as $p_1p_2p_3$. This process of adding and subtracting sums is called the *inclusion–exclusion principle*. We will continue the process until we count every number less than or equal to n which is not co-prime to n exactly once. Then, the totient function may be calculated from $\varphi(n)=n-\psi(n)$. The reader is encouraged to calculate $\varphi(n)=(p_1-1)(p_2-1)\cdots(p_k-1)$ using the given approach and check that it is compatible with the formula 3.4. The very same approach may be applied to the general case $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ to finally prove formula 3.4. We strongly recommend the reader try this method for several examples (e.g., $n=p^2q$ or $n=p^3q^4r^5$) and then prove the whole thing.

Using the same method, we can prove a stronger result.

Theorem 3.2.10 (Generalization of φ). *Let m and n be positive integers and let $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ be the prime factorization of n. The number of positive integers less than or equal to m which are co-prime to n is $m-\Psi(m)$, where*

$$\Psi(m)=\sum_{1\le i_1\le k}\left\lfloor\frac{m}{p_{i_1}}\right\rfloor-\sum_{1\le i_1<i_2\le k}\left\lfloor\frac{m}{p_{i_1}p_{i_2}}\right\rfloor+\cdots+(-1)^{k+1}\left\lfloor\frac{m}{p_1p_2\cdots p_k}\right\rfloor$$

We already stated (but did not prove) some properties of Euler's totient function in proposition 2.3.3. Here, we are going to prove them beside a few more.

Theorem 3.2.11 (Properties of φ). *Let m and n be positive integers. Then,*

(a) φ is a multiplicative function. That is, if $m\perp n$, then

$$\varphi(mn)=\varphi(m)\cdot\varphi(n)$$

(b) For all $n\ge 3$, $\varphi(n)$ is even.

(c) φ is neither increasing, injective, nor surjective.

(d) If n is factorized as $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$, then

$$\begin{aligned}\varphi(n)&=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)\\&=p_1^{\alpha_1-1}p_2^{\alpha_2-1}\cdots p_k^{\alpha_k-1}(p_1-1)\cdots(p_k-1)\end{aligned}$$

Proof.

(a) Write the numbers $1,2,\cdots,mn$ in a table with m rows and n columns as below:

[6] Notice the indices under the summation notation

$$\begin{array}{ccccc} 1 & m+1 & 2m+1 & \dots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \dots & (n-1)m+2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ m & 2m & 3m & \dots & nm \end{array}$$

The numbers in the rth row of the table are of the form $km+r$, where $k = 0, 1, 2, \cdots, m-1$. Since $(km + r, m) = (r, m)$, one of these two cases happen: either all numbers in a row are co-prime to m or all of them are not co-prime to m. As we are looking for numbers co-prime to mn, which are obviously those co-prime to both m and n, we consider the rows with all numbers co-prime to m. There are $\varphi(m)$ such rows. Consider one such row in th table:

$$r \quad m+r \quad 2m+r \quad \dots \quad (n-1)m+r$$

The set $\{0, 1, 2, \cdots, n\}$ is a complete residue system modulo n. Since $(m, n) = 1$, by proposition 2.3.2 of chapter Chapter 2, the numbers in the above row of table also form a complete residue system modulo n. This means that all the remainders $0, 1, 2, \cdots, n-1$ happen when you take the numbers in this row modulo n. Now, how many numbers in this row are relatively prime to n? The answer is the same number of integers co-prime to n in the set $\{0, 1, 2, \cdots, n\}$, which is $\varphi(n)$ by definition (try to figure out why). Therefore, there are totally $\varphi(m) \cdot \varphi(n)$ numbers in the table which are co-prime to both m and n, and hence mn. On the other hand, by definition, there are $\varphi(mn)$ numbers co-prime to mn. The conclusion follows.

(b) $\varphi(n)$ is the number of positive integers k such that $k \leq n$ and $k \perp n$. The point is that if k is co-prime to n, then so is $n-k$. Therefore, for $n \geq 3$, one can match all numbers co-prime to n in pairs of $(k, n-k)$, which means that $\varphi(n)$ must be even.

(c) Take $\varphi(5) > \varphi(6)$, $\varphi(n) = \varphi(2n)$ for all odd $n \geq 1$, and $\varphi(n) \equiv 1 \pmod 2$ as counterexamples.

(d) We have already provided the sketch of a proof in the beginning of this section. Here is another proof using multiplicativity of φ. Since $\varphi(n)$ is multiplicative, it suffices to prove the result when n is a power of a prime. Let p be a prime and $\alpha \geq 1$ be an integer. The only numbers which are *not* co-prime to p^α between $1, 2, \cdots, p^\alpha$ are multiples of p. How many multiples of p are there among these numbers? The answer is $p^\alpha/p = p^{\alpha-1}$ (why?). Therefore,

$$\begin{aligned} \varphi(p^\alpha) &= p^\alpha - p^{\alpha-1} \\ &= p^{\alpha-1}(p-1) \end{aligned}$$

Now, if we factorize n as $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, we can write

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) \\ &= \varphi(p_1^{\alpha_1}) \varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k}) \\ &= p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdots p_k^{\alpha_k - 1} (p_1 - 1) \cdots (p_k - 1) \end{aligned}$$

□

Corollary 3.2.12. *If $a \mid b$, then $\varphi(a) \mid \varphi(b)$.*

Theorem 3.2.13. *Prove that*

$$\sum_{d \mid n} \varphi(d) = n$$

holds for all positive integers n

Instead of a full proof, we provide an example and the readers are encouraged to complete the proof for themselves. Let $n = 15$ and consider the following 15 fractions:

$$\frac{1}{15}, \frac{2}{15}, \frac{3}{15}, \frac{4}{15}, \frac{5}{15}, \frac{6}{15}, \frac{7}{15}, \frac{8}{15}, \frac{9}{15}, \frac{10}{15}, \frac{11}{15}, \frac{12}{15}, \frac{13}{15}, \frac{14}{15}, \frac{15}{15}$$

Put all these fractions into lowest terms:

$$\frac{1}{15}, \frac{2}{15}, \frac{1}{5}, \frac{4}{15}, \frac{1}{3}, \frac{2}{5}, \frac{7}{15}, \frac{8}{15}, \frac{3}{5}, \frac{2}{3}, \frac{11}{15}, \frac{4}{5}, \frac{13}{15}, \frac{14}{15}, \frac{1}{1}$$

Obviously, the denominators are all the divisors of 15. Also, there are 15 fractions. Now, note that only those fractions whose numerator is relatively prime to 15 have denominator equal to 15. These are

$$\frac{1}{15}, \frac{2}{15}, \frac{4}{15}, \frac{7}{15}, \frac{8}{15}, \frac{11}{15}, \frac{13}{15}, \frac{14}{15},$$

which are $\varphi(15) = 8$ fractions. Similarly, there are $\varphi(5) = 4$ fractions

$$\frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}$$

which have denominator equal to 5, and $\varphi(3) = 2$ fractions

$$\frac{1}{3}, \frac{2}{3}$$

which have denominator equal to 3. Therefore, we find that the number of fractions is 15 on one hand and $\varphi(15) + \varphi(5) + \varphi(3)$ on the other hand. These two must be equal, hence $\varphi(15) + \varphi(5) + \varphi(3) = 15$.

Camille Jordan generalized the definition of Euler's totient function and introduced *Jordan's totient functions*.

Definition. Let n and k be positive integers. The number of sequences

$$a_1, a_2, \cdots, a_k$$

of positive integers less than or equal to n such that $(a_1, a_2, \cdots, a_k, n) = 1$ is called the k^{th} *Jordan's totient function* and is denoted by $J_k(n)$.

Note. Here, $(a_1, a_2, \cdots, a_k, n)$ is the notation for greatest common divisor of all numbers $a_1, a_2, \cdots, a_k$, and n.

Example.

- $J_k(1) = 1$ for all positive integers k.
- Obviously, $J_1(n) = \varphi(n)$. That is, the first Jordan totient function is Euler's totient function.
- $J_k(p) = p^k - 1$ because all positive integers less than p are co-prime to p.
- Let us write all pairs (a, b) of positive integers less than 6 such that $(a, b, 6) = 1$.

$$
\begin{gathered}
(1,1),(1,2),(1,3),(1,4),(1,5),(1,6),\\
(2,1),(2,3),(2,5),\\
(3,1),(3,2),(3,4),(3,5),\\
(4,1),(4,3),(4,5),\\
(5,1),(5,2),(5,3),(5,4),(5,5),(5,6),\\
(6,1),(6,5)
\end{gathered}
$$

  There are 24 such pairs. Hence, $J_2(6) = 24$.

We will state and prove the properties of Jordan's totient function later in section 3.4.3.

§§3.3 Dirichlet Product and Möbius Inversion

When working with arithmetic functions, we are mostly interested in the *Dirichlet product* of two functions rather than their normal product. As you keep reading this section, you find out why Dirichlet products are important when studying arithmetic functions.

Dirichlet Product or Dirichlet Convolution. For two arithmetic functions f and g, we define their Dirichlet product as

$$h(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$$

where the sum extends over all positive divisors d of n. We denote this by $h = f * g$. In other words,

$$(f * g)(n) = \sum_{ab=n} f(a) g(b)$$

Example. Let f be the constant 1 function. Let us find $(f*f)(n)$. By definition,

$$\begin{aligned}(f*f)(n) &= \sum_{d|n} f(d)f\left(\frac{n}{d}\right)\\ &= \sum_{d|n} 1\\ &= \underbrace{1+1+\cdots+1}_{\text{repeated } \tau(n) \text{ times}}\\ &= \tau(n)\end{aligned}$$

where $\tau(n)$ is the number of divisors of n. More details about this function will be explained in section 3.4.1.

Example. This time, we aim to find the convolution of constant 1 function f with the identity function. Again, by definition,

$$\begin{aligned}(\mathrm{id}*f)(n) &= \sum_{d|n} \mathrm{id}(d)f\left(\frac{n}{d}\right)\\ &= \sum_{d|n} d\\ &= \sigma(n)\end{aligned}$$

where $\sigma(n)$ is the sum of divisors of n. If we show the constant 1 function by $1(n)$, we can write $(\mathrm{id}*1)(n)=\sigma(n)$ or simply $\mathrm{id}*1=\sigma$.

Proposition 3.3.1 (Properties of Dirichlet Convolution). *Let f, g, and h be any arithmetic functions. The Dirichlet product is*

1. *commutative, that is, $f*g=g*f$,*
2. *associative. This means that $(f*g)*h=f*(g*h)$,*
3. *distributive, which means that $f*(g+h)=f*g+f*h$.*

Furthermore, the unit function $\varepsilon(n)$ acts as a unit element for Dirichlet product. That is, $\varepsilon*f=f*\varepsilon=f$ for all arithmetic functions f.

Proof. The proof for commutativity of Dirichlet convolution is pretty straightforward using the definition $(f*g)(n)=\sum_{ab=n} f(a)g(b)$. Obviously, since there is no difference between a and b in the latter formula, we can write it as

$$\begin{aligned}(f*g)(n) &= \sum_{ab=n} f(a)g(b)\\ &= \sum_{ab=n} f(b)g(a)\\ &= \sum_{ab=n} g(a)f(b)\\ &= (g*f)(n)\end{aligned}$$

Let us prove the associativity property now. By definition,

$$\begin{aligned}((f*g)*h)(n) &= \sum_{cd=n}(f*g)(d)h(c)\\ &= \sum_{cd=n}\left(\sum_{ab=d}f(a)g(b)\right)h(c)\\ &= \sum_{cd=n}\left(\sum_{ab=d}f(a)g(b)h(c)\right)\\ &= \sum_{abc=n}f(a)g(b)h(c)\end{aligned}$$

Again, since there is a symmetry between a, b, and c, we find that the order of f, g, and h in the expression $(f*g)*h$ does not change the result. Hence, the Dirichlet product is associative. The proof for distributivity is similar and is left for the reader. It is also trivial by definition that ε is the unit element of Dirichlet convolution. □

We are going define the Möbius function $\mu(n)$, which doesn't seem very natural at first sight. As we go deeper in this chapter and in chapter Chapter 4 on primes, we will find out why this is in fact very important. It will help us a lot when solving problems concerning inclusion and exclusion. In other words, the definition of the Möbius function is natural in the way that it's trying to alternate positive and negative signs in an inclusion-exclusion argument.

Möbius Function. The Möbius function $\mu(n)$ is defined as

$$\mu(n)=\begin{cases}1 & \text{if } n=1\\ 0 & \text{if } n \text{ is divisible by } p^2 \text{ for some prime } p\\ (-1)^k & \text{if } n=p_1p_2\cdots p_k\end{cases}$$

Example. $\mu(20)=0$ because $2^2 \mid 20$. Also, $\mu(105)=(-1)^3=-1$ since $105=3\cdot 5\cdot 7$. The values of $\mu(n)$ for $n=1,2,\cdots,100$ can be found in table 3.1.

Note. Why do we care about Möbius? We can express long, ugly-looking, tedious sums into a very brief expression including sums over $\mu(n)$. If you feel comfortable with arithmetic functions so far, you might like to see an application of the Möbius function $\mu(n)$ in Theorem 4.3.3. You would be able to make sense of a beautiful application of this function.

Möbius function has amazing properties. The first is that it is multiplicative.

Proposition 3.3.2. *The Möbius function is multiplicative.*

Hint. Take $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ and $n=p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}$ and consider the factorization of the product mn. Use the definition of Möbius function to finish the proof.

n	$\mu(n)$	n	$\mu(n)$	n	$\mu(n)$	n	$\mu(n)$
1	1	26	1	51	1	76	0
2	−1	27	0	52	0	77	1
3	−1	28	0	53	−1	78	−1
4	0	29	−1	54	0	79	−1
5	−1	30	−1	55	1	80	0
6	1	31	−1	56	0	81	0
7	−1	32	0	57	1	82	1
8	0	33	1	58	1	83	−1
9	0	34	1	59	−1	84	0
10	1	35	1	60	0	85	1
11	−1	36	0	61	−1	86	1
12	0	37	−1	62	1	87	1
13	−1	38	1	63	0	88	0
14	1	39	1	64	0	89	−1
15	1	40	0	65	1	90	0
16	0	41	−1	66	−1	91	1
17	−1	42	−1	67	−1	92	0
18	0	43	−1	68	0	93	1
19	−1	44	0	69	1	94	1
20	0	45	0	70	−1	95	1
21	1	46	1	71	−1	96	0
22	1	47	−1	72	0	97	−1
23	−1	48	0	73	−1	98	0
24	0	49	0	74	1	99	0
25	0	50	0	75	0	100	0

Table 3.1: The Möbius function values for the first 100 positive integers.

You may be wonder why would someone define such a not-very-nice-looking function? What is the motivation behind Möbius function? In fact, this function is the *inverse* of a specific arithmetic function. Before going further, we must define the Dirichlet inverse of an arithmetic function.

Dirichlet Inverse Function. Let f be an arithmetic function. The arithmetic function g for which

$$f * g = \varepsilon$$

is called the *Dirichlet inverse* of f. The function g is often denoted by f^{-1}. You now see why we call ε the *unit* function. Back to our discussion: let f be an arithmetic function. Compute the Dirichlet product of f and constant 1 function and let the result be F, which is also an arithmetic function. By definition of convolution, we have

$$\begin{aligned} F(n) &= (f * 1)(n) \\ &= \sum_{d|n} f(d) \end{aligned}$$

This function F is called the *summatory function* of f. In number theory, there are times when we know what $F = f * 1$ is and we want to know what f is. This is where Möbius function comes in. Suppose that you do not know Möbius function, and you just define $\mu(n)$ as the Dirichlet inverse of $1(n)$. That is, you define $\mu(n)$ be a function such that $\mu * 1 = \varepsilon$. Then, multiply F by μ and use proposition 3.3.1 to get

$$\begin{aligned} F * \mu &= (f * 1) * \mu \\ &= f * (1 * \mu) \\ &= f * \varepsilon \\ &= f \end{aligned}$$

In other words, you just need to multiply F by μ to find f. So, we just need to find out what our defined function μ is. A few computations help us find μ, the Dirichlet inverse of 1. First, $(\mu * 1)(1) = \varepsilon(1) = 1$, which gives $\mu(1) = 1$. Let p be a prime and α be a positive integer. Then,

$$\begin{aligned} (\mu * 1)(p^\alpha) &= \varepsilon(p^\alpha) \\ &= 0 \end{aligned}$$

On the other hand, by definition of Dirichlet product and using the fact that the only divisors of p^α are $1, p, \cdots, p^\alpha$,

$$\begin{aligned} (\mu * 1)(p^\alpha) &= \sum_{d|p^\alpha} \mu(d) \\ &= \mu(1) + \mu(p) + \cdots + \mu(p^\alpha) \\ &= 0 \end{aligned}$$

Since we chose α arbitrarily, the equation $\mu(1)+\mu(p)+\cdots+\mu(p^\alpha)=0$ must be true for all values of α. For $\alpha=1$, we find $1+\mu(p)=0$, hence $\mu(p)=-1$. Similarly, for $\alpha\geq 2$, we find that $\mu(p^\alpha)=0$. Finally,

$$\mu(p^\alpha)=\begin{cases}1 & \text{if } \alpha=0\\ -1 & \text{if } \alpha=1\\ 0 & \text{if } \alpha\geq 2\end{cases}$$

The general definition of μ, as stated in definition 3.3, can be inferred from the above result using the fact that μ is a multiplicative function.

As you can observe, the μ function is defined to help us find an arithmetic function f given its summatory function F. In fact, $f=F*\mu$. This was first introduced by Möbius in 19^{th} century and is known as the *Möbius Inversion Formula*.

Theorem 3.3.3 (Möbius Inversion Formula). *If the summatory function of an arithmetic function f is $F(n)=\sum_{d\mid n}f(d)$, then*

$$f(n)=\sum_{d\mid n}\mu(d)F\left(\frac{n}{d}\right)$$

In other words, $f=\mu*F$.

When we first discussed Dirichlet inverse of a function, you might have wondered if this inverse always exists. The following theorem sheds light on this issue.

Theorem 3.3.4. *For an arithmetic function f with $f(1)\neq 0$, the Dirichlet inverse f^{-1} exists and is unique. In fact, f^{-1} can be defined recursively as*

$$f^{-1}(n)=\begin{cases}\dfrac{1}{f(1)} & \text{if } n=1\\[2ex] \dfrac{-1}{f(1)}\displaystyle\sum_{\substack{d\mid n\\ d<n}}f^{-1}(d)f\left(\frac{n}{d}\right) & \text{if } n>1\end{cases}$$

As discussed above, $\mu(n)$ is the Dirichlet inverse of the simplest arithmetic function, $1(n)$. The next theorem follows.

Theorem 3.3.5. *The Dirichlet inverse of the Möbius function is the constant 1 function. In other words, $1=\mu^{-1}$ or*

$$\sum_{d\mid n}\mu(n)=\varepsilon(n)$$

Theorem 3.3.6. *Let f be an arithmetic function and denote by F its summatory function. That is, for all positive integers n,*

$$F(n)=\sum_{d\mid n}f(d)$$

Then,

$$\sum_{k=1}^{n} F(k) = \sum_{k=1}^{n} f(k) \left\lfloor \frac{n}{k} \right\rfloor$$

Proof. By definition of F, we can write

$$\begin{aligned} \sum_{k=1}^{n} F(k) &= \sum_{k=1}^{n} \sum_{d|k} f(d) \\ &= \sum_{d|1} f(d) + \sum_{d|2} f(d) + \cdots + \sum_{d|n-1} f(d) + \sum_{d|n} f(d) \end{aligned}$$

In the last formula, $f(1)$ is repeated n times because 1 divides all integers. Also, $f(2)$ is repeated $\lfloor n/2 \rfloor$ times because there are exactly $\lfloor n/2 \rfloor$ numbers between 1 and n (inclusive) which are even. Analogously, there are exactly $\lfloor n/k \rfloor$ multiples of k ($1 \leq k \leq n$) in this interval and thus $f(k)$ is repeated $\lfloor n/k \rfloor$ times. The proof is complete. □

Example. According to Theorem 3.3.5, the summatory function of μ is ε. Therefore,

$$\sum_{k=1}^{n} \varepsilon(k) = \sum_{k=1}^{n} \mu(k) \left\lfloor \frac{n}{k} \right\rfloor$$

Since $\varepsilon(k)$ equals one when $k = 1$ and zero otherwise, the sum on the left side equals one. Consequently,

$$\sum_{k=1}^{n} \mu(k) \left\lfloor \frac{n}{k} \right\rfloor = 1$$

You can check the correctness of this formula by trying some small values for n.

§§3.4 More on Multiplicative Functions

The most interesting feature of Dirichlet product is that it preserves multiplicativity. That is, if two arithmetic functions are multiplicative, their Dirichlet product is also multiplicative. Before we prove this, we show a simple case. As we saw in previous sections, the summatory function F of an arithmetic function f is defined by $F = f * 1$. So, if f is multiplicative, so is F.

Theorem 3.4.1. *Let n be a positive integer with prime factorization $n = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$. If f is a multiplicative function with summatory function $F(n) = \sum_{d|n} f(d)$, then*

$$\begin{aligned} F(n) &= (1+f(p_1)+\ldots+f(p_1^{e_1}))\cdots(1+f(p_k)+\ldots+f(p_k^{e_k})) \\ &= \prod_{i=1}^{k}\sum_{j=0}^{e_i} f\left(p_i^j\right) \\ &= \prod_{i=1}^{k} F\left(p_i^{e_i}\right) \end{aligned} \tag{3.5}$$

Proof. The proof somewhat follows from the unique prime factorization. Assume T is the expansion of the right side of equation 3.5. If d is a divisor of n, then $d = p_1^{w_1}p_2^{w_2}\cdots p_k^{w_k}$, where $0 \le w_i \le e_i$ for $i = 1, 2, \cdots, k$. Therefore,

$$\begin{aligned} f(d) &= f\left(p_1^{w_1}p_2^{w_2}\cdots p_k^{w_k}\right) \\ &= f\left(p_1^{w_1}\right)f\left(p_2^{w_2}\right)\cdots f\left(p_k^{w_k}\right) \end{aligned}$$

which is a term that is present in T. Thus, we conclude that each term in the sum $F(n) = \sum_{d|n} f(d)$ appears in T. We can easily find that the converse is also true. After expanding the right side of equation 3.5, we see that every term in T is of the form

$$f\left(p_1^{w_1}\right)f\left(p_2^{w_2}\right)\cdots f\left(p_k^{w_k}\right)$$

where w_i are integers with $0 \le w_i \le e_i$ for all i. Since f is multiplicative, we can write this as

$$f\left(p_1^{w_1}p_2^{w_2}\cdots p_k^{w_k}\right)$$

which equals $f(d)$. Therefore, every term in T is also in $F(n)$. Combining these two, $T = F(n)$. □

Corollary 3.4.2. *If f is a non-zero multiplicative arithmetic function and $n = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ is the prime factorization of a positive integer n,*

$$\sum_{d|n}\mu(d)f(d) = \prod_{i=1}^{k}(1-f(p_i))$$

Theorem 3.4.3 (Multiplicative Function Theorem (MFT)). *Let f, g, and h be arithmetic functions.*

1. *If f and g are both multiplicative, then so is $f * g$.*
2. *If f is multiplicative, then so is its Dirichlet inverse.*
3. *If $f * g$ and f are both multiplicative, then so is g.*

Proof.

1. Let $f * g = h$. We need to prove that if a and b are co-prime positive integers, $h(ab) = h(a)h(b)$. We have

$$\begin{aligned} h(a)h(b) &= [(f*g)(a)] \cdot [(f*g)(b)] \\ &= \sum_{d_1 \mid a} f(d_1) g\left(\frac{a}{d_1}\right) \cdot \sum_{d_2 \mid b} f(d_2) g\left(\frac{b}{d_2}\right) \\ &= \sum_{d_1 \mid a, d_2 \mid b} f(d_1) f(d_2) g\left(\frac{a}{d_1}\right) g\left(\frac{b}{d_2}\right) \\ &= \sum_{d_1 \mid a, d_2 \mid b} f(d_1 d_2) g\left(\frac{ab}{d_1 d_2}\right) \\ &= \sum_{d \mid ab} f(d) g\left(\frac{ab}{d}\right) \\ &= (f*g)(ab) \\ &= h(ab) \end{aligned}$$

   which is what we wanted.

2. f is multiplicative, hence $f(mn) = f(m)f(n)$ for all co-prime positive integers m and n. Put $m = n = 1$ in this equation to get $f(1) = f(1)^2$, which immediately gives $f(1) = 1$ because f only accepts positive integer values. Let g be the Dirichlet inverse of f. By Theorem 3.3.4, $g(1) = 1$. We will prove by induction that g is multiplicative. The base case $n = 1$ is true. Suppose that $n > 1$ and whenever $ab < n$ with $(a, b) = 1$, then $g(ab) = g(a)g(b)$. Also, suppose that $xy = n$ with $(x, y) = 1$. We will show that $g(xy) = g(x)g(y)$. Since g is the inverse of f, we have $(f * g)(n) = \varepsilon(n)$. Also, $\varepsilon(n) = 0$ for $n > 1$. Therefore,

$$\begin{aligned} 0 &= \sum_{d \mid n} f(d) g\left(\frac{n}{d}\right) \\ &= \sum_{d \mid xy} f(d) g\left(\frac{xy}{d}\right) \\ &= g(xy) + \sum_{\substack{d \mid xy \\ d > 1}} f(d) g\left(\frac{xy}{d}\right) \end{aligned} \tag{3.6}$$

   The sum in equation 3.6 includes terms of te form $f(d)g(xy/d)$, and since d is larger than 1, xy/d is less than $xy = n$. Since $x \perp y$, there exist positive integers d_1 and d_2

such that $d = d_1 d_2$, $d_1 \mid x$, and $d_2 \mid y$. As a result,

$$\begin{aligned}
g(xy) &= -\sum_{\substack{d \mid xy \\ d>1}} f(d) g\left(\frac{xy}{d}\right) \\
&= -\sum_{\substack{d_1 \mid x, d_2 \mid y \\ d_1 d_2 > 1}} f(d_1 d_2) g\left(\frac{x}{d_1}\frac{y}{d_2}\right) \\
&= -\sum_{\substack{d_1 \mid x, d_2 \mid y \\ d_1 d_2 > 1}} f(d_1) f(d_2) g\left(\frac{x}{d_1}\right) g\left(\frac{y}{d_2}\right) \\
&= -\left[\sum_{d_1 \mid x, d_2 \mid y} f(d_1) f(d_2) g\left(\frac{x}{d_1}\right) g\left(\frac{y}{d_2}\right)\right] + g(x)g(y) \\
&= -\Bigg[\underbrace{\sum_{d_1 \mid x} f(d_1) g\left(\frac{x}{d_1}\right)}_{=(f*g)(x)} \underbrace{\sum_{d_2 \mid y} f(d_2) g\left(\frac{y}{d_2}\right)}_{=(f*g)(y)}\Bigg] + g(x)g(y) \\
&= -\left[(f*g)(x)\right]\left[(f*g)(y)\right] + g(x)g(y)
\end{aligned}$$

So, $g(xy) = -(f*g)(x) \cdot (f*g)(y) + g(x)g(y)$. Note that since $xy > 1$, at least one of x or y is larger than 1. Therefore, since g is the Dirichlet inverse of f, at least one of $(f*g)(x)$ or $(f*g)(y)$ is equal to zero. Finally, $g(xy) = g(x)g(y)$ and we are done.

3. Let $f*g = h$. Multiply both sides by f^{-1}, the Dirichlet inverse of f, to get $g = h*f^{-1}$ (why?). Multiplicativity of f implies the multiplicativity of f^{-1} by part 2. Now, from part 1, since both h and f^{-1} are multiplicative, their product, g must also be multiplicative.

□

Note. If two functions f and g are *completely* multiplicative, their Dirichlet product is multiplicative, but not necessarily completely multiplicative. An example would be $(1*1)(n) = \tau(n)$. Although the constant 1 function is completely multiplicative, the number of divisors function d is not.

The same is true for part 2: if f is completely multiplicative, then f^{-1} is multiplicative, but not in general completely multiplicative.

In proposition 2.3.3, we stated that Euler's totient function φ is multiplicative. We can now prove this result.

Proposition 3.4.4. *Prove that φ is multiplicative.*

Proof. As proved in Theorem 3.2.13, we know that $\varphi * 1 = \mathrm{id}$. Obviously, both $1(n)$ and $\mathrm{id}(n)$ are multiplicative. The conclusion follows from part 3 of Theorem 3.4.3. □

Although it is not always easy to find the Dirichlet inverse of an arithmetic function, there is an exception for completely multiplicative functions.

Theorem 3.4.5 (Inverse of Completely Multiplicative Functions). *Let f be a multiplicative function. Then f is completely multiplicative if and only if*

$$f^{-1}(n) = \mu(n)f(n)$$

for all $n \in \mathbb{N}$.

Note. Here, $\mu(n)f(n)$ is the *point-wise multiplication* of μ and f at point n. It is not to be confused with Dirichlet product $(\mu * f)(n)$.

Proof. First, if f is completely multiplicative, define $g(n) = \mu(n)f(n)$. Then, by definition of Dirichlet product,

$$\begin{aligned}(g*f)(n) &= \sum_{d|n} g(d)f\left(\frac{n}{d}\right)\\ &= \sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right)\\ &= \sum_{d|n} \mu(d)f\left(d\cdot\frac{n}{d}\right)\\ &= f(n)\sum_{d|n}\mu(d)\\ &= f(n)\varepsilon(n)\\ &= \varepsilon(n)\end{aligned}$$

The last equality holds because $f(1) = \varepsilon(1) = 1$ (why?) and $\varepsilon(n) = 0$ for all $n \geq 2$. This means that g is the Dirichlet inverse of f.

For the converse, suppose that $f^{-1}(n) = \mu(n)f(n)$ and we want to prove that f is completely multiplicative. It suffices to prove that $f(p^\alpha) = f(p)^\alpha$ for every prime p and any positive integer α (why?). We will proceed by induction. The base case $\alpha = 1$ is obvious. Suppose that we know $f(p^{\alpha-1}) = f(p)^{\alpha-1}$ and we want to show that $f(p^\alpha) = f(p)^\alpha$. For any $n \geq 2$, $(f*f^{-1})(n) = \varepsilon(n) = 0$. Therefore,

$$\sum_{d|n}\mu(d)f(d)f\left(\frac{n}{d}\right) = 0$$

Put $n = p^\alpha$ in the above equation to obtain

$$\begin{aligned}\sum_{d|p^\alpha}\mu(d)f(d)f\left(\frac{n}{d}\right) &= \mu(1)f(1)f(p^\alpha) + \mu(p)f(p)f(p^{\alpha-1}) + \cdots + \mu(p^\alpha)f(p^\alpha)f(1)\\ &= \mu(1)f(1)f(p^\alpha) + \mu(p)f(p)f(p^{\alpha-1})\\ &= f(p^\alpha) - f(p)f(p^{\alpha-1})\\ &= 0\end{aligned}$$

That is, $f(p^\alpha) = f(p)f(p^{\alpha-1})$. Using induction hypothesis, we immediately get the result. □

§§§3.4 More on τ

We provide two proofs for this theorem. The first one uses the concept of multiplicative functions discussed in previous sections. The second solution has a combinatorial spirit.

Proof. Since d is multiplicative, it suffices to find $\tau(n)$ only when n is a power of a prime. Let $n = p^\alpha$ for some prime p and a positive integer α. There exist $\alpha+1$ divisors $1, p, p^2, \cdots, p^\alpha$ for n. Therefore, $d(p^\alpha) = \alpha + 1$. To prove the theorem in the general case, take $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ and write

$$\begin{aligned} d(n) &= d(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) \\ &= d(p_1^{e_1}) d(p_2^{e_2}) \cdots d(p_k^{e_k}) \\ &= (e_1 + 1)(e_2 + 1) \cdots (e_k + 1) \\ &= \prod_{i=1}^{k} (1 + e_i) \end{aligned}$$

□

Example.

- $\tau(p) = 2$ for all primes p.
- $\tau(100) = \tau(2^2 \cdot 5^2) = (2 + 1)(2 + 1) = 9$.

Problem 3.4.6. Show that $1 = \tau * \mu$.

Solution. By Theorem 3.3.5, $1 * \mu = \varepsilon$. Multiply both sides of this equation by 1 and use the fact that $1 * 1 = \tau$, we find

$$\begin{aligned} \tau * \mu &= 1 * 1 * \mu \\ &= 1 * \varepsilon \\ &= \varepsilon \end{aligned}$$

As mentioned in section 3.2.1, the number of solutions to $ab = n$ in positive integers is $\tau(n)$. For the sake of completeness, we will state this result as a theorem.

Theorem 3.4.7. *Let n be a positive integer. The number of pairs (a, b) of positive integers which satisfy $ab = n$ is $\tau(n)$.*

Proof. First, if for some positive integers a and b the equation $ab = n$ holds, then a is a divisor of n. Second, for any divisor a of n, the number $b = n/a$ is an integer that satisfies $ab = n$. Therefore, $\tau(n)$ counts exactly all the solutions of $ab = n$. □

Here is a more interesting question:

Question 3.4.8. Let $x \geq 1$ be a *real* number. Find the number of pairs (a, b) of positive integers which satisfy

$$ab \leq x \tag{3.7}$$

n	$\tau(n)$
1	1
2	2
3	2
4	3
5	2
6	4
7	2
8	4
9	3
10	4

Table 3.2: Value of $\tau(n)$ for $n = 1, 2, \cdots, 10$.

One way to answer this question is to break the condition $ab \leq x$ into smaller conditions. Obviously, the equation $ab = y$ does not have any solutions in integers if y is not an integer. So, in order to find the number of solutions to the inequality 3.7, we only need to find the number of solutions to each of $ab = 1, ab = 2, \cdots, ab = \lfloor x \rfloor$ and the answer would be the sum of these numbers. According to Theorem 3.4.7, the answer is

$$\tau(1) + \tau(2) + \cdots + \tau(\lfloor x \rfloor)$$

We are seeking a way to determine this sum.

Definition. Let $x \geq 1$ be a real number. Denote by $T(x)$ the number of positive integer solutions to $ab \leq x$.

From what we have already found,

$$T(x) = \sum_{k=1}^{\lfloor x \rfloor} \tau(k) \tag{3.8}$$

Example. Let us find $T(10.2)$. We need to compute $\tau(1), \tau(2), \cdots, \tau(10)$. According to table 3.2 and equation 3.8, $T(10.2)$ is equal to the sum of numbers in the second column, which is 27.

As you observe in the above example, it would be a tedious job to calculate $T(x)$ by summing up the τ values. There is another way to compute $T(x)$. Let a be a fixed positive integer. The inequality $ab \leq x$ is equivalent to

$$b \leq \frac{x}{a}$$

Since b is a positive integer, it can take the values $1, 2, \cdots, \lfloor \frac{x}{a} \rfloor$. These are $\lfloor \frac{x}{a} \rfloor$ numbers. Since a can take all the values $1, 2, \cdots, \lfloor x \rfloor$, we have

$$T(x) = \left\lfloor \frac{x}{1} \right\rfloor + \left\lfloor \frac{x}{2} \right\rfloor + \cdots + \left\lfloor \frac{x}{\lfloor x \rfloor} \right\rfloor$$

Example. Let us calculate $T(10.2)$ with the new approach. We have

$$\begin{aligned} T(10.2) &= \left\lfloor \frac{10.2}{1} \right\rfloor + \left\lfloor \frac{10.2}{2} \right\rfloor + \cdots + \left\lfloor \frac{10.2}{10} \right\rfloor \\ &= 10 + 5 + 3 + 2 + 2 + 1 + 1 + 1 + 1 + 1 \\ &= 27 \end{aligned}$$

which is in agreement with our previous result.

The formula

$$T(x) = \sum_{k=1}^{\lfloor x \rfloor} \left\lfloor \frac{x}{k} \right\rfloor \tag{3.9}$$

is more convenient than 3.8. That is, we can find $T(x)$ using equation 3.9 with less number of calculations. In fact, to compute $T(x)$ from 3.8, we need to calculate the number of divisors of $\lfloor x \rfloor$ numbers, which obviously needs more computations than $\lfloor x \rfloor$ computations needed in formula 3.9. However, this can be refined even more.

We will divide the solutions to $ab \leq x$ into two classes. The first class includes solutions in which $a \leq \sqrt{x}$ and the second one includes all solutions such that $a > \sqrt{x}$. Let $T_1(x)$ be the number of solutions in the first class and let $T_2(x)$ be that of the second class. Therefore,

$$T(x) = T_1(x) + T_2(x)$$

For the first class of solutions, let us consider $1 \leq a \leq \sqrt{x}$ is a fixed integer. The inequality $ab \leq x$, can be written as $b \leq \frac{x}{a}$. Therefore, in order to satisfy $ab \leq x$, b can take only the values $1, 2, \cdots, \lfloor \frac{x}{a} \rfloor$, which are $\lfloor \frac{x}{a} \rfloor$ different numbers. Keeping in mind that a can take the values $1, 2, \cdots, \lfloor \sqrt{x} \rfloor$, the number of solutions in the first class is

$$T_1(x) = \sum_{a=1}^{\lfloor \sqrt{x} \rfloor} \left\lfloor \frac{x}{a} \right\rfloor$$

For the second class, we must find how many pairs (a, b) of integers satisfy the following inequalities:

$$\begin{aligned} ab &\leq x \\ a &> \sqrt{x} \end{aligned}$$

This can be written as

$$\sqrt{x} < a \leq \frac{x}{b}$$

Obviously, since the product of a and b is less than or equal to x and $a > \sqrt{x}$, we must have $b \leq \sqrt{x}$ (otherwise ab would be larger than x). Fix b. The only possible values for a are

$$\lfloor \sqrt{x} \rfloor + 1, \lfloor \sqrt{x} \rfloor + 2, \cdots, \left\lfloor \frac{x}{b} \right\rfloor$$

These are $\left\lfloor \frac{x}{b} \right\rfloor - \lfloor \sqrt{x} \rfloor$ numbers. So, since b can take all values $1, 2, \cdots, \lfloor \sqrt{x} \rfloor$, we have

$$T_2(x) = \sum_{b=1}^{\lfloor \sqrt{x} \rfloor} \left(\left\lfloor \frac{x}{b} \right\rfloor - \lfloor \sqrt{x} \rfloor \right) \tag{3.10}$$

In order to add $T_1(x)$ and $T_2(x)$ to obtain $T(x)$, we have to make their summation parameter the same. We already know that changing the summation parameter does not change the value of the sum. Therefore, we can change b to a in equation 3.10 and write $T_2(x)$ as

$$T_2(x) = \sum_{a=1}^{\lfloor \sqrt{x} \rfloor} \left(\left\lfloor \frac{x}{a} \right\rfloor - \lfloor \sqrt{x} \rfloor \right)$$

We can now add up $T_1(x)$ and $T_2(x)$ and write

$$\begin{aligned} T(x) &= T_1(x) + T_2(x) \\ &= \sum_{a=1}^{\lfloor \sqrt{x} \rfloor} \left\lfloor \frac{x}{a} \right\rfloor + \left(\sum_{a=1}^{\lfloor \sqrt{x} \rfloor} \left(\left\lfloor \frac{x}{a} \right\rfloor - \lfloor \sqrt{x} \rfloor \right) \right) \\ &= 2 \sum_{a=1}^{\lfloor \sqrt{x} \rfloor} \left\lfloor \frac{x}{a} \right\rfloor - \left(\underbrace{\lfloor \sqrt{x} \rfloor + \lfloor \sqrt{x} \rfloor + \cdots + \lfloor \sqrt{x} \rfloor}_{\lfloor \sqrt{x} \rfloor \text{ times}} \right) \\ &= 2 \sum_{a=1}^{\lfloor \sqrt{x} \rfloor} \left\lfloor \frac{x}{a} \right\rfloor - \lfloor \sqrt{x} \rfloor^2 \end{aligned}$$

Finally, we have the formula

$$T(x) = 2 \sum_{a=1}^{\lfloor \sqrt{x} \rfloor} \left\lfloor \frac{x}{a} \right\rfloor - \lfloor \sqrt{x} \rfloor^2 \tag{3.11}$$

Equation 3.11 needs $\lfloor \sqrt{x} \rfloor$ computations to calculate $T(x)$, which is obviously less than $\lfloor x \rfloor$ computations needed to find $T(x)$ from 3.9.

Example. We will calculate the number of positive integer solutions to $ab \leq 100.2$. Since $x = 100.2$ is large in this case, the best way to calculate $T(x)$ is from formula 3.11. We find

$$\begin{aligned} T(100.2) &= 2 \sum_{a=1}^{10} \left\lfloor \frac{100.2}{a} \right\rfloor - 100 \\ &= 2\,(100 + 50 + 33 + 25 + 20 + 16 + 14 + 12 + 11 + 10) - 100 \\ &= 482 \end{aligned}$$

Theorem 3.4.9 (An Approximation for Average Value of $\tau(n)$). *Let n be a positive integer. Prove that*

$$\frac{\tau(1) + \tau(2) + \cdots + \tau(n)}{n} = \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n} - e$$

where e is a number between zero and one.

Proof. Assuming $x = n$, we employ equations 3.8 and 3.9 to write

$$\sum_{k=1}^{n} \tau(k) = \sum_{k=1}^{n} \left\lfloor \frac{n}{k} \right\rfloor$$

The right hand side of the above equation can be written as

$$\sum_{k=1}^{n} \left\lfloor \frac{n}{k} \right\rfloor = \sum_{k=1}^{n} \left(\frac{n}{k} - \left\{ \frac{n}{k} \right\} \right)$$

where $\{n/k\}$ is the fractional part of n/k. Therefore,

$$\sum_{k=1}^{n} \tau(k) = \sum_{k=1}^{n} \frac{n}{k} - \sum_{k=1}^{n} \left\{ \frac{n}{k} \right\} \tag{3.12}$$

Dividing both sides of this last equation by n, we find

$$\frac{\sum_{k=1}^{n} \tau(k)}{n} = \sum_{k=1}^{n} \frac{1}{k} - \frac{\sum_{k=1}^{n} \left\{ \frac{n}{k} \right\}}{n} \tag{3.13}$$

We already know that $0 \leq \{n/k\} < 1$. Therefore, the second sum in the right hand side of equation 3.12 is between zero and n. Therefore,

$$0 < \frac{\sum_{k=1}^{n} \{n/k\}}{n} < 1$$

(it is never equal to zero, can you see why?). The proof is complete. □

Note. This theorem states that the average value of number-of-divisors function (i.e., $[\tau(1) + \tau(2) + \cdots + \tau(n)]/n$) is approximately equal to sum of reciprocals of positive integers up to n. We represent this as

$$\frac{\tau(1) + \tau(2) + \cdots + \tau(n)}{n} \sim \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n}$$

§§§3.4 More on σ and its Generalization

Let us prove that σ is multiplicative.

Proposition 3.4.10. *The sum-of-divisors function σ is a multiplicative arithmetic function.*

Proof. If you look more closely, you will observe that

$$\begin{aligned}\sigma(n) &= \sum_{d|n} d \\ &= \sum_{d|n} d \cdot 1\left(\frac{n}{d}\right) \\ &= (\mathrm{id} * 1)(n)\end{aligned}$$

Now, since both id and constant 1 function are multiplicative, part 1 of Theorem 3.4.3 implies that σ is also multiplicative. □

Problem 3.4.11. Prove that for two positive integers a and b, if $a \mid b$, then

$$\frac{\sigma(a)}{a} \leq \frac{\sigma(b)}{b}$$

Solution. Let $b = \prod_{p|b} p^e$ be the prime factorization of b. Then, since $a \mid b$, the factorization of a would be $a = \prod_{p|b} p^f$ with $0 \leq f \leq e$ for each prime p dividing b. From Theorem 3.2.7,

$$\sigma(b) = \prod_{p|b} \frac{p^{e+1}-1}{p-1}$$

$$\sigma(a) = \prod_{p|b} \frac{p^{f+1}-1}{p-1}$$

Thus, we need to show that

$$\prod_{p|b} \frac{p^{f+1}-1}{p^f(p-1)} \leq \prod_{p|b} \frac{p^{e+1}-1}{p^e(p-1)}$$

Now it suffices to prove that

$$\begin{aligned}&\frac{p^{e+1}-1}{p^e(p-1)} \geq \frac{p^{f+1}-1}{p^f(p-1)} \\ \iff\ & p^{e+f+1}(p-1) - p^f(p-1) \geq p^{e+f+1}(p-1) - p^e(p-1) \\ \iff\ & p^e(p-1) \geq p^f(p-1)\end{aligned}$$

which is true since $e \geq f$.

Proposition 3.4.12. *Let n be a composite positive integer. Prove that $\sigma(n) > n + \sqrt{n}$.*

Proof. Since n is composite, we know from proposition 1.1.12 that n has a prime factor p less than or equal to $\sqrt{n}$. Then, n/p is a divisor of n and $n/p \geq \sqrt{n}$. Since n has at least three divisors n, n/p, and 1,

$$\begin{aligned}\sigma(n) &\geq n + \frac{n}{p} + 1 \\ &\geq n + \sqrt{n} + 1 \\ &> n + \sqrt{n}\end{aligned}$$

□

Theorem 3.4.13. *Let $k > 1$ be a given positive integer. Show that the equation*

$$\sigma(n) = n + k$$

has a finite number of solutions for n.

Proof. Suppose that $\sigma(n) = n + k$ holds for some positive integer n. Since $k > 1$, n must be composite (otherwise $\sigma(n) = n + 1$). According to theorem 3.4.12, $\sigma(n) > n + \sqrt{n}$. As a result, we find $\sqrt{n} < k$ or $n < k^2$. Obviously, there are at most k^2 values $1, 2, \cdots, k^2$ possible for n. This finishes the proof. □

Theorem 3.4.14. *Let k be an arbitrary positive integer. Show that there exists a positive integer n_0 such that for any $n > n_0$,*

$$\frac{\sigma(n!)}{n!} > k$$

In other words, prove that

$$\lim_{n\to\infty} \frac{\sigma(n!)}{n!} = \infty$$

Proof. According to Theorem 3.2.6,

$$\frac{\sigma(n!)}{n!} = \sum_{d|n!} \frac{1}{d}$$

Since $1, 2, \cdots, n$ all divide $n!$, we can write

$$\begin{aligned}\frac{\sigma(n!)}{n!} &= \sum_{d|n!} \frac{1}{d} \\ &> \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n}\end{aligned}$$

It suffices to find an n such that

$$\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n} > k$$

Take $n = 2^{2k}$. Then,

$$\begin{aligned}\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{2^{2k}} &> 1 + \frac{1}{2} + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) \\ &\quad + \cdots + \left(\underbrace{\frac{1}{2^{2k}} + \frac{1}{2^{2k}} + \cdots + \frac{1}{2^{2k}}}_{2^{2k-1}\text{ times}}\right) \\ &> 1 + 2k\left(\frac{1}{2}\right) \\ &= 1 + k \\ &> k\end{aligned}$$

as desired. □

Theorem 3.4.15. *$\sigma(n)$ is odd if and only if $n = k^2$ or $n = 2k^2$ for some integer k.*

Proof. Let $n = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ be the factorization of n and suppose that $\sigma(n)$ is odd. We will prove that n is either a perfect square or twice a perfect square. According to Theorem 3.2.7, since $\sigma(n)$ is odd, all the terms in the product $\prod_{i=1}^{k}\frac{p_i^{e_i+1}-1}{p-1}$ must be odd. That is,

$$1 + p_i + p_i^2 + \cdots + p_i^{e_i} \tag{3.14}$$

must be odd for $i = 1, 2, \cdots, k$. There are two cases: if $p_i \neq 2$ for all i, then the number of terms in the expression 3.14 must be odd so that their sum is also odd (they are all odd). That is, e_i must be even for $i = 1, 2, \cdots, k$. Hence, n is a perfect square.

The other case is when some p_i, say p_1 is equal to 2. The expression 3.14 is odd for $p_1 = 2$. Now, in order for expression 3.14 to be odd, all e_i must be even for $2 \leq i \leq k$ (exactly like the previous case). Now, if the power of 2 that divides n is even, n is of the form k^2 and if it is odd, n is of the form $2k^2$.

The proof of the converse is now obvious. □

Corollary 3.4.16. *If n is an odd positive integer, then n is a square if and only if $\sigma(n)$ is odd.*

Proposition 3.4.17. *Let n be a positive integer. The number of positive integers less than or equal to n with even sum of divisors is*

$$n - \lfloor\sqrt{n}\rfloor - \left\lfloor\sqrt{\frac{n}{2}}\right\rfloor$$

Proof. There are n positive integers less than or equal to n. We know from Theorem 3.4.15 that numbers that are a perfect square or twice a perfect square have an even σ. The number of perfect squares less than or equal to n is $\lfloor\sqrt{n}\rfloor$ (why?). Similarly, the number of integers less than or equal to n that is twice a perfect square is $\lfloor\sqrt{n/2}\rfloor$. The conclusion follows. □

A family of numbers that are related to the sum of divisors function are *perfect numbers*.

Definition. A positive integer n is a *perfect number* if $\sigma(n) = 2n$.

Example. The only perfect numbers less than 10^4 are $6, 28, 496$, and 8128.

Theorem 3.4.18. *Let $k > 1$ be a positive integer. If $2^k - 1$ is a prime number, then $2^{k-1}(2^k - 1)$ is a perfect number. Also, every even perfect number has this form.*

Proof. First, suppose that $p = 2^k - 1$ is a prime. We will prove that $n = 2^{k-1}(2^k - 1)$ is perfect. Notice that $\sigma(p) = p + 1 = 2^k$ and since σ is multiplicative,

$$\begin{aligned}
\sigma(n) &= \sigma\left(2^{k-1}(2^k - 1)\right) \\
&= \sigma(2^{k-1})\sigma(p) \\
&= \left(1 + 2 + 2^2 + \cdots + 2^{k-1}\right)\left(2^k\right) \\
&= \left(2^k - 1\right)2^k \\
&= 2n
\end{aligned}$$

Now, suppose that n is an even perfect number. We want to show that it is of the form $2^{k-1}(2^k-1)$. We will use the trick stated in Theorem 1.5.3. One can write n as $2^k s$ for a positive integer k and an odd integer s. Again by multiplicativity of σ,

$$\begin{aligned}\sigma(n) &= \sigma(2^k s)\\ &= \sigma(2^k)\sigma(s)\\ &= \left(2^{k+1}-1\right)\sigma(s)\end{aligned}$$

On the other hand, as n is a perfect number, $\sigma(n) = 2n = 2^{k+1}s$. Therefore,

$$2^{k+1}s = \left(2^{k+1}-1\right)\sigma(s) \tag{3.15}$$

This means that $2^{k+1}-1$ divides $2^{k+1}s$, but since $(2^{k+1}, 2^{k+1}-1) = 1$, we have $2^{k+1}-1 \mid s$. Consequently, there exists an integer t such that $s = \left(2^{k+1}-1\right)t$. Substituting this in equation 3.15, one realizes that

$$\begin{aligned}2^{k+1}t &= \sigma(s)\\ &\geq s+t\\ &= 2^{k+1}t\end{aligned}$$

Therefore, $\sigma(s) = s+t$. It means that s must be a prime and its only divisors are itself (s) and one (t) (why?). Hence $n = 2^k(2^{k+1}-1)$, $2^{k+1}-1$ is a prime, and n has the desired form. □

Remark. We do not know whether there exist infinitely many perfect numbers. In fact, even perfect numbers are formed by *Mersenne primes* (see Theorem 1.5.22 and its remark), and it has not yet been proved that there are infinitely many Mersenne primes. Furthermore, it is not known whether there are any odd perfect numbers. Mathematicians have tested the first 10^{1500} natural numbers but did not find any odd perfect number among them, so they guess there probably does not exist any.

Theorem 3.4.19. *Let n be a positive integer. Then, $\sigma(n)$ is a power of 2 if and only if n is a product of some Mersenne primes.*

Proof. It is obvious that sum of divisors of the product of some Mersenne primes is a power of 2 (prove it yourself). We will now show that if $\sigma(n) = 2^k$ for some natural k, then n is a product of Mersenne primes. Let $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_m^{\alpha_m}$ be the prime factorization of n. Since σ is multiplicative, $\sigma(p_i^{\alpha_i})$ must be a power of 2 for $i = 1, 2, \cdots, m$. Therefore, it suffices to prove that if for a prime p and a positive integer α, $\sigma(p^\alpha) = 2^k$, then p is a Mersenne prime and $\alpha = 1$. The only divisors of p^α are $1, p, p^2, \cdots, p^\alpha$, so,

$$2^k = 1 + p + p^2 + \cdots + p^\alpha$$

This means that α is odd. Take $\alpha = 2\beta + 1$. Then we can factorize the right hand side as

$$2^k = (1+p)\left(1 + p^2 + p^4 + \cdots + p^{2\beta}\right) \tag{3.16}$$

This leads us to the conclusion that $1+p$ is a power of 2, which means p is a Mersenne prime. Now suppose that $\alpha > 1$. From equation 3.16, we observe that β must be odd. Take $\beta = 2\gamma + 1$ and write

$$\begin{aligned} 2^t &= 1 + p^2 + p^4 + \cdots + p^{2\beta} \\ &= \left(1 + p^2\right)\left(1 + p^4 + p^8 + \cdots + p^{4\gamma}\right) \end{aligned}$$

for some natural t. This means that $1+p^2$ is a power of 2. However, since p is a Mersenne prime, there exists some s for which $p = 2^s - 1$. Therefore,

$$\begin{aligned} 1 + p^2 &= 1 + (2^s - 1)^2 \\ &= 2 + 2^{2s} - 2^{s+1} \end{aligned}$$

But this last expression is not divisible by 4 and cannot be a power of 2. This is a contradiction. Thus, $a = 1$ and we are done. □

Problem 3.4.20. Prove that for any positive integer n,

$$\left| \sum_{d|n} \frac{\mu(d)\sigma(d)}{d} \right| \geq \frac{1}{n}$$

Solution. Let $f(n) = \mu(n)\sigma(n)/n$. Sine all three functions μ, σ, and id are multiplicative, so is f. Theorem 3.4.1 implies that the summatory function of f is also multiplicative. Therefore, it suffices to prove the given inequality only when $n = p^\alpha$, where p is a prime and α is a positive integer. Since $\mu(p^x)$ is zero for $x \geq 2$, $\mu(1) = 1$, and $\mu(p) = -1$,

$$\begin{aligned} \left| \sum_{d|p^\alpha} \frac{\mu(d)\sigma(d)}{d} \right| &= \left| \frac{\mu(1)\sigma(1)}{1} + \frac{\mu(p)\sigma(p)}{p} + \cdots + \frac{\mu(p^\alpha)\sigma(p^\alpha)}{p^\alpha} \right| \\ &= \left| \frac{\mu(1)\sigma(1)}{1} + \frac{\mu(p)\sigma(p)}{p} \right| \\ &= \left| \frac{1}{1} - \frac{p+1}{p} \right| \\ &= \frac{1}{p} \\ &\geq \frac{1}{p^\alpha} \end{aligned}$$

The reader is supposed to draw the conclusion and finish the proof.

We can generalize the concept of number-of-divisors and sum-of-divisors functions to define *divisor functions*.

Definition. Let n be a positive integer and $\alpha \geq 0$ be an integer[7]. The sum of α^{th} powers of positive divisors of n is denoted by $\sigma_\alpha(n)$. In other words,

$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha$$

[7]More generally, one can assume that α is any non-negative real number.

The functions σ_α are called *divisor functions*. According to this definition, the number-of-divisors function τ is equal to σ_0 and the sum-of-divisors function σ is equal to σ_1.

Theorem 3.4.21 (Properties of Divisor Functions). *For every non-negative integer α and positive integer n,*

1. *σ_α is multiplicative (but not completely multiplicative),*
2. *$\sigma_\alpha = 1 * id^\alpha$,*
3. *if α is non-zero and $n = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ is the prime factorization of n,*

$$\begin{aligned}\sigma_\alpha(n) &= \prod_{i=1}^{k}\frac{p_i^{\alpha(e_i+1)}-1}{p-1}\\ &= \prod_{i=1}^{k}\left(1+p_i^\alpha+p_i^{2\alpha}+\cdots+p_i^{a_i\alpha}\right)\end{aligned}$$

4. *the Dirichlet inverse of σ_α is obtained by*

$$\sigma_\alpha^{-1}(n) = \sum_{d\mid n} d^\alpha \mu(d)\mu\left(\frac{n}{d}\right)$$

Proof. We only prove parts 2 and 4.

2. Notice that

$$\begin{aligned}(1*\mathrm{id}^\alpha)(n) &= (\mathrm{id}^\alpha * 1)(n)\\ &= \sum_{d\mid n}\mathrm{id}^\alpha(d)\cdot 1\left(\frac{n}{d}\right)\\ &= \sum_{d\mid n} d^\alpha\\ &= \sigma_\alpha(n)\end{aligned}$$

4. From Theorem 3.4.5, sine the function id^α is completely multiplicative, its Dirichlet inverse is $\mu\,\mathrm{id}^\alpha$. Hence, from part 2 of this theorem,

$$\begin{aligned}(\sigma_\alpha^{-1})(n) &= \left(1*\mathrm{id}^\alpha\right)^{-1}(n)\\ &= \left(1^{-1}*\left(\mathrm{id}^\alpha\right)^{-1}\right)(n)\\ &= \left(\mu*\mu\,\mathrm{id}^\alpha\right)(n)\\ &= \sum_{d\mid n} d^\alpha\mu(d)\mu\left(\frac{n}{d}\right)\end{aligned}$$

□

§§§3.4 More on $\varphi(n)$ and $J_k(n)$

Theorem 3.4.22. *Let n be a positive integer. Prove that*

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$$

Proof. Let $f(n) = \varphi(n)$. By Theorem 3.2.13, we know that $F(n) = \sum_{d|n} \varphi(d) = n$. Therefore, by Möbius inversion formula,

$$\begin{aligned} \varphi(n) = f(n) &= \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \mu(d) \left(\frac{n}{d}\right) \\ &= n \sum_{d|n} \frac{\mu(d)}{d} \end{aligned}$$

as desired. □

Corollary 3.4.23. $\varphi = \mu * id$.

In Theorem 3.2.13, we proved that $\sum_{d|n} \varphi(d) = n$. We will now prove that the converse of this theorem is also true. That is, φ is the only arithmetic function with this property.

Theorem 3.4.24. *If f is an arithmetic function such that for all $n \in \mathbb{N}$,*

$$\sum_{d|n} f(d) = n$$

then $f(n) = \varphi(n)$ for all $n \in \mathbb{N}$.

Proof. By Möbius inversion formula, $f = \mu * F$, where $F(n) = \sum_{d|n} f(d)$. So, in this case $f = \mu * \mathrm{id}$. On the other hand, we already know from corollary 3.4.23 that $\varphi = \mu * \mathrm{id}$. Thus, $f = \varphi$. □

Theorem 3.4.25. *Let n be a positive integer. Prove that*

1. $\sum_{d|n} \mu(d)\varphi(d) = \prod_{p|n} (2 - p)$
2. $\sum_{d|n} \mu(d)^2 \varphi(d)^2 = \prod_{p|n} (1 + (p-1)^2)$

3. $\displaystyle\sum_{d|n}\frac{\mu(d)}{\varphi(d)}=\prod_{p|n}\left(1-\frac{1}{p-1}\right)$

Proof. We will only prove 1 here. The other two parts are similar. Let $f(n)=\mu(n)\varphi(n)$. Since μ and φ are both multiplicative, their product f is also multiplicative. By Theorem 3.4.1, the summatory function of f is multiplicative as well. Therefore, it suffices to find the sum $F(n)=\sum_{d|n}\mu(d)\varphi(d)$ only when n is a power of a prime. Let $n=p^\alpha$. Then, since $\mu(p^\beta)=0$ for integer $\beta>1$,

$$\begin{aligned}\sum_{d|p^\alpha}\mu(d)\varphi(d)&=\mu(1)\varphi(1)+\mu(p)\varphi(p)+\cdots+\mu(p^\alpha)\varphi(p^\alpha)\\&=\mu(1)\varphi(1)+\mu(p)\varphi(p)\\&=1-(p-1)\\&=2-p\end{aligned}$$

Suppose that $n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ is the prime factorization of n. Then, again by Theorem 3.4.1,

$$\begin{aligned}\sum_{d|n}\mu(d)\varphi(d)&=\prod_{i=1}^{k}\sum_{j=0}^{e_i}\mu(d)\varphi(d)\\&=\prod_{i=1}^{k}(2-p_i)\end{aligned}$$

□

Theorem 3.4.26. *Let n be a composite integer larger than 6. Then,*

$$\varphi(n)\le n-\sqrt{n}$$

Proof. Let $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ be the prime factorization of n. Since n is composite, we get from proposition 1.1.12 that it must have a prime factor, say p_1, which is less than or equal to $\sqrt{n}$. Then, using the formula in part (d) of Theorem 3.2.11,

$$\begin{aligned}\varphi(n)&=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)\\&\le n\left(1-\frac{1}{p_1}\right)\\&\le n\left(1-\frac{1}{\sqrt{n}}\right)\\&=n-\sqrt{n}\end{aligned}$$

□

Theorem 3.4.27. *Let k be an arbitrary positive integer. Show that there exists a positive integer n_0 such that for any $n > n_0$,*

$$\varphi(n) > k$$

In other words, prove that $\lim_{n\to\infty} \varphi(n) = \infty$.

Proof. We will prove that $\varphi(n) \geq \frac{\sqrt{n}}{2}$ and the result immediately follows. First, suppose that n is odd. Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be the prime factorization of n. Then, because of the fact that p_i are primes larger than 2, $1 \leq i \leq k$, we can use the inequality $p_i - 1 \geq p_i^{1/2}$ (prove it yourself) to write

$$\begin{aligned}\varphi(n) &= p_1^{\alpha_1-1} p_2^{\alpha_2-1} \cdots p_k^{\alpha_k-1} (p_1 - 1) \cdots (p_k - 1) \\ &\geq p_1^{\alpha_1-1} p_2^{\alpha_2-1} \cdots p_k^{\alpha_k-1} \cdot p_1^{1/2} p_2^{1/2} \cdots p_k^{1/2} \\ &\geq p_1^{\alpha_1-1/2} p_2^{\alpha_2-1/2} \cdots p_k^{\alpha_k-1/2}\end{aligned}$$

Now, since α_i is a positive integer for all i, the inequality $\alpha_i - 1/2 \geq \alpha_i/2$ holds true. Hence,

$$\begin{aligned}\varphi(n) &\geq p_1^{\alpha_1-1/2} p_2^{\alpha_2-1/2} \cdots p_k^{\alpha_k-1/2} \\ &\geq p_1^{\alpha_1/2} p_2^{\alpha_2/2} \cdots p_k^{\alpha_k/2} \\ &= \sqrt{n}\end{aligned}$$

For even n, let $n = 2^\alpha t$ for some positive integer α and odd t. Then, $\varphi(n) = \varphi(2^\alpha)\varphi(t)$. Since t is odd, we already know that $\varphi(t) \geq \sqrt{t}$. Thus,

$$\begin{aligned}\varphi(n) &= \varphi(2^\alpha)\varphi(t) \\ &= 2^{\alpha-1}\varphi(t) \\ &\geq 2^{\alpha-1}\sqrt{t} \\ &\geq 2^{\alpha/2-1}\sqrt{t} \\ &= \frac{1}{2}2^{\alpha/2}\sqrt{t} \\ &= \frac{1}{2}\sqrt{n}\end{aligned}$$

Consequently, $\varphi(n) \geq \frac{\sqrt{n}}{2}$ for all positive integers n. To finish the proof, select $n_0 = 4k^2$ so that for any $n > n_0$,

$$\begin{aligned}\varphi(n) &\geq \frac{1}{2}\sqrt{n} \\ &> \frac{1}{2}\sqrt{n_0} \\ &= k\end{aligned}$$

□

Corollary 3.4.28. *Let k be an arbitrary integer. The number of positive integers n for which $\varphi(n) = k$ is finite.*

Theorem 3.4.29. *Let n be a positive integer. Then,*

$$\sum_{k=1}^{n} \varphi(k) = \frac{1}{2} + \frac{1}{2} \sum_{k=1}^{n} \mu(k) \left\lfloor \frac{n}{k} \right\rfloor^2$$

Proof. Define

$$f(n) = \frac{1}{2} \sum_{k=1}^{n} \mu(k) \left\lfloor \frac{n}{k} \right\rfloor^2$$

Then, from Theorem 1.4.5,

$$\begin{aligned} f(n+1) - f(n) &= \frac{1}{2} \sum_{k=1}^{n+1} \mu(k) \left\lfloor \frac{n+1}{k} \right\rfloor^2 - \frac{1}{2} \sum_{k=1}^{n} \mu(k) \left\lfloor \frac{n}{k} \right\rfloor^2 \\ &= \frac{1}{2} \sum_{k=1}^{n+1} \mu(k) \left(\left\lfloor \frac{n+1}{k} \right\rfloor^2 - \left\lfloor \frac{n}{k} \right\rfloor^2 \right) \\ &= \frac{1}{2} \sum_{k \mid (n+1)} \mu(k) \left(2\frac{n+1}{k} - 1 \right) \\ &= (n+1) \sum_{k \mid (n+1)} \frac{\mu(k)}{k} - \frac{1}{2} \sum_{k \mid (n+1)} \mu(k) \end{aligned}$$

By Theorem 3.4.22, the first term in the last line of above equations equals $\varphi(n+1)$, and by Theorem 3.3.5, the second term is $\frac{1}{2}\varepsilon(n+1)$. Therefore,

$$f(n+1) - f(n) = \varphi(n+1) - \frac{1}{2}\varepsilon(n+1)$$

Now, from Sum of Differences,

$$\begin{aligned}
\frac{1}{2}\sum_{k=1}^{n}\mu(k)\left\lfloor\frac{n}{k}\right\rfloor^2 &= f(n)\\
&= f(1)+\sum_{k=1}^{n-1}(f(k+1)-f(k))\\
&= \frac{1}{2}+\sum_{k=1}^{n-1}\left(\varphi(k+1)-\frac{1}{2}\varepsilon(k+1)\right)\\
&= \frac{1}{2}+\sum_{k=1}^{n-1}\varphi(k+1)-\frac{1}{2}\underbrace{\sum_{k=1}^{n-1}\varepsilon(k+1)}_{=0}\\
&= \frac{1}{2}+\sum_{k=1}^{n-1}\varphi(k+1)\\
&= \frac{1}{2}+\sum_{k=1}^{n}\varphi(k)-\varphi(1)\\
&= \sum_{k=1}^{n}\varphi(k)-\frac{1}{2}
\end{aligned}$$

The proof is complete. □

Theorem 3.4.30. *For all positive integers n,*

$$\sum_{k=1}^{n}\frac{\varphi(k)}{k}=\sum_{k=1}^{n}\frac{\mu(k)}{k}\left\lfloor\frac{n}{k}\right\rfloor$$

First Proof. In an analogous way to the proof of previous theorem, we use Theorem 1.4.5. Define $f(n)=\sum_{k=1}^{n}\frac{\mu(k)}{k}\left\lfloor\frac{n}{k}\right\rfloor$. In this case,

$$\begin{aligned}
f(n+1)-f(n) &= \sum_{k=1}^{n+1}\frac{\mu(k)}{k}\left\lfloor\frac{n+1}{k}\right\rfloor-\sum_{k=1}^{n}\frac{\mu(k)}{k}\left\lfloor\frac{n}{k}\right\rfloor\\
&= \sum_{k=1}^{n+1}\frac{\mu(k)}{k}\left(\left\lfloor\frac{n+1}{k}\right\rfloor-\left\lfloor\frac{n}{k}\right\rfloor\right)\\
&= \sum_{k\mid(n+1)}\frac{\mu(k)}{k}\\
&= \frac{\varphi(n+1)}{n+1}
\end{aligned}$$

by Theorem 3.4.22. Consequently,

$$\begin{aligned}\sum_{k=1}^{n} \frac{\mu(k)}{k}\left\lfloor \frac{n}{k} \right\rfloor &= f(n) \\ &= f(1) + \sum_{k=1}^{n-1} (f(k+1) - f(k)) \\ &= 1 + \sum_{k=1}^{n-1} \frac{\varphi(k+1)}{k+1} \\ &= 1 + \sum_{k=1}^{n} \frac{\varphi(k)}{k} - \frac{\varphi(1)}{1} \\ &= \sum_{k=1}^{n} \frac{\varphi(k)}{k}\end{aligned}$$

as desired. □

Second Proof. Take $f(n) = \dfrac{\mu(n)}{n}$. Then, $F(n)$, the summatory function of f, would be

$$\begin{aligned}F(n) &= \sum_{d|n} \frac{\mu(d)}{d} \\ &= \frac{1}{n}\left(n \sum_{d|n} \frac{\mu(d)}{d}\right)\end{aligned}$$

According to Theorem 3.4.22, the expression in the parenthesis equals $\varphi(n)$. Therefore,

$$F(n) = \frac{\varphi(n)}{n}$$

The conclusion follows from Theorem 3.3.6. □

Theorem 3.4.31 (Properties of Jordan's Totient Function). *Let n and k be positive integers. Then,*

1. $J_k(n) = n^k \prod_{p|n}\left(1 - \frac{1}{p^k}\right)$
2. *J_k is multiplicative*
3. $\sum_{d|n} J_k(d) = n^k$
4. $J_k = id^k * \mu$
5. *J_k is even if and only if $n \geq 3$*

Proof.

1. Let $p_1, p_2, \cdots, p_m$ be the prime factors of n. Consider all $k-$tuples $(x_1, x_2, \cdots, x_k)$ of positive integers so that $x_i \leq n$ for $i = 1, 2, \cdots, n$. The number of such $k-$tuples is n^k (why?). In order to find $J_k(n)$, we must find out how many of these n^k $k-$tuples have the property that $(x_1, x_2, \cdots, x_k, n) = 1$. In other words, we need to omit the $k-$tuples in which all x_i $(1 \leq i \leq k)$ are divisible by at least one of p_j $(1 \leq j \leq m)$. There are exactly $(n/p_1)^k$ $k-$tuples in which all x_i are divisible by p_1. So, the number of $k-$tuples in which not all x_i are divisible by p_1 is

$$n_1 = n^k \left(1 - \frac{1}{p_1^k}\right)$$

Among these n_1 $k-$tuples, there are $n_2 = n_1 \left(1 - \frac{1}{p_2^k}\right)$ ones in which not all x_i are divisible by p_2. Continuing this way, assuming n_j $(1 \leq j \leq m)$ to be the number of $k-$tuples $(x_1, x_2, \cdots, x_k)$ in which not all x_i $(1 \leq i \leq k)$ are divisible by $p_1, p_2, \cdots,$ or p_j,

$$\begin{aligned} n_3 &= n_2 \left(1 - \frac{1}{p_3^k}\right) \\ n_4 &= n_3 \left(1 - \frac{1}{p_4^k}\right) \\ &\vdots \\ n_m &= n_{m-1} \left(1 - \frac{1}{p_m^k}\right) \end{aligned}$$

It is now obvious that $J_k(n) = n_m$, thus

$$\begin{aligned} J_k(n) &= n^k \left(1 - \frac{1}{p_1^k}\right)\left(1 - \frac{1}{p_2^k}\right)\cdots\left(1 - \frac{1}{p_m^k}\right) \\ &= n^k \prod_{p \mid n} \left(1 - \frac{1}{p^k}\right) \end{aligned}$$

2. Let m and n be co-prime positive integers. We will show that $J_k(mn) = J_k(m)J_k(n)$. Suppose that

$$\begin{aligned} m &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t} \\ n &= q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s} \end{aligned}$$

are the prime factorizations of m and n, respectively. Then, according to part 1 of

this theorem,

$$\begin{aligned} J_k(mn) &= (mn)^k \prod_{p \mid mn} \left(1 - \frac{1}{p^k}\right) \\ &= \left(m^k \prod_{p \mid m} \left(1 - \frac{1}{p^k}\right)\right)\left(n^k \prod_{p \mid n} \left(1 - \frac{1}{p^k}\right)\right) \\ &= J_k(m) J_k(n) \end{aligned}$$

3. Since Jordan's totient function is multiplicative, it suffices to prove that

$$\sum_{d \mid p^\alpha} J_k(d) = (p^\alpha)^k$$

where p is a prime and α is a positive integer. According to part 2 of this theorem, for any positive integer i,

$$J_k(p^i) = p^{ki} - p^{k(i-1)}$$

Therefore,

$$\begin{aligned} \sum_{d \mid p^\alpha} J_k(d) &= J_k(1) + J_k(p) + \cdots + J_k(p^\alpha) \\ &= 1 + \sum_{i=1}^{\alpha} \left(p^{ki} - p^{k(i-1)}\right) \end{aligned}$$

Now, from Sum of Differences,

$$\begin{aligned} \sum_{d \mid p^\alpha} J_k(d) &= 1 + \sum_{i=1}^{\alpha} \left(p^{ki} - p^{k(i-1)}\right) \\ &= 1 + (p^{k\alpha} - 1) \\ &= (p^\alpha)^k \end{aligned}$$

4. The equation $\sum_{d \mid n} J_k(d) = n^k$ can be represented as $1 * J_k = \mathrm{id}^k$. Then, since the inverse of function 1 is μ (Theorem 3.3.5),

$$\begin{aligned} J_k &= 1^{-1} * (1 * J_k) \\ &= 1^{-1} * \mathrm{id}^k \\ &= \mu * \mathrm{id}^k \end{aligned}$$

5. Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ be the prime factorization of n. One can write the formula in part 1 of this theorem as

$$\begin{aligned} J_k(n) &= n^k \left(1 - \frac{1}{p_1^k}\right)\left(1 - \frac{1}{p_2^k}\right) \cdots \left(1 - \frac{1}{p_m^k}\right) \\ &= \left(p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdots p_m^{\alpha_m - 1}\right)^k (p_1^k - 1)(p_2^k - 1) \cdots (p_m^k - 1) \end{aligned}$$

The proof is obvious now.

□

§§3.5 Menon's Identity

Menon's Identity is a very nice theorem in number theory, though not popular. Here, we prove it using a powerful theorem. First, we need the following lemma.

Lemma 3.5.1. *Let m and n be positive integers such that $(m,n)=d$. Prove that*

$$\varphi(mn)=\varphi(m)\varphi(n)\cdot\frac{d}{\varphi(d)}$$

Proof. Using part (d) of Theorem 3.2.11, we know that $\varphi(x)=x\prod_{p\mid x}\left(1-\frac{1}{p}\right)$, where x is a positive integer and p ranges over all prime divisors of x. So,

$$\begin{aligned}\varphi(mn)&=mn\prod_{p\mid mn}\left(1-\frac{1}{p}\right)\\&=mn\cdot\frac{\prod_{p\mid m}\left(1-\frac{1}{p}\right)\cdot\prod_{p\mid n}\left(1-\frac{1}{p}\right)}{\prod_{p\mid d}\left(1-\frac{1}{p}\right)}\\&=\frac{m\prod_{p\mid m}\left(1-\frac{1}{p}\right)\cdot n\prod_{p\mid n}\left(1-\frac{1}{p}\right)\cdot d}{d\prod_{p\mid d}\left(1-\frac{1}{p}\right)}\\&=\varphi(m)\varphi(n)\cdot\frac{d}{\varphi(d)}\end{aligned}$$

□

Theorem 3.5.2. *Given integers r,d,k, and n so that $n=dk, d,k>0, n\geq 1$, and $\gcd(r,d)=1$. Then the number of integers of the form $r+id$ (for $1\leq i\leq k$) which are co-prime to n is $\dfrac{\varphi(n)}{\varphi(d)}$.*

Proof. First, let us write $\dfrac{\varphi(n)}{\varphi(d)}$ in another way. Let $s=(d,k)$. Then, from Theorem 3.5.1,

$$\begin{aligned}\frac{\varphi(n)}{\varphi(d)}&=\frac{\varphi(kd)}{\varphi(d)}\\&=\frac{\frac{\varphi(k)\varphi(d)s}{\varphi(s)}}{\varphi(d)}\\&=s\frac{\varphi(k)}{\varphi(s)}\end{aligned}$$

Notice that if $(r+id,n)=1$ for some i, then $(r+id,k)=1$. The reason is that if $(r+id,k)=g$, then $g \mid k$, which in turn means $g \mid n$. Now, g divides $r+id$ and n and hence it also divides their gcd, which is 1. So, $g=1$. On the other hand, if $(r+id,k)=1$ for some i, then $(r+id,n)=1$ since $r \perp d$.

Therefore, the problem reduces to showing that the number of integers of the form $r+id$ $(1 \le i \le k)$ which are co-prime to k is $s\dfrac{\varphi(k)}{\varphi(s)}$.

Since $s=(d,k)$, there exist positive integers k_1 and d_1 such that $k=k_1 s$ and $d=d_1 s$. So, the numbers $r+id$ (for $1 \le i \le k$) will become $r+id_1 s$ (for $1 \le i \le k_1 s$). Classify these numbers in the following manner:

$$\begin{matrix} r+d_1 s & r+2d_1 s & \cdots & r+k_1 d_1 s \\ r+(k_1+1)d_1 s & r+(k_1+2)d_1 s & \cdots & r+2k_1 d_1 s \\ \vdots & \vdots & \vdots & \vdots \\ r+[(s-1)k_1+1]d_1 s & r+[(s-1)k_1+2]d_1 s & \cdots & r+sk_1 d_1 s \end{matrix}$$

We want to prove that the number of integers among these numbers which are co-prime to k is $s\dfrac{\varphi(k)}{\varphi(s)}$. Let us prove the case when $s=1$ first. In this case, $k \perp d$, $k=k_1$, and $d=d_1$. Therefore, the numbers in the first row are $r+d, r+2d, \cdots, r+kd$, which are all different modulo k (why?). This means that they form a complete residue system modulo k. Obviously, there are

$$\varphi(k)=\frac{\varphi(k)}{\varphi(s)}$$

numbers co-prime to k among these integers. So, the theorem is proved for the case $s=1$. Now assume that $s>1$. There are s rows of numbers. So, if we prove that there are $\dfrac{\varphi(k)}{\varphi(s)}$ numbers co-prime to k in each row, we are done. Similar to the above, for any i, we have $(r+id_1 s,k)=1$ if and only if $(r+id_1 s,k_1)=1$. Moreover, the numbers in each column are congruent modulo k_1. We know that if $a \equiv b \pmod{k_1}$, then $(a,k_1)=(b,k_1)$. This means that the number of integers co-prime to k_1 (and thus k) in all the rows are equal.

So, it suffices to prove that there are exactly $\dfrac{\varphi(k)}{\varphi(s)}$ numbers co-prime to k_1 in the first row of numbers, namely, $r+is$ for $i=d_1, 2d_1, \cdots, k_1 d_1$. If you look closely, this is exactly the same thing as the original theorem when we replace n by k, k by k_1, and d by s (the only difference is that here, the possible values for i are k_1 numbers $d_1, 2d_1, \cdots, k_1 d_1$, while possible values for i in the original theorem are $1, 2, \cdots, k$).

In the new version of the theorem, which we want to prove, there are k_1 numbers of the form $r+is$, while this number is $k=k_1 s$ in the original theorem. Since $s>1$, we have $k_1<k$. Take $s_1=(s,k_1)$ and let k_2 and d_2 be integers such that $k_1=k_2 s_1$ and $s=d_2 s_1$. With the same method as above, classify the numbers $r+d_1 s, r+2d_1 s, \cdots, r+k_1 d_1 s$ as:

$$\begin{matrix} r+d_1 d_2 s_1 & r+2d_1 d_2 s_1 & \cdots & r+k_2 d_1 d_2 s_1 \\ r+(k_2+1)d_1 d_2 s_1 & r+(k_2+2)d_1 d_2 s_1 & \cdots & r+2k_2 d_1 d_2 s_1 \\ \vdots & \vdots & \vdots & \vdots \\ r+[(s-1)k_2+1]d_1 d_2 s_1 & r+[(s-1)k_2+2]d_1 d_2 s_1 & \cdots & r+s_1 k_2 d_1 d_2 s_1 \end{matrix}$$

With the exact same reasoning as above, we can reduce the problem to showing that there are $\frac{\varphi(k_2)}{\varphi(s_1)}$ integers co-prime to k_2 in the first row of above numbers. If $s_1 = 1$, we are done. Otherwise, we have $k_2 < k_1$ and we can take $s_2 = (s_1, k_2)$, $k_2 = k_3 s_2$, and $s_1 = d_3 s_2$. If we continue this process, we will finally reach a point where the gcd becomes one. That is, the sequence $s, s_1, s_2, \cdots$ will eventually reach 1. The reason is that the sequence $k, k_1, k_2, \cdots$ is strictly decreasing and contains only positive integers. This means that for some m, we will have $k_m = 1$ and then the sequence stops. In that point, $k_{m-1} = k_m$, which in turn means s_{m-1}, the gcd of k_m and s_{m-1}, equals one. We have already showed that when this gcd is one, the theorem is true. The proof is complete. □

Theorem 3.5.3 (Menon's Identity). *Let n be a positive integer. Then,*

$$\sum_{\substack{i=1\\(i,n)=1}}^{n} (i-1,n) = \tau(n)\varphi(n)$$

where $\tau(n)$ is the number of divisors of n.

Proof. We can write the sum as

$$\begin{aligned}\sum_{\substack{i=1\\(i,n)=1}}^{n} (i-1,n) &= \sum_{\substack{i=1\\(i,n)=1}}^{n} \sum_{d\mid(i-1,n)} \varphi(d) \\ &= \sum_{d\mid n} \varphi(d) \sum_{\substack{i=1\\(i,n)=1\\ i\equiv 1 \pmod d}}^{n} 1\end{aligned}$$

According to Theorem 3.5.2, the second sum in the last line equals $\varphi(n)/\varphi(d)$. Therefore,

$$\begin{aligned}\sum_{\substack{i=1\\(i,n)=1}}^{n} (i-1,n) &= \sum_{d\mid n} \varphi(d)\frac{\varphi(n)}{\varphi(d)} \\ &= \sum_{d\mid n} \varphi(n)\end{aligned}$$

Since $\varphi(n)$ is independent from d in the last summation, we have

$$\begin{aligned}\sum_{\substack{i=1\\(i,n)=1}}^{n} (i-1,n) &= \varphi(n)\sum_{d\mid n} 1 \\ &= \tau(n)\varphi(n)\end{aligned}$$

which is what we wanted. □

§§3.6 Liouville Function

Liouville function is of high interest in many sections of number theory. As a reminder, we are going to state the definitions of the functions $\omega(n)$, $\Omega(n)$, and $\lambda(n)$ once again.

Big Omega Function. Let n be a positive integer. The number of prime factors of n (with multiplicity) is denoted by $\Omega(n)$.

Small Omega Function. Let n be a positive integer. The number of distinct prime factors of n is denoted by $\omega(n)$.

Liouville Function. For a natural number n, the Liouville function $\lambda(n)$ is defined as

$$\lambda(n) = (-1)^{\Omega(n)}$$

Proposition 3.6.1. *Let $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ be the prime factorization of a positive integer n. Then, $\omega(n) = k$ and $\Omega(n) = \alpha_1 + \alpha_2 + \cdots + \alpha_k$. In other words,*

$$\omega(n) = \sum_{i=1}^{k} 1$$

$$\Omega(n) = \sum_{i=1}^{k} \alpha_i$$

Note. $\omega(1) = \Omega(1) = 0$, as 1 does not have any prime factors.

Proposition 3.6.2. *For a natural number n, $\Omega(n) = \omega(n)$ if and only if n is square-free.*

Proof. If n is square-free, then it is obvious that $\omega(n) = \Omega(n)$. Now, suppose that $\omega(n) = \Omega(n)$ holds for some positive integer n with prime factorization $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$. In this case,

$$\alpha_1 + \alpha_2 + \cdots + \alpha_k = k$$

Notice that all α_i are positive integers ($1 \leq i \leq k$) and the above equation only occurs when all of them are equal to 1. In other words, n is not divisible by the square of any prime and is therefore square-free. □

Proposition 3.6.3.

- *ω is an additive function,*
- *Ω is a completely additive function.*

The reader should have a decent idea of what to use in order to prove it!

Theorem 3.6.4. *Prove that the Dirichlet inverse of Liouville function is the absolute value of Möbius function.*

Proof. We want to prove that $\lambda * |\mu| = \varepsilon$. From Theorem 3.4.3, since both λ and $|\mu|$ are multiplicative, their Dirichlet product is also multiplicative. Therefore, it suffices to prove that $(\lambda * |\mu|)(p^\alpha) = \varepsilon(p^\alpha)$, where p is a prime and α is a positive integer. Notice that $\varepsilon(p^\alpha) = 0$, so we have to prove that $(\lambda * |\mu|)(p^\alpha) = 0$. We have

$$\begin{aligned}(\lambda * |\mu|)(p^\alpha) &= \sum_{d|p^\alpha} |\mu(d)|\lambda\left(\frac{p^\alpha}{d}\right) \\ &= |\mu(1)|\lambda(p^\alpha) + |\mu(p)|\lambda(p^{\alpha-1}) + \cdots + |\mu(p^\alpha)|\lambda(1) \\ &= |\mu(1)|\lambda(p^{\alpha-1}) + |\mu(p)|\lambda(p^{\alpha-2}) \\ &= (-1)^\alpha + (-1)^{\alpha-1} \\ &= 0\end{aligned}$$

as desired. □

The following theorem is due to Sierpiński and Schinzel.[8]

Theorem 3.6.5. *Let s be an arbitrary integer. Then, for all integers $n > 1$ with prime factorization $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$,*

$$\sum_{d|n} \lambda(d) d^s = \prod_{i=1}^{k} \frac{(-1)^{\alpha_i} p_i^{(\alpha_i+1)s} + 1}{p_i^s + 1}$$

Proof. Since both $\lambda(d)$ and d^s are completely multiplicative functions, their product is a multiplicative function. We find from Theorem 3.4.1 that $\sum_{d|n} \lambda(d) d^s$ is also multiplicative. Therefore, it suffices to prove the theorem for the case when n is a power of a prime. Take $n = p^\alpha$ for some prime p and positive integer α. Then,

$$\begin{aligned}\sum_{d|p^\alpha} \lambda(d) d^s &= \lambda(1)1^s + \lambda(p)p^s + \lambda(p^2)\left(p^2\right)^s + \lambda(p^3)\left(p^3\right)^s + \cdots + \lambda(p^\alpha)\left(p^\alpha\right)^s \\ &= 1^s - p^s + p^{2s} - p^{3s} + \cdots + (-1)^\alpha p^{\alpha s}\end{aligned}$$

This is a geometric progression with initial term 1 and common ratio $-p^s$. Therefore, by the formula for geometric series,

$$\begin{aligned}\sum_{d|p^\alpha} \lambda(d) d^s &= \sum_{i=0}^{\alpha} (-1)^{si} p^{si} \\ &= \frac{\left(-p^s\right)^{\alpha+1} - 1}{-p^s - 1} \\ &= \frac{(-1)^\alpha p^{(\alpha+1)s} + 1}{p^s + 1}\end{aligned}$$

[8] Sierpiński and Schinzel, *Elementary theory of numbers*, Chapter §IV, Section 11, Page 196 – 197.

Applying this result to $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, using multiplicativity of the functions as discussed,

$$\begin{aligned}\sum_{d|n} \lambda(d) d^s &= \prod_{i=1}^{k} \sum_{d|p_i^{\alpha_i}} \lambda(d) d^s \\ &= \frac{(-1)^{\alpha_i} p_i^{(\alpha_i+1)s} + 1}{p_i^s + 1}\end{aligned}$$

as desired. □

The previous theorem is pretty strong. The following theorem, which is an example case of the preceding theorem, is useful and important.

Theorem 3.6.6. *Let x be the summatory function of λ. That is, let x be an arithmetic function such that*

$$x(n) = \sum_{d|n} \lambda(d)$$

Then,

$$x(n) = \begin{cases} 1 & \text{if } n \text{ is a perfect square,} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Take $s = 0$ in Theorem 3.6.5. Then, assuming $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ as the prime factorization of n,

$$\sum_{d|n} \lambda(d) = \prod_{i=1}^{k} \frac{1 + (-1)^{\alpha_i}}{2}$$

If n is a perfect square, that is, if all the α_i (for $1 \leq i \leq k$) are even, the above product equals one. Otherwise, at least one of α_i is odd and thus $1 + (-1)^{\alpha_i} = 0$, making the product equal to zero. □

Remark. The sum $L(n) = \sum_{k=1}^{n} \lambda(k)$ has been investigated for a long time. It was first conjectured that $L(n) < 0$ for all integers $n > 1$. You can check and see that it is true for small integers. However, in 1980, Minoru Tanaka found that $n = 906150257$ is the smallest counter-example to this conjecture.

Theorem 3.6.7. *Let n be a positive integer. Then,*

$$\lambda(n) = \sum_{k^2|n} \mu\left(\frac{n}{k^2}\right)$$

Proof. Assume that $\varkappa(n) = \sum_{d|n} \lambda(d)$. Then, by Möbius inversion formula (Theorem 3.3.3),

$$\begin{aligned}\lambda(n) &= \sum_{d|n} \mu(d)\varkappa\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \varkappa(d)\mu\left(\frac{n}{d}\right) \\ &= \sum_{k^2|n} \mu\left(\frac{n}{k^2}\right)\end{aligned}$$

because $\varkappa(d)$ is 1 whenever d is a perfect square (i.e., $d = k^2$ for some k), and zero otherwise. □

Theorem 3.6.8. *Prove that for every positive integer n,*

$$\sum_{k=1}^{n} \lambda(k)\left\lfloor\frac{n}{k}\right\rfloor = \lfloor\sqrt{n}\rfloor$$

Proof. The summatory function of λ is $\varkappa$. Therefore, from Theorem 3.3.6,

$$\sum_{k=1}^{n} \mu(k)\left\lfloor\frac{n}{k}\right\rfloor = \sum_{k=1}^{n} \varkappa(k)$$

We know by Theorem 3.6.6 that $\varkappa(k)$ is 1 if k is a perfect square and 0 otherwise. So, $\sum_{k=1}^{n} \varkappa(k)$ is exactly $\lfloor\sqrt{n}\rfloor$. □

§§3.7 Exercises

Problem 3.7.1. How many integers between a and b are divisible by n? Note that a and b are not necessarily positive.

Problem 3.7.2. Let n be a positive integer. Prove that for any prime p,

$$v_p(n) = \sum_{k=1}^{\infty} \left(\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n-1}{p^k} \right\rfloor \right)$$

Problem 3.7.3. Let n be a positive integer. Show for every prime p that

$$\frac{n}{p-1} - \frac{\ln(n+1)}{\ln p} \leq v_p(n!) \leq \frac{n-1}{p-1}$$

Problem 3.7.4. Let $n > 1$ be an integer. Prove that $(|\mu| * 1)(n) = 2^n$. Here, $|\cdot|$ denotes the absolute value.

Problem 3.7.5. Prove for any positive integer n that

$$\sum_{d|n} \frac{\mu(d)^2}{\varphi(d)} = \frac{n}{\varphi(n)}$$

Problem 3.7.6. Let n be a positive integer. Show that

$$\sum_{d|n} d^2 \mu\left(\frac{n}{d}\right) = n\varphi(n) \prod_{p|n} \left(1 + \frac{1}{p}\right)$$

Problem 3.7.7. Prove that for any even positive integer n,

$$\sum_{d|n} \mu(d)\varphi(d) = 0$$

Problem 3.7.8. Prove that $\tau^3 * 1 = (\tau * 1)^2$.

Problem 3.7.9. Let s be an arbitrary integer. Prove for all integers $n > 1$ with prime factorization $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ that

$$\sum_{d|n} \mu(d) d^s = \prod_{i=1}^{k} (1 - p_i^s)$$

Problem 3.7.10. For every integer $n \geq 1$, show that

$$\mu^2(n) = \sum_{d^2|n} \mu(d)$$

Problem 3.7.11. Let m and n be positive integers such that $n \geq 2$. Prove that

$$\sum_{\substack{d \mid n \\ \omega(d) \leq m}} \mu(d)$$

is non-negative if m is even and non-positive if m is odd.

Problem 3.7.12. Prove that the product of all divisors of a positive integer n is $n^{\tau(n)/2}$.

Problem 3.7.13. Let n be a positive integer. Show that

$$\frac{\sigma(n)^2}{n} \geq \tau(n)^2$$

Hint. Use the fact that

$$\begin{aligned} \sigma(n) &= \sum_{d \mid n} d \\ &= \sum_{d \mid n} \frac{n}{d} \end{aligned}$$

Then exploit the Cauchy–Schwarz inequality.

Problem 3.7.14 (Romania TST 2010). Given a positive integer a, prove that $\sigma(am) < \sigma(am+1)$ for infinitely many positive integers m.

Problem 3.7.15. Prove that there exist infinitely many positive integers n such that $\sigma(n) = 2n + 12$.

Problem 3.7.16. Let $k \geq 2$ be an integer. Prove that there exist no positive integer n such that $\sigma(n) = n^k$.

Problem 3.7.17. Show for any three positive integers α, m, and n that

$$\sigma_\alpha(m)\sigma_\alpha(n) = \sum_{d \mid (m,n)} d^2 \sigma_\alpha\left(\frac{mn}{d^2}\right)$$

Problem 3.7.18. Let p be a prime that generates the even perfect number $E_p = 2^{p-1}(2^p - 1)$. Then E_p is expressible as the sum of the cubes of the first n consecutive positive integers, where $n = 2^{(p-1)/2}$.

Problem 3.7.19. Prove that if existing, an odd perfect number would be of the form $12n + 1$.

Problem 3.7.20 (Putnam 1976). A positive integer n is called *quasi-perfect* if $\sigma(n) = 2n + 1$. Prove that any quasi-perfect number is the square of an odd integer.

Problem 3.7.21 (Romania TST 2014). Show that a positive integer n, which has at most two distinct prime factors, satisfies the condition $\sigma(n) = 2n - 2$ if and only if $n = 2^k(2^{k+1} + 1)$, where k is a non-negative integer and $2^{k+1} + 1$ is prime.

Problem 3.7.22 (IMO Longlist 1979). If n has at most 5 distinct prime divisors, prove that $\sigma(n) < \frac{77}{16}n$. Also prove that there exists a positive integer n for which $\sigma(n) < \frac{76}{16}n$ holds.

Problem 3.7.23. Let n be a positive integer. Show that

$$\varphi(n) = \sum_{k=1}^{n-1} \left\lfloor \frac{1}{(n,k)} \right\rfloor$$

Problem 3.7.24. For a positive integer n, find the value of the following sum

$$\sum_{d|n} (-1)^{n/d} \varphi(d)$$

Problem 3.7.25. For $n \geq 2$, show that

$$\frac{\sigma(n)}{n} < \frac{n}{\varphi(n)} < \frac{\pi^2}{6} \frac{\sigma(n)}{n}$$

Hint. For the right side, use the fact that

$$\prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^2}\right) = \frac{6}{\pi^2}$$

where the product extends over all primes p.

Problem 3.7.26. Prove that for any integer $n \geq 2$,

$$\sum_{\substack{1 \leq k \leq n \\ (k,n)=1}} k = \frac{1}{2} n \varphi(n)$$

Problem 3.7.27. Prove that for any integer n larger than 6,

$$\varphi(n) \geq \sqrt{n}$$

Problem 3.7.28. For all positive integers n, show that

$$\sum_{k=1}^{n} \left\lfloor \frac{n}{k} \right\rfloor \varphi(k) = \frac{n(n+1)}{2}$$

Problem 3.7.29. Let a be an arbitrary integer. Prove that for every positive integer n,

$$\sum_{d|n} \varphi\left(\frac{n}{d}\right) a^d \equiv 0 \pmod{n}$$

Problem 3.7.30. Prove that for any integer $n \geq 3$,

$$\varphi(2) + \varphi(3) + \varphi(4) + \cdots + \varphi(n) \geq \frac{n(n-1)}{4} + 1$$

Problem 3.7.31. Let x be a positive real number. Prove that

$$\sum_{n\leq x}\left\lfloor\sqrt{\frac{x}{n}}\right\rfloor=\sum_{n\leq\sqrt{x}}\left\lfloor\frac{x}{n^2}\right\rfloor$$

Hint. Use Theorem 3.6.8.

Problem 3.7.32. Find all positive integers n such that

$$\varphi(n)+\sigma(n)=2n$$

Problem 3.7.33. Prove that if $\sigma(n)=5n$ than n has more than 5 distinct prime divisors.

Problem 3.7.34 (Belarus 2010). Find the greatest real number a such that for all $n>1$ the following inequality is true

$$\frac{\sigma(n)}{\tau(n)}\geq a\sqrt{n}$$

Problem 3.7.35. Show that a positive integer n is prime if and only if $\sigma(n)+\varphi(n)=n\cdot\tau(n)$.

Problem 3.7.36 (China Western Mathematical Olympiad 2015). Let k be a positive integer and take $n=(2^k)!$. Prove that $\sigma(n)$ has at least a prime divisor larger than 2^k.

Problem 3.7.37 (Cono Sur Shortlist 2012). Find all integers $1<n<2012$ for which $(p(n))^2=\sigma(n)+423$, where $p(n)$ is the product of all prime divisors of n.

Problem 3.7.38. Prove that for every positive integer n the following inequality holds

$$\sum_{k=1}^{n}\tau(k)\ln k\leq 2n\cdot\sum_{k=1}^{n}\frac{\ln k}{k}$$

Problem 3.7.39 (Russia 2011). Show that if $\sigma(n)=5n/3$, then $\sigma(5n)=10n$.

Problem 3.7.40. Find all positive integers k and n such that

$$\varphi(n)\cdot\tau(n)\cdot\sigma(n)=k\cdot(n^k-1)$$

Problem 3.7.41 (Ukraine 2006). Let n be a positive integer and define $N=2^{2^n}+1$. Prove that

$$\frac{\sigma(N)}{N}<2$$

Problem 3.7.42. Let n be a positive integer such that $\sigma(n)=2n+1$. Show that $\sqrt{n}$ is an odd number.

Problem 3.7.43. Prove that a positive integer n is prime if and only if $\varphi(n)\mid n-1$ and $n+1\mid\sigma(n)$.

Problem 3.7.44. Prove that $6 \mid \sigma(6n+5)$ for all positive integers n.

Problem 3.7.45 (China TST 2014). Prove that there exist finitely many positive integers n satisfying the following two conditions:

1. $\tau(n) = a$
2. $n \mid \phi(n) + \sigma(n)$

Problem 3.7.46 (Serbia Additional TST 2012). For every $n \in \mathbb{N}$ define $f(n)$ as number of natural numbers $m, m \leq n$, for which $\sigma(m)$ is odd number. Prove that there are infinitely many natural numbers n, such that $f(n) \mid n$.

Problem 3.7.47 (Iran Third Round 2009). We call a permutation π on the set $A_n = \{1, 2, \cdots, n\}$ steply constant if the set $\{\pi(k) - k | k = 1, 2, \cdots, n\}$ has exactly two elements. Prove that the number of steply constant permutations of A_n is $\sigma(n) - \tau(n)$.

Problem 3.7.48 (Belarus 1999). For any integer $n \geq 2$, prove that

$$\sigma(n) < n\sqrt{2\tau(n)}$$

Problem 3.7.49 (All Russian Olympiads 2000). A perfect number greater than 28 is divisible by 7. Prove that it is also divisible by 49.

Problem 3.7.50. Find all positive integers n such that

$$\frac{\tau(n)\varphi(n)\sigma(n) + 2\omega(n)}{\varphi(n) + \sigma(n)} = \varphi(n) + \omega(n)$$

Problem 3.7.51 (IMS 2008). Find all natural numbers such that

$$n\sigma(n) \equiv 2 \pmod{\varphi(n)}$$

§§4 Primes

§§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 the 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 Olympiad style topics. We do not give the elementary proof of *Prime Number Theorem* by *Erdős* and *Selberg*[1]

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?

[1]There was a dispute over the prime number theorem whether Erdős and Selberg would write a joint paper or not. Goldfeld (D. Goldfeld. "The Elementary Proof of the Prime Number Theorem: An Historical Perspective". In: *Number Theory* [2004], pp. 179–192. DOI: 10.1007/978-1-4419-9060-0_10) and Baas and Skau (Nils A. Baas and Christian F. Skau. "The lord of the numbers, Atle Selberg. On his life and mathematics". In: *Bulletin of the American Mathematical Society* 45.4 [2008], pp. 617–617. DOI: 10.1090/s0273-0979-08-01223-8) are great reads in this regard.

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 357879581^2. 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 such factorization or similar tasks. And they are used in a lot of area such as security. For example, every time you log into 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.

[2]We used this number because long time ago the first author used to think this is a prime.

[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.

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

$$\begin{aligned}\zeta(s) &= \frac{1}{1^s} + \frac{1}{2^s} + \cdots \\ &= \sum_{i \geq 1} \frac{1}{i^s}\end{aligned}$$

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 $P = \{p_1, p_2, \dots, p_k\}$ be the set of all primes. Euclid's idea was to construct a number 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,

$$(N, p) = (p_1 \cdots p_k + 1, p_i) \tag{4.1}$$
$$= (1, p_i) \tag{4.2}$$
$$= 1 \tag{4.3}$$

for some $p_i \in P$, which is in contradiction with $p \mid N$. 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 $p_1, p_2, \dots, p_k$ 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 relatively prime 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 relatively prime. 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 relatively prime to each other. □

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

Proof. Note the identity:

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

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

There are other proofs that use the same idea of relatively prime 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 (1.2.4) 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

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

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

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

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

$$\frac{1}{p_1} + \cdots + \frac{1}{p_k} = \frac{a}{P} \tag{4.4}$$

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 $1 \le i \le k$ and rewrite equation (4.4) to obtain

$$a = \frac{P}{p_1} + \cdots + \frac{P}{p_i} + \cdots + \frac{P}{p_k} \tag{4.5}$$

Obviously, $p_i \mid \frac{P}{p_j}$ for all $j \neq i$. On the other hand, p divides a. Equation (4.5) now forces $p_i \mid \frac{P}{p_i}$, 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 $n \ge 1$. Now

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

Therefore,

$$\sum_{i \ge 1}^{\prime} \frac{1}{i^2} = 2 - m \tag{4.6}$$

for some positive real m. Let's get to the proof. Like before, we assume there are only k primes $p_1, p_2 \dots, p_k$. 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

$$\begin{aligned} N &\le 2^k + \sum_{i=1}^{k} \left\lfloor \frac{N}{p_i^2} \right\rfloor \\ &< 2^k + \sum_{i=1}^{k} \frac{N}{p_i^2} \\ &= 2^k + N \sum_{i=1}^{k} \frac{1}{p_i^2} \end{aligned} \tag{4.7}$$

From equation (4.6), we get

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

Substitute this into equation (4.7),

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

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). □

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.

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

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

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

$$\begin{aligned} S &= 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots \\ &= \left(1 + \frac{1}{2} + \frac{1}{2^2} + \cdots\right) \cdot \left(1 + \frac{1}{3} + \frac{1}{3^2} + \cdots\right) \cdot \left(1 + \frac{1}{5} + \frac{1}{5^2} + \cdots\right) \cdots \\ &= \prod_{p \in \mathbb{P}} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) \end{aligned} \tag{4.8}$$

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 (4.8), we get the desired result

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

□

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 (Euler's theorem).

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

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). $\zeta(2)=\frac{\pi^2}{6}$. *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 relatively prime to P. If we discard 1, there is at least one other positive integer which is relatively prime 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 1.5.14 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 relatively prime 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 (2.8.10), 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 2.12.8 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 relatively prime 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 relatively prime positive integers, then there are infinitely many primes the arithmetic progression*

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

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

§§4.3 Number of 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 $p \mid P(kp)$ 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. □

Here, we focus on finding $\pi(n)$ rather than a direct formula for p_n.

Theorem 4.3.2. *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 $i > 1$. 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 $i \mid s + 1$ 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 relatively prime 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 $p_1, p_2, \dots, p_k$ 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 $\{p_1, p_2, \dots, p_k\}$.

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 $p_2, \dots, p_k$. 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.

Theorem 4.3.3. *Let n be a positive integer and $p_1, p_2, \dots, p_k$ 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*

(4.9)

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

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,

$$\pi(x) - \pi(\sqrt{x}) + 1 = \lfloor x \rfloor - \sum_{p_i} \left\lfloor \frac{x}{p_i} \right\rfloor + \sum_{p_i < p_j} \left\lfloor \frac{x}{p_i p_j} \right\rfloor - \sum_{p_i < p_j < p_k} \left\lfloor \frac{x}{p_i p_j p_k} \right\rfloor + \cdots \tag{4.10}$$

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

$$\pi(n)-\pi(\sqrt{n})+1=\sum_{i=1}^{P}\mu(i)\left\lfloor\frac{n}{i}\right\rfloor \tag{4.11}$$

where $P=p_1p_2\cdots p_k$. This is probably not obvious to you, so we explain how the above fomula is obtained[8]. It is now a very good time to mention a point the importance of the Möbius μ function defined in defintion (3.3) as:

$$\mu(n)=\begin{cases}1 & \text{if } n=1\\ 0 & \text{if } n \text{ is divisible by } p^2 \text{ for some prime } p\\ (-1)^k & \text{if } n=p_1p_2\cdots p_k\end{cases}$$

We stated in the previous chapter that Möbius comes handy when dealing with inclusion–exclusion arguments. Here, we have a nice one. We will investigate equation (4.11) 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, $1\le j\le k$). That's exactly the first group of terms in equation (4.9). 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 $\{i_1,i_2,\dots,i_s\}\subseteq\{1,2,\dots,k\}$, 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 (4.9).

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.

§§4.4 Bertrand's Postulate and Erdős's 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

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

it, using analytic number theory tools. Ramanujan, Meher, and Murty[9] proved it using properties of *Gamma function*, which is beyond the scope of this book. The first elementary proof of this theorem was given by Erdős.[10] It was the first paper he published! We will show that proof here.

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 $n < p < 2n$. The following are equivalent formulation.*

- *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*

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

Lemma 4.4.2. *For any positive integer n,*

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

Proof. From binomial the 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 other 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 (1.4.3) of previous chapter, we defined $v_p(n)$ to be the highest power of a prime p which divides n.

Lemma 4.4.3. *Let n be a positive integer and let $2n/3 < p \leq n$ be a prime. Then $p \nmid \binom{2n}{n}$.*

[9] Srinivasa Ramanujan, Jaban Meher, and Ram M. Murty. "Ramanujan's Proof of Bertrand's Postulate". In: *The American Mathematical Monthly* 120.7 (2013), p. 650. DOI: 10.4169/amer.math.monthly.120.07.650.

[10] Paul Erdős. "Beweis eines Satzes von Tschebyschef". In: *Acta Litt. Sci. Szeged* 5 (1932), pp. 194–198.

Proof. We have

$$\begin{aligned} v_p\left(\binom{2n}{n}\right) &= v_p\left(\frac{(2n)!}{(n!)^2}\right) \\ &= v_p((2n)!) - v_p((n!)^2) \\ &= v_p((2n)!) - 2v_p((n!)) \end{aligned}$$

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

$$\begin{aligned} v_p\left(\binom{2n}{n}\right) &= v_p((2n)!) - 2v_p((n!)) \\ &= 2 - 2 \cdot 1 \\ &= 0 \end{aligned}$$

□

Lemma 4.4.4. *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 Theorem 1.4.13 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 4.4.5. *Let n be a positive integer. Any prime p with $n + 2 \leq p \leq 2n + 1$ divides $\binom{2n+1}{n}$.*

Proof. Since $p > n + 1$,

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

□

Lemma 4.4.6. *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 4.4.7. *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

$$\begin{aligned}\prod_{p \leq n} p &= \prod_{p \leq 2m+1} p \\ &= \left(\prod_{p \leq m+1} p\right)\left(\prod_{m+2 \leq p \leq 2m+1} p\right)\end{aligned}$$

By induction hypothesis, the first product, $\prod_{p \leq m+1} p$, is less than or equal to 4^{m+1}. From lemma Theorem 4.4.5, 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 Theorem 4.4.6, we get

$$\begin{aligned}\prod_{p \leq n} p &\leq 4^{m+1}\binom{2m+1}{m} \\ &\leq 4^{m+1}2^{2m} \\ &= 4^{2m+1} \\ &= 4^n\end{aligned}$$

So, 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 Theorem 4.4.4, $p_i^{v_{p_i}(N)} \leq 2n$ (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 Theorem 4.4.4, 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 Theorem 4.4.3 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,

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

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,

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

Note that we have used lemma Theorem 4.4.7 for writing the last line.

Combining this with the result of lemma Theorem 4.4.2, we see that

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

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 $\{n+1, n+2, \dots, 2n\}$ 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 4.4.8. *For any positive integer n, the set $S = \{1, 2, \dots, 2n\}$ 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 $\{1, 2, \dots, 2k\}$ 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 $\{m, m+1, \dots, 2n\}$. It has an even number of elements. Also, we can make pairs of $(m, 2n), (m+1, 2n-1), \dots$ with sum p, which is a prime. Now we only have to prove that the set $\{1, 2, \dots, m-1\}$ can be paired into elements with a prime sum. This is true by induction hypothesis because $m - 1 < 2n$. The proof is complete. □

Problem 4.4.9. Let $n > 5$ be an integer and let $p_1, p_2, \dots, p_k$ 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 Theorem 4.4.1,

$$\begin{aligned}\sum_{i=1}^{k+1} p_i &= p_{k+1} + \sum_{i=1}^{k} p_i \\ &> 2p_{k+1} \\ &> p_{k+2}\end{aligned}$$

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 4.4.10 (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 $n+1 \mid \binom{2n}{n}$. 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 Theorem 1.4.14, 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 4.4.11. 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[11] proved the case for $c = 1/5$.

Theorem 4.4.12 (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 the 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 4.4.13. Let k be a positive integer. Does there always exist a prime between kn and $(k+1)n$?

Bachraoui[12] proved the case $k = 2$. The idea is an extension of Erdős's proof.

[11] Jitsuro Nagura. "On the interval containing at least one prime number". In: *Proceedings of the Japan Academy* 28.4 (1952), pp. 177–181. DOI: 10.3792/pja/1195570997.

[12] M. El Bachraoui. "Primes in the interval [2n,3n]". In: *International Journal of Contemporary Mathematical Sciences* (2006), pp. 617–621. DOI: 10.12988/ijcms.2006.06065.

Theorem 4.4.14 (Bachraoui). *For a positive integer $n > 1$, there is always a prime in the interval $[2n, 3n]$.*

Loo[13] proved the case for $k = 3$ without using prime number theorem or any deep analytical method.

Theorem 4.4.15 (Loo). *For a positive integer $n \geq 2$, there is always a prime in the interval $(3n, 4n)$.*

C., Shevelev, and Greathouse[14] proves the following theorem.

Theorem 4.4.16. *The list of integers k for which every interval $(kn, (k+1)n)$ contains a prime for $n > 1$ is $\{1, 2, 3, 5, 9, 14\}$ and no others, at least for $k \leq 10^9$.*

There are some nice conjectures involving this theorem.

Conjecture 4.1 (Legendre's conjecture). *There always exists a prime in the interval $[n^2, (n+1)^2]$.*

Theorem 4.4.17 (Mitra's conjecture). *Assume the general Bertrand's postulate. There exists at least two primes in the interval $[n^2, (n+1)^2]$.*

Theorem 4.4.18 (Brocard's conjecture). *Assume the general Bertrand's postulate. For each $n > 1$, there are at least 4 primes in the interval $[p_n^2, p_{n+1}^2]$.*

Theorem 4.4.19 (Andrica's conjecture). *Assume the general Bertrand's postulate holds true. For any positive integer n, $\sqrt{p_{n+1}} - \sqrt{p_n} < 1$.*

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.

§§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 $1 < i < n + 2$. □

[13] Andy Loo. "On the Primes in the Interval [3n, 4n]". In: *International Journal of Contemporary Mathematical Sciences* 6.38 (2011). URL: `http://www.m-hikari.com/ijcms-2011/37-40-2011/looIJCMS37-40-2011.pdf`.

[14] Peter Moses J. C., Vladimir Shevelev, and Charles R. Greathouse. "On Intervals $(kn, (k+1)n)$ Containing a Prime for All $n \geq 1$". In: *Journal of Integer Sequences*. 13.7.3 16.7 (2013).

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

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

If we write shortly, we need $x \equiv -i \pmod{p_{2i-1}p_{2i}}$ for $0 \leq i \leq n-1$. 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 2.4.9, 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 $p \mid a+id$ for some $i < n$. This now gives $p \mid a+(p-i)d$ and $p \mid a+(i-p)d$. 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

$$\begin{aligned} p_{n+1} &\geq p_n + 2 \\ &> 2n + 2 \\ &= 2(n+1) \end{aligned}$$

□

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 4.4.1. 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 relatively prime is $\frac{6}{\pi^2}$.*

Proof. Two positive integers are relatively prime 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 relatively prime. 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 $(0, 1, \dots, p-1)$. 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[15], 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

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

In the last line, we used 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

[15] 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.

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 about 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 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 Chebyshev Functions

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

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

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 $2, 3, 5, \dots, 137, 139$. So

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

Corollary 4.6.1. *If $p_1, p_2, \dots, p_k$ are primes less than or equal to x, then*

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

Lemma 4.6.2. *Let k and n be positive integers such that $k < n < 2k + 1$. Then*

$$\binom{n}{k} \ge \prod_{k < p \le n} p$$

where the product extends over all primes p between k and n.

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

$$\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(k+2)(k+1)}{(n-k)!} \tag{4.12}$$

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 (4.12) can be regarded as the product of $p_1 p_2 \cdots p_m$ 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,

$$\begin{aligned}\binom{n}{k} &= \frac{p_1 p_2 \cdots p_m \cdot s}{(n-k)!} \\ &= p_1 p_2 \cdots p_m \cdot \frac{s}{(n-k)!} \\ &\geq p_1 p_2 \cdots p_m \\ &= \prod_{k<p\leq n} p\end{aligned}$$

as claimed. □

Proposition 4.6.3. *Let $x > 0$ be a real number. Then*

$$\vartheta(x) \leq 2x \ln 2 \tag{4.13}$$

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

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

where we have used lemma (4.6.2) 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. 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 $p_1, p_2, \dots, p_k$ 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 4.6.4. *Let $p_1, p_2, \dots, p_k$ be primes not exceeding a positive real number x. Also, assume that $p_1^{a_1}, p_2^{a_2}, \dots, p_k^{a_k}$ 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 4.6.5. *Let x be a positive real number. Then*

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

Proof. Let $p_1, p_2, \dots, p_k$ be primes which do not exceed x. Let $p_1^{a_1}, p_2^{a_2}, \dots, p_k^{a_k}$ be the largest powers of these primes which do not exceed x. Each number in the set $A = \{1, 2, \dots, \lfloor x\rfloor\}$ 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 $i = 1, 2, \dots, k$). It is easy to check (see proposition (1.2.7)) 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 4.6.6. *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 4.6.7 (Chebyshev Estimates). *If the following limits exist, they are all equal to* 1.

$$\lim_{x\to\infty} \frac{\vartheta(x)}{x}, \quad \lim_{x\to\infty} \frac{\psi(x)}{x}, \quad \textit{and} \quad \lim_{x\to\infty} \frac{\pi(x)\ln(x)}{x} \tag{4.14}$$

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 4.6.8. *shape For all integers $m \geq 2$,*

$$\frac{1}{6}\frac{m}{\ln m} < \pi(m) < 4\frac{m}{\ln m} \tag{4.15}$$

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

$$2^n \leq \binom{2n}{n} < 4^n \tag{4.16}$$

Using the fact that $\binom{2n}{n} = (2n)!/(n!)^2$, we can take logarithms from (4.16) to obtain

$$n\ln 2 \leq \ln(2n)! - 2\ln n! \tag{4.17}$$

$$< n\ln 4 \tag{4.18}$$

We must now find a way to compute $\ln(2n)!$ and $\ln n!$. Let k be a positive integer. By theorem (1.4.13), we have

$$v_p(k!) = \sum_{i=1}^{\alpha} \left\lfloor \frac{k}{p^i} \right\rfloor \tag{4.19}$$

where α is some positive integer. Here, we need to find α. See proof of theorem (1.4.13) 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 $a = \left\lfloor \frac{\ln k}{\ln p} \right\rfloor$. Finally, substituting n and $2n$ for k in equation (4.19), we get

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

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

It is clear that $n! = \prod_{p \le n} p^{v_p(n!)}$, 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:

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

Similarly,

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

Hence, the left hand side of inequality (4.17) becomes

$$\begin{aligned} n \ln 2 \le \ln(2n)! - 2\ln n! &= \sum_{p \le 2n} \sum_{i=1}^{\left\lfloor \frac{\ln 2n}{\ln p} \right\rfloor} \left\lfloor \frac{2n}{p^i} \right\rfloor \ln p - 2 \sum_{p \le n} \sum_{i=1}^{\left\lfloor \frac{\ln n}{\ln p} \right\rfloor} \left\lfloor \frac{n}{p^i} \right\rfloor \ln p \\ &= \sum_{p \le 2n} \sum_{i=1}^{\left\lfloor \frac{\ln 2n}{\ln p} \right\rfloor} \left\lfloor \frac{2n}{p^i} \right\rfloor \ln p - \sum_{p \le 2n} \sum_{i=1}^{\left\lfloor \frac{\ln 2n}{\ln p} \right\rfloor} 2 \left\lfloor \frac{n}{p^i} \right\rfloor \ln p \\ &= \sum_{p \le 2n} \sum_{i=1}^{\left\lfloor \frac{\ln 2n}{\ln p} \right\rfloor} \left(\left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor \right) \ln p \end{aligned} \tag{4.20}$$

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

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

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

$$\begin{aligned} \pi(2n) &\geq \frac{n \ln 2}{\ln 2n} \\ &> \frac{1}{2} \frac{n}{\ln 2n} \\ &= \frac{1}{4} \frac{2n}{\ln 2n} \\ &> \frac{1}{6} \frac{2n}{\ln 2n} \end{aligned}$$

So the left side inequality of (4.15) is proved for even positive integers $m = 2n$. We now prove it for $m = 2n + 1$. Since $2n/(2n+1) \geq 2/3$, we get

$$\begin{aligned} \pi(2n+1) &\geq \pi(2n) \\ &> \frac{1}{4} \frac{2n}{\ln 2n} \\ &> \frac{1}{4} \frac{2n}{2n+1} \frac{2n+1}{\ln(2n+1)} \\ &\geq \frac{1}{6} \frac{2n+1}{\ln(2n+1)} \end{aligned}$$

and this proves the left hand inequality of (4.15) for all $m \geq 2$.

We will now prove the other inequality of (4.15). We shall make use of proposition (4.6.3). Let α be an arbitrary real number such that $0 < \alpha < 1$. Then $n > n^\alpha$ and so $\pi(n) \geq \pi(n^\alpha)$. Using equation (4.13), one can write

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

This already means that

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

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:

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

□

Here is an interesting problem which combines several concepts. This problem appeared in Hardy and Wright,[16] and we are going to show an elegant solution by Nasehpour.[17]

Problem 4.6.9. Let r be a real number whose decimal representation is

$$\begin{aligned}r &= 0.r_1r_2 \ldots r_n \ldots \\ &= 0.011010100010 \ldots\end{aligned}$$

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. Now, by the definition of r and Prime Number Theorem,

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

and so r is irrational!

[16] Godfrey Harold Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford University Press, 1971, Chapter §9, section 9, 3, Theorem 137, Page 145.

[17] Peyman Nasehpour. "A computational criterion for the irrationality of some real numbers". In: (June 2018). URL: https://arxiv.org/abs/1806.07560v4.

Theorem 4.6.10 (Euler). *The sum*

$$\begin{aligned} S &= \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \dots \\ &= \sum_{p \in \mathbb{P}} \frac{1}{p} \end{aligned}$$

diverges i.e. does not have a finite summation.

The proof is due to Mixon.[18]

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,

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

[18] Dustin G. Mixon. "Another Simple Proof that the Sum of the Reciprocals of the Primes Diverges". In: *The American Mathematical Monthly* 120.9 (2013), pp. 831–831. DOI: 10.4169/amer.math.monthly.120.09.831. eprint: https://www.tandfonline.com/doi/pdf/10.4169/amer.math.monthly.120.09.831. URL: https://www.tandfonline.com/doi/abs/10.4169/amer.math.monthly.120.09.831.

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 using elementary means only. The starting point of the proof is known as what Selberg called *the Fundamental Identity*.

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 Möbius inversion theorem (theorem (3.3.3)).

□

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 4.7.3. *Let f and g be arithmetic functions. Then*[19]

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

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

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

□

Von Mangoldt Function. For any positive integer n, the von Mangoldt function, denoted by $\Lambda(n)$ is defined[20] 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 4.7.4. *Let n be a positive integer. Then* $\ln n = \sum_{d|n} \Lambda(d)$.

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

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

[19] 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.)

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

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 4.7.5 (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 (4.7.4) 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 (3.3.5)) 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 2.12.17, 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 2.12.1, $d \mid n-1$. 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

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

which is in contradiction with the second condition since q is a prime such that $q \mid x \mid n-1$. 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 appears in Koblitz.[21]

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. $q \mid n-1$ *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 2.4.9 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 $p \mid n$, 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 $p \mid a^{(n-1)/q} - 1$. Combining the latter result with $p \mid n$, we have

$$\begin{aligned}
p &\mid \left(a^{\frac{n-1}{q}} - 1, n\right) \\
&= 1
\end{aligned}$$

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 relatively prime 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*.

[21] Neal Koblitz. *A course in number theory and cryptography*. Springer, 2012, Chapter §VI, section 6.3, proposition 6.3.1, Page 187.

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

Definition. 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 (2.8.3). Then a is called an *Euler witness for compositeness of* n, or simply an *Euler witness for* n.

Theorem 4.8.4 (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 relatively prime to n,

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n} \tag{4.21}$$

So, if for some a relatively prime 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 (4.21) holds true for a composite integer n and an integer $a > 1$ relatively prime 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. Let $n = 2^s d + 1$ where s and d are positive integers and d is odd. Let $a > 1$ be an integer relatively prime to n. Then a is said to be a *witness for compositeness of* n, or simply a witness for n when

$$\begin{aligned} a^d &\not\equiv 1 \pmod{n} \\ a^{2^r d} &\not\equiv -1 \pmod{n} \end{aligned}$$

for $0 \leq r < s$.

Theorem 4.8.5 (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 $p \mid a^{p-1} - 1$ 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 4.8.6. *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 1.5.27 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, $p^v \mid n$ 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 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. 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 4.8.7. *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 1.5.23. □

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 4.8.8 (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 2.8.5),

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

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

Proof. See Theorem 1.5.22. □

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}[22] and M_{257}[23] 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 Ribenboim[24] for more details about Mersenne primes.

Theorem 4.8.10. *Let $q > 2$ be a prime. For every divisor n of M_q, we have*

$$\begin{aligned} n &\equiv \pm 1 \pmod 8 \\ n &\equiv 1 \pmod q \end{aligned}$$

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 $\operatorname{ord}_p(2) \mid q$, which means that $\operatorname{ord}_p(2) = q$ since q is a prime. By corollary (2.12.2), $q = \operatorname{ord}_p(2) \mid \varphi(p) = p - 1$. 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,

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

Theorem 2.8.13 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 Bruce[25] for a proof if interested.

Theorem 4.8.11 (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, $2047 = 23 \cdot 89$.

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

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

[24] Paulo Ribenboim. "The Little Book of Big Primes". In: (1991). DOI: 10.1007/978-1-4757-4330-2.

[25] J. W. Bruce. "A Really Trivial Proof of the Lucas-Lehmer Test". In: *The American Mathematical Monthly* 100.4 (1993), p. 370. DOI: 10.2307/2324959.

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.

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

Definition. 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.

Theorem 4.8.12 (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 4.8.13. *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*

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

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

$$x^{n-1} \equiv 1 \pmod{q} \tag{4.22}$$

$$x^{(n-1)/p} \not\equiv 1 \pmod{q} \tag{4.23}$$

because $q \mid n$. 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 $d \mid ma$. On the other hand, the congruence relation (4.22) shows that $d \mid n - 1 = p^k sa$. This implies $d \mid (ma, p^k sa)$. Suppose that $m = p^l t$. Then

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

(We have used propositions (1.2.1) and (1.2.7) in writing second and third lines.) Now, the congruence equation (4.23) implies that $d \nmid \frac{n-1}{p} = p^{k-1}as$, which is in contradiction with $d \mid a p^{\min(l,k)}(t, s)$. 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 $p_i \mid n$, 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 $p_i \mid n$, p_i would be the largest prime factor of n.

§§§4.9 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 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.

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.

§§§4.9 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. This algorithm is due to Pollard,[26] Brent.[27]

- 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:

$$\begin{aligned} x_0 &= c \\ x_{i+1} &\equiv g(x_i) \pmod{n} \end{aligned}$$

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

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

[26] J. M. Pollard. "A monte carlo method for factorization". In: *Bit* 15.3 (1975), pp. 331–334. DOI: 10.1007/bf01933667.

[27] Richard P. Brent. "An improved Monte Carlo factorization algorithm". In: *Bit* 20.2 (1980), pp. 176–184. DOI: 10.1007/bf01933190.

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 $x_0 = 2$. [28]

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 $T \mid k$. Then obviously $T \mid 2k$ 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 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.

[28] It was later found out that $g(x) = x^2 + 1$ usually work for almost all the cases.

i	x_i	$\mid x_{2i} - x_i \mid \pmod{391}$	$(\mid x_{2i} - x_i \mid, 391)$
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.

Example. Let us factorize $n = 391$ using Pollard's Rho algorithm. The process is shown in table 4.3. In 10^{th} step, where $(\mid x_{2i} - x_i \mid, 391)$ 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, 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	$\mid x_{2i} - x_i \mid \pmod{16843009}$	$(\mid x_{2i} - x_i \mid, 16843009)$
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 (4.6.6) 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 *Möbius 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

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

   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

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

   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 $p \nmid \binom{n}{k}$, then $p \nmid \binom{n+1}{k}$.

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

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

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,*

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

§§5 Special Topics

> 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 relatively prime to n. Then, there are integers x and y so that*

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

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, neither x nor 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 relatively prime 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 relatively prime 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*

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

Now we demonstrate some applications of the lemma. First, we show an elegant proof of Fermat's $4n + 1$ theorem, restated in theorem 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 a sum of two squares.*

Proof. We already know from theorem Theorem 2.8.7 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

$$p \leq a^2+b^2$$
$$a^2+b^2 < p+p = 2p$$

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

Remark. We can prove a stronger result than that of Theorem Theorem 5.1.5 using Fibonacci-Brahmagupta Identity (see Fibonacci-Brahmagupta Identity). 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 1.5.14), 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 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

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

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

Proof. First, assume that $p \mid x^2 + ny^2$. Then, y must be relatively prime 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

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

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

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

□

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 relatively prime integers x and y, then every divisor d of n is of the same form as n.*

Proof. According to the Fibonacci-Brahmagupta Identity,

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

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

$$\begin{aligned} n &= p_1^{e_1} \cdots p_k^{e_k} \\ &= \prod_{i=1}^{k} p_i^{e_i} \end{aligned}$$

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

$$d = \prod_{i=1}^{k} p_i^{f_i}$$

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 Theorem 5.1.8, $-D$ is a quadratic residue modulo p_i. Now, by theorem 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 theorem which we proved in section 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 $p \mid a^2 + ab + b^2$, 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 purpose of bounding! 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 relatively prime 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?

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 $a_1, \dots, a_n$ are natural numbers so that $(a_1, \dots, a_n) = 1$, the largest natural number that can not be written as $a_1x_1 + \dots a_nx_n$ for nonnegative $x_1, \dots, x_n$ is the Frobenius number. It is denoted as $F_n(a_1, \dots, a_n)$. Here, we will deal with the case $n = 2$, $F_2(a, b)$. The following theorem answers this question.

Theorem 5.2.5 (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 5.2.6. *$ab - a - b$ 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, $a \mid b(y + 1)$ but $a \perp b$. So, $a|y + 1$. Again, $b \mid a(x - b + 1)$ but $b \perp a$ so $b \mid x - b + 1$ or $b \mid x + 1$. We get $x + 1 \geq b$ and $y + 1 \geq a$, and so

$$\begin{aligned} x &\geq b - 1 \\ y &\geq a - 1 \end{aligned}$$

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. □

The above lemma shows that $F_2(a, b) \geq ab - a - b$. It only remains to prove the following lemma:

Lemma 5.2.7. *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

$$au + bv = 1 \tag{5.1}$$
$$\implies anu + bnv = n$$
$$\implies ax_0 + by_0 = n \tag{5.2}$$

We need to show that such $x_0, y_0 \geq 0$ exist. If (x_0, y_0) is a solution of equation (5.2), 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 5.2.8 (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 non-trivial 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 5.2.9 (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 non-negative 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. From McNugget theorem, any integer greater than $ab - a - b$ is good. So we substitute $ab - a - b + 1 + t$ for some non-negative t into the equation and 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. Again, every integer greater than $abc - ab - c$ is good. So we substitute $ct + zab = abc - ab - c + 1 + w$ for some non-negative w. Then

$$\begin{aligned} xbc + yca + zab &= abc - bc - ca + c + ct + zab \\ &= abc - bc - ca + c + abc - ab - c + 1 + w \\ &= 2abc - ab - bc - ca + 1 + w \end{aligned}$$

This shows that all integers greater than $2abc - ab - bc - ca$ are good. Finally, in order to prove the claim, we just have to show that $2abc - ab - bc - ca$ is bad. To the contrary, assume that $2abc - ab - bc - ca = xbc + yca + zab$ for some non-negative x, y, z. We have

$$bc(x + 1) + ca(y + 1) + ab(z + 1) = 2abc$$

Clearly, $a \mid x + 1$ because $a | bc(x + 1)$ but $\gcd(a, bc) = 1$. Similarly, $b \mid y + 1$ and $c \mid z + 1$. This gives us $bc(x + 1) + ca(y + 1) + ab(z + 1) \geq bca + cab + abc$ or $2abc \geq 3abc$ which is obviously wrong.

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

$$x_1 + x_2 = -\frac{b}{a}$$
$$x_1 x_2 = \frac{c}{a}$$

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

$$\begin{aligned} x &= \frac{b^2-k}{a} \\ &< \frac{b^2}{a} \\ &\leq \frac{a^2}{a} = a \end{aligned}$$

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

$$x = \frac{b^2+1}{a} \tag{5.3}$$

$$= kb - a \tag{5.4}$$

Equation (5.3) implies that x is positive and equation (5.4) implies that x is an integer. Now, if $a = b$, we already get that $k = \frac{1^2+1^2+1}{1 \cdot 1} = 3$. So we are left with $a > b$. But then,

$$\begin{aligned} x &= \frac{b^2+1}{a} \\ &< \frac{b^2+2b+1}{a} \\ &= \frac{(b+1)^2}{a} \\ &\leq \frac{a^2}{a} \\ &= a \end{aligned}$$

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:

$$\begin{aligned} x^2 - x(kb-b) + b^2 + k = 0 \\ \implies x + a = kb - b \\ \implies x = kb - a - b \\ xa = b^2 + k \\ \implies x = \frac{b^2+k}{a} \end{aligned}$$

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 $k = \dfrac{a^2+ab+b^2}{ab-1}$, so

$$\begin{aligned} &\frac{a^2+ab+b^2}{ab-1} \geq a^2-b^2 \\ \implies\ &a^2+ab+b^2 \geq (a^2-b^2)(ab-1) \\ &= ab(a+b)(a-b)-a^2+b^2 \\ \implies\ &a(a+b) \geq ab(a+b)(a-b)-a^2 \\ \implies\ &a \geq (a+b)(ab-b^2-1) \end{aligned} \tag{5.5}$$

(5.6)

If $a=b$, then $k = \dfrac{3a^2}{a^2-1}$. 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 $k = \dfrac{a^2+a+1}{a-1}$ so $a-1$ divides a^2+a+1.

$$\begin{aligned} &a-1 \mid a^2-1 \\ \implies\ &a-1 \mid a^2+a+1-(a^2-1) \\ &a+2 \\ \implies\ &a-1 \mid (a+2)-(a-1)=3 \end{aligned}$$

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 (5.6). 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 (1.4.3) 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*

$$g = (x-y, f(x,y,n)) \mid n$$

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

$$\begin{aligned} f(y,y,n) &= y^{n-1} + y^{n-2}\cdot y + \ldots + y^{n-1} \\ &= ny^{n-1} \end{aligned}$$

From Euclidean algorithm, we can infer

$$\begin{aligned} (x-y, f(x,y,n)) &= (x-y, f(y,y,n)) \\ &= (x-y, ny^{n-1}) \end{aligned}$$

Earlier we assumed $x \perp y$, and so $x - y \perp y^{n-1}$ because $(x-y, y) = (x,y) = 1$. Thus

$$\begin{aligned} g &= (x-y, f(x,y,n)) \\ &= (x-y, n) \end{aligned}$$

which results in $g \mid n$. □

Corollary 5.4.2. *The following result is true for any odd positive integer n:*

$$\left(x+y, \frac{x^n + y^n}{x+y}\right) \mid n$$

Corollary 5.4.3. *For a prime p,*

$$(x-y, f(x,y,p)) \in \{1, p\}$$

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,

$$g = (x + y, f(x, y, 3))$$
$$g \mid (x + y, 3)$$

This means $g \mid 3$. If $g = 3$, then we have $3 \mid p$ 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, $p - 1\left|\dfrac{p^x - 1}{p - 1}\right.$ and so from the lemma, $p - 1|x$ or $x \geq p - 1$. So

$$\begin{aligned}(p - 1)! &= p^x - 1 \\ &\geq p^{p-1} - 1\end{aligned}$$

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 (2.4.13) of chapter (2).

Lemma 5.5.1. *Let a, b, and n be three positive integers such that $(a, n) = (b, n) = 1$ and*

$$a^x \equiv b^x \pmod{n}$$
$$a^y \equiv b^y \pmod{n}$$

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 (2.12.1) 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 $h \mid k$.

Proof. From the lemma, we have $a^{(h,k)} \equiv b^{(h,k)} \pmod{n}$. We have $(h,k) \leq h$ and $(h,k) \mid k$. Now, if $(h,k) < h$ then (h,k) is smaller than h which satisfies the condition. So we must have $(h,k) = h$, or $h \mid k$. □

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 $d \mid (p-1, k)$.*

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, $d \mid (k, p-1)$. □

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 (2.4.13). 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 $pq \mid p^p + q^q + 1$.

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 $pq \mid (5^p - 2^p)(5^q - 2^q)$.

Solution. If $p \mid 5^p - 2^p$, 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, $q \mid 5^p - 2^p = 5^3 - 2^3 = 117 = 3^2 \cdot 13$ so $q = 13$. Now, we can assume $p \mid 5^q - 2^q$ and $q \mid 5^p - 2^p$. 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 is actually an overkill for many 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 (1.4.3) 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 $6x + 1 = 2 \cdot 3 \cdot x + 1$ is odd, we can write

$$2^{6x+1} + 1 = (2+1)\left(2^{6x} - 2^{6x-1} + 2^{6x-2} - \cdots - 2 + 1\right)$$

$\left(2^{6x} - 2^{6x-1} + 2^{6x-2} - \cdots - 2 + 1\right)$ is not divisible by 3 (try to figure out why, using induction on x). Therefore

$$\begin{aligned} v_3\left(2^{6x+1}+1\right) &= v_3(2+1) + v_3\left(2^{6x} - 2^{6x-1} + 2^{6x-2} - \cdots - 2 + 1\right) \\ &= 1 + 0 \\ &= 1 \end{aligned}$$

This means that $2y = 1$, which is impossible since y is an integer.

§§§5.6 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*

$$v_p\left(x^n - y^n\right) = v_p(x - y)$$

Proof. We use the fact that

$$x^n - y^n = (x-y)\left(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + y^{n-1}\right)$$

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*

$$v_p\left(x^n + y^n\right) = v_p(x + y)$$

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

$$\begin{aligned} & v_p\left(x^n - (-y)^n\right) = v_p(x - (-y)) \\ \implies & v_p\left(x^n + y^n\right) = v_p(x + y) \end{aligned}$$

Note that since n is an odd positive integer we can replace $(-y)^n$ with $-y^n$. □

§§§5.6 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:

$$v_p(x^p - y^p) = v_p(x - y) + 1 \tag{5.7}$$

In order to prove this, we will show that

$$p \mid x^{p-1} + x^{p-2}y + \cdots + xy^{p-2} + y^{p-1} \tag{5.8}$$

and

$$p^2 \nmid x^{p-1} + x^{p-2}y + \cdots + xy^{p-2} + y^{p-1} \tag{5.9}$$

For (5.8), 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

$$\begin{aligned}
y^tx^{p-1-t} &\equiv (x+kp)^tx^{p-1-t}\\
&\equiv x^{p-1-t}\left(x^t+t(kp)(x^{t-1})+\frac{t(t-1)}{2}(kp)^2(x^{t-2})+\cdots\right)\\
&\equiv x^{p-1-t}\left(x^t+t(kp)(x^{t-1})\right)\\
&\equiv x^{p-1}+tkpx^{p-2} \pmod{p^2}
\end{aligned}$$

This means

$$y^tx^{p-1-t}\equiv x^{p-1}+tkpx^{p-2} \pmod{p^2}$$

Using this fact, we have

$$\begin{aligned}
&x^{p-1}+x^{p-2}y+\cdots+xy^{p-2}+y^{p-1}\\
&\quad\equiv x^{p-1}+\left(x^{p-1}+kpx^{p-2}\right)+\left(x^{p-1}+2kpx^{p-2}\right)+\cdots+\left(x^{p-1}+(p-1)kpx^{p-2}\right)\\
&\quad\equiv px^{p-1}+(1+2+\cdots+p-1)\,kpx^{p-2}\\
&\quad\equiv px^{p-1}+\left(\frac{p(p-1)}{2}\right)kpx^{p-2}\\
&\quad\equiv px^{p-1}+\left(\frac{p-1}{2}\right)kp^2x^{p-1}\\
&\quad\equiv px^{p-1}\\
&\quad\not\equiv 0 \pmod{p^2}
\end{aligned}$$

So we proved the relation (5.9) and the proof of equation (5.7) 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

$$\begin{aligned}
v_p(x^n-y^n) &= v_p\left((x^{p^\alpha})^b-(y^{p^\alpha})^b\right)\\
&= v_p\left(x^{p^\alpha}-y^{p^\alpha}\right)=v_p\left((x^{p^{\alpha-1}})^p-(y^{p^{\alpha-1}})^p\right)\\
&= v_p\left(x^{p^{\alpha-1}}-y^{p^{\alpha-1}}\right)+1=v_p\left((x^{p^{\alpha-2}})^p-(y^{p^{\alpha-2}})^p\right)+1\\
&= v_p\left(x^{p^{\alpha-2}}-y^{p^{\alpha-2}}\right)+2\\
&\;\;\vdots\\
&= v_p\left((x^{p^1})^1-(y^{p^1})^1\right)+\alpha-1=v_p\left(x-y\right)+\alpha\\
&= v_p\left(x-y\right)+v_p\left(n\right)
\end{aligned}$$

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 (5.7.1)), 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 $0 \le i < k$.*

§§§5.6 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*

$$v_2\left(x^n - y^n\right) = v_2(x-y) + v_2(n)$$

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*

$$v_2\left(x^n - y^n\right) = v_2(x-y) + v_2(x+y) + v_2(n) - 1$$

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

$$\begin{aligned} v_2\left(x^n - y^n\right) &= v_2\left(x^{m\cdot 2^k} - y^{m\cdot 2^k}\right) \\ &= v_2\left((x^2)^{2^{k-1}} - (y^2)^{2^{k-1}}\right) \\ &\vdots \\ &= v_2\left(x^2 - y^2\right) + k - 1 \\ &= v_2(x-y) + v_2(x+y) + v_2(n) - 1 \end{aligned}$$

□

§§§5.6 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
$$v_p\left(x^n - y^n\right) = v_p(x-y) + v_p(n)$$
- if $p = 2$ and $4 \mid x - y$, then
$$v_2\left(x^n - y^n\right) = v_2(x-y) + v_2(n)$$
- if $p = 2$, n is even, and $2 \mid x - y$, then
$$v_2\left(x^n - y^n\right) = v_2(x-y) + v_2(x+y) + v_2(n) - 1$$

(b) For an odd positive integer n, if $p \mid x + y$, then

$$v_p\left(x^n + y^n\right) = v_p(x+y) + v_p(n)$$

(c) For a positive integer n with $\gcd(p, n) = 1$, if $p \mid x - y$, we have

$$v_p\left(x^n - y^n\right) = v_p(x-y)$$

If n is odd, $\gcd(p, n) = 1$, and $p \mid x + y$, then we have

$$v_p\left(x^n + y^n\right) = v_p(x+y)$$

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 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

$$\begin{aligned} 1 + 2^k &= 3^{v_3(k)+1} \\ &= 3 \cdot \underbrace{3^{v_3(k)}}_{\leq k} \\ &\leq 3k \\ \implies 2^k + 1 &\leq 3k \end{aligned}$$

   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

$$v_q(x_1^p + y_1^p) = v + v_q(p)$$
$$v_q(d^{m-p}(x_1 + y_1)^m) \geq mv$$

   (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

$$b^a \mid a^b - 1$$

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

$$\begin{aligned} a - 1 &\leq (a-1)v_p(b) \\ &\leq v_p(a-1) \end{aligned}$$

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

$$\begin{aligned} a &\leq (a-1)v_2(b) + 1 \\ &\leq v_2(a-1) + v_2(a+1) \end{aligned}$$

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. We do not prove this theorem here, interested readers can see Billal and Riasat[1] for a proof (it is completely elementary although a little beyond the scope of this book).

Primitive Divisor. For a sequence of integers $a_1, a_2, \cdots, a_n, \cdots$ 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.

[1] Masum Billal and Samin Riasat. *Integer sequences: Divisibility, Lucas and Lehmer sequences*. 1st ed. Springer, 2021, §6.2.

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 5.7.1 (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 5.7.2 (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 $a^k + b^k$.

$$\begin{aligned} p \mid a^l(a^n + b^n) \\ = a^k + a^l b^n \\ p \mid b^l(a^n + b^n) \\ = a^n b^l + b^k \end{aligned}$$

Therefore

$$p \mid a^k + a^l b^n + a^n b^l + b^k$$

We already know $p | a^k + b^k$, so if $n = l + m$ (since $l \leq n$), then

$$\begin{aligned} p \mid a^l b^n + a^n b^l \\ = a^l b^l (a^m + b^m) \end{aligned}$$

Since $p \perp ab$, we have $p \perp a^l b^l$. So $p \mid a^m + b^m$ where $m < n$, which is a contradiction. □

In a similar fashion, we can prove the following theorem.

Theorem 5.7.3 (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 from the 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 5.7.4 (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 5.7.5 (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 5.7.6 (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

$$(a, b, p, n) \in \{(2 \cdot 3^r, 3^r, 3, 3r + 2), (3^r, 2 \cdot 3^r, 3, 3r + 2)\}$$

for any positive integer r.

The next problem is from the IMO Shortlist.

Problem 5.7.7 (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 generalized form of this problem. You can certainly see how much the problem can be improved with this theorem.

Theorem 5.7.8. *If $p_1, p_2, \dots, p_n$ 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 5.7.9. *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 $M = p_1 p_2 \dots p_n$ has $\underbrace{(1+1)(1+1)\dots(1+1)}_{n \text{ times}} = 2^n$ divisors. Say the divisors are

$$1 = d_1 < d_2 < \cdots < d_{2^n} = p_1 \cdots p_n$$

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 $q_1, q_2, \dots, q_{2^n}$. Then,

$$N = q_1 q_2 \cdots q_{2^n} K$$

for some integer $K \geq 1$. Thus, every divisor of $D = q_1 q_2 \dots q_{2^n}$ is a divisor of N and so, N has at least 2^{2^n} divisors. □

This theorem can be generalized even more.

Theorem 5.7.10. *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 5.7.11 (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 5.7.12 (IMO Shortlist 2000). Find all positive integers a, m, and n such that

$$a^m + 1 \mid (a+1)^n$$

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.

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:

$$A_{m\times n} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

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

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

$$B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \\ 7 & 8 \end{pmatrix}$$

$$C = \begin{pmatrix} -1 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

A is 3×3, B is 4×2, and C is 2×4.

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.

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 $i = j$.

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.

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

$$A_{m\times n} + B_{m\times n} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix}$$

$$= \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \cdots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \cdots & a_{2n}+b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}+b_{m1} & a_{m2}+b_{m2} & \cdots & a_{mn}+b_{mn} \end{pmatrix}$$

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

$$A_{m\times n} \times B_{n\times p} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1p} \\ b_{21} & b_{22} & \cdots & b_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{np} \end{pmatrix}$$

$$= \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1p} \\ c_{21} & c_{22} & \cdots & c_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mp} \end{pmatrix}$$

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

$$A = \begin{pmatrix} 1 & 1 & 5 \\ 2 & 3 & 1 \\ 4 & 6 & 1 \\ 2 & 1 & 3 \end{pmatrix}$$

$$B = \begin{pmatrix} 3 & 1 & 0 & 2 \\ 5 & 1 & 0 & 1 \\ 4 & 0 & 1 & 1 \end{pmatrix}$$

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

$$\begin{pmatrix} \boxed{1} & \boxed{1} & \boxed{5} \\ 2 & 3 & 1 \\ 4 & 6 & 1 \\ 2 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} \boxed{3} & 1 & 0 & 2 \\ \boxed{5} & 1 & 0 & 1 \\ \boxed{4} & 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} \boxed{c_{11}} & c_{12} & c_{13} & c_{14} \\ c_{21} & c_{22} & c_{23} & c_{24} \\ c_{31} & c_{32} & c_{33} & c_{34} \\ c_{41} & c_{42} & c_{43} & c_{44} \end{pmatrix}$$

From the definition, the entry c_{11} of C is calculated by multiplying the corresponding entries of the first row of A and the 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*.

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.

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 the determinant. We will first explain how to calculate the determinant of a 2×2 matrix and then move to the precise definition of determinants.

Definition. The determinant of a 2×2 matrix is the product of entries on its main diagonal minus the product of the 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. For this, you need to know what cofactors and minors are first.

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

$$A = \begin{pmatrix} \boxed{1} & 1 & 5 \\ \boxed{2} & 3 & 1 \\ \boxed{4} & 6 & 1 \end{pmatrix}$$

The corresponding row and column (which should be deleted in order to calculate the minor) are shown in the matrix. Therefore, $M_{21} = \begin{vmatrix} 1 & 5 \\ 6 & 1 \end{vmatrix} = 1 - 30 = -29.$

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

$$M = \begin{pmatrix} 3-6 & 2-4 & 12-12 \\ 1-30 & 1-20 & 6-4 \\ 1-15 & 1-10 & 3-2 \end{pmatrix} = \begin{pmatrix} -3 & -2 & 0 \\ -29 & -19 & 2 \\ -14 & -9 & 1 \end{pmatrix}$$

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 an even number, then the cofactor is the same as the minor. If the row and column of the entry add up to 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 are now be able to make sense of the 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 the matrix of minors and the 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. 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

$$\begin{aligned} \det(A) &= a_{1j}C_{1j} + a_{2j}C_{2j} + a_{3j}C_{3j} + \cdots + a_{nj}C_{nj} \\ &= \sum_{i=1}^{n} a_{ij}C_{ij} \end{aligned}$$

The cofactor expansion along the i^{th} row gives:

$$\begin{aligned} \det(A) &= a_{i1}C_{i1} + a_{i2}C_{i2} + a_{i3}C_{i3} + \cdots + a_{in}C_{in} \\ &= \sum_{j=1}^{n} a_{ij}C_{ij} \end{aligned}$$

Example. Consider the matrix A in the previous examples. If we use the cofactor expansion along the second column, we get

$$\begin{aligned}\det(A) &= a_{12}C_{12} + a_{22}C_{22} + a_{32}C_{32} \\ &= 1 \cdot 2 + 3 \cdot (-19) + 6 \cdot 9 \\ &= -1\end{aligned}$$

Also, if we use the cofactor expansion along the third row, we get

$$\begin{aligned}\det(A) &= a_{31}C_{31} + a_{32}C_{32} + a_{33}C_{33} \\ &= 4 \cdot (-14) + 6 \cdot 9 + 1 \cdot 1 \\ &= -1\end{aligned}$$

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 the 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 basics and you can find the determinant of any $n \times n$ matrix. It's just the matter of time it takes to find it.

The definition of the 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 theoretical approach. We will only use the formula for determinant of 2×2 matrices, however we included the definition of the 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 book on *linear algebra*.

Theorem 5.8.1. *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 5.8.2. *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 5.8.3 (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 5.8.4. 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 the determinant of some matrix. This is pretty simple. Assume the matrices

$$\mathcal{M} = \begin{pmatrix} x & yd \\ -y & x \end{pmatrix}$$
$$\mathcal{N} = \begin{pmatrix} u & vd \\ -v & u \end{pmatrix}$$

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) 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 5.8.5. 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 5.8.6. 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

$$\mathcal{A} = \begin{pmatrix} a & b \\ -b & a+b \end{pmatrix}$$
$$\mathcal{B} = \begin{pmatrix} c & d \\ -d & c+d \end{pmatrix}$$

After this, the process is analogous to previous problems.

Note. We could factorize a^2+ab+b^2 as $(a+\xi b)(a+\xi^2 b)$, where $\xi^3 = 1$ is the third root of unity (don't worry if this is unfamiliar for you, it needs some knowledge in complex numbers).

§§§5.8 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:

$$0, 1, 1, 2, 3, 5, 8, 13, \cdots$$

We define general Fibonacci numbers G_n by

$$G_n = \begin{cases} a & \text{if } n = 0 \\ b & \text{if } n = 1 \\ n = pG_{n-1} + qG_{n-2} & \text{if } n > 1 \end{cases}$$

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 5.8.7.

$$\begin{pmatrix} p & q \\ 1 & 0 \end{pmatrix}^{n-1} \begin{pmatrix} G_2 & G_1 \\ G_1 & G_0 \end{pmatrix} = \begin{pmatrix} G_{n+1} & G_n \\ G_n & G_{n-1} \end{pmatrix} \tag{5.10}$$

Corollary 5.8.8.

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$$

Proof. We can use induction. It's rather straight-forward. □

Theorem 5.8.9.

$$G_{n+1}G_{n-1} - G_n^2 = (-1)^{n-1}q^{n-1}\left(a^2p + abq - b^2\right)$$

Proof. Take determinant of both sides of equation (5.10). □

Applying the above theorem for Fibonacci and Lucas sequences, we find the following corollaries.

Corollary 5.8.10.

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n$$

Corollary 5.8.11.

$$L_{n+1}L_{n-1} - L_n^2 = 5 \cdot (-1)^{n-1}$$

Problem 5.8.12. Prove that

$$F_{m+n+1} = F_{m+1}F_{n+1} + F_mF_n \tag{5.11}$$

Solution. Consider $I = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Then, $I^{m+n} = I^mI^n$. Note that

$$I^m = \begin{pmatrix} F_{m+1} & F_m \\ F_m & F_{m-1} \end{pmatrix}$$
$$I^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$$
$$I^{m+n} = \begin{pmatrix} F_{m+n+1} & F_{m+n} \\ F_{m+n} & F_{m+n-1} \end{pmatrix}$$

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 5.8.13.

$$F_{mk+n} = F_{mk+1}F_n + F_{mk}F_{n-1}$$

Corollary 5.8.14. *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 matrices can actually be.

§§5.9 A Proof for the Law of Quadratic Reciprocity

Law of quadratic reciprocity (theorem (2.8.16)) 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*[2]. 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 (2.8.14)).

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

$$ka = pq_k + r_k$$
$$-\frac{p-1}{2} < r_k < \frac{p-1}{2}$$

[2] Do not confuse it with Einstein.

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

$$\begin{aligned}\left\lfloor \frac{ka}{p} \right\rfloor &= q_k + \left\lfloor \frac{r_k}{p} \right\rfloor \\ -\frac{1}{2} &< \frac{r_k}{p} \\ &< \frac{1}{2}\end{aligned}$$

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

$$\begin{aligned}\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor &\equiv \sum_{k=1}^{\frac{p-1}{2}} q_k - \mu(a,p) \\ &\equiv 0 - \mu(a,p) \\ &\equiv \mu(a,p) \pmod 2\end{aligned}$$

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 $r_1, r_2, \dots, r_{\frac{p-1}{2}}$ are equal to the numbers $\pm 1, \pm 2, \dots, \pm\frac{p-1}{2}$ in some order, with each number appearing once with either a plus

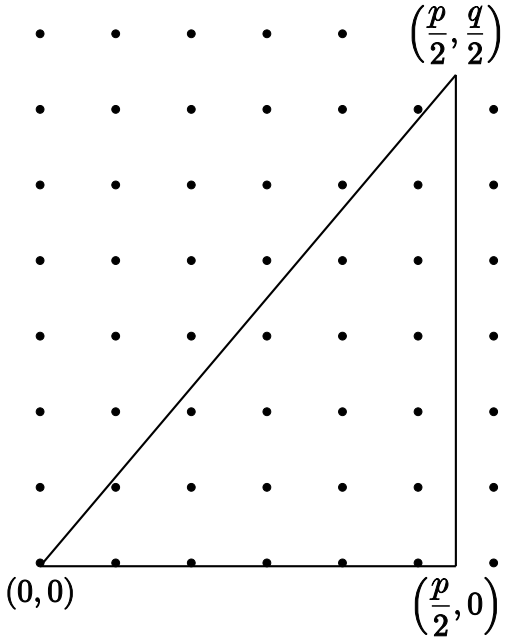
sign or a minus sign. We also know that $x \equiv -x \pmod 2$ for any integer x. So, we can say that

$$\sum_{k=1}^{\frac{p-1}{2}} r_k \equiv \sum_{k=1}^{\frac{p-1}{2}} k \pmod 2$$
$$\implies \sum_{k=1}^{\frac{p-1}{2}} q_k \equiv 0 \pmod 2$$

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 $(p/2,q/2)$.

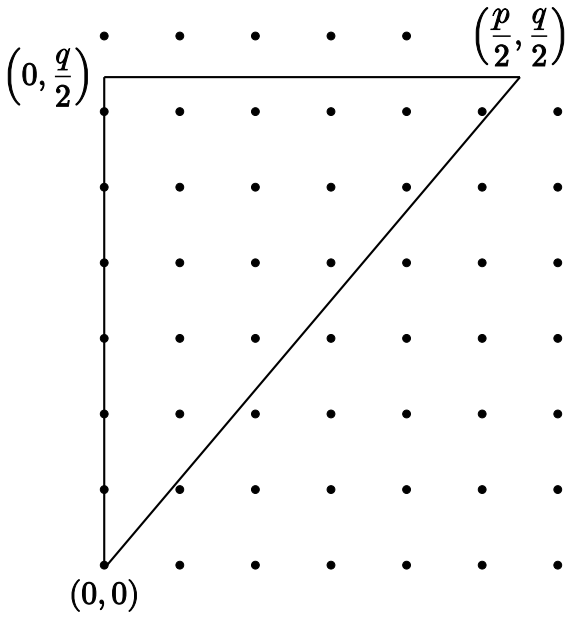


The number of points with integer coordinates inside this triangle equals

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor.$$

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 $1 \le k \le \frac{p-1}{2}$) 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 $y = 1, y = 2, ...,$ 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 $(p/2, q/2)$.

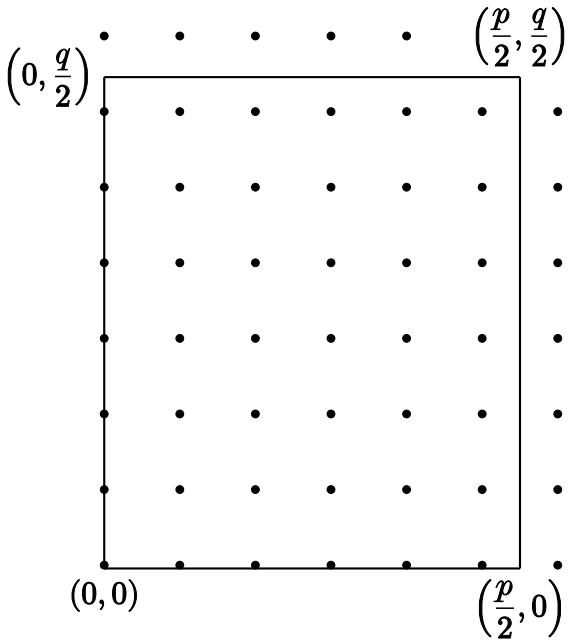
Let x be number of the points with integer coordinates inside this rectangle. Obviously, x is equal to the sum of such points in triangles (notice that since p and q are different, there is no point with integer coordinates on the hypotenuse of triangles). So

$$x = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor$$

According to lemma (5.9), it follows that

$$x \equiv \mu(q, p) + \mu(p, q) \pmod 2 \tag{5.12}$$

Let's count x in another way.



Clearly, number of points with integer coordinates inside this rectangle is

$$x = \left\lfloor \frac{p}{2} \right\rfloor \cdot \left\lfloor \frac{q}{2} \right\rfloor \tag{5.13}$$

$$= \frac{p-1}{2} \cdot \frac{q-1}{2} \tag{5.14}$$

Combining equations (5.12) and (5.13),

$$\mu(q,p) + \mu(p,q) \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} \pmod 2$$

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 (1.4.3) 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. 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 (1.4.3).

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 $p \mid a$, then $v_p(x) > 0$. If p divides none of a and b, then $v_p(x) = 0$. And if $p \mid b$, then $v_p(x) < 0$. Also, $v_p(xy) = v_p(x) + v_p(y)$ and $v_p(x+y) \geq \min\left(v_p(x), v_p(y)\right)$ for all rationals x and y.

We can now generalize the concept of congruency to include rational numbers.

Definition. 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 5.10.1. Let $p \geq 3$ be a prime. Prove that $p \mid 2^{p-2} + 3^{p-2} + 6^{p-2} - 1$.

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

$$\begin{aligned} 2^{p-2} + 3^{p-2} + 6^{p-2} - 1 &\equiv \frac{1}{2} + \frac{1}{3} + \frac{1}{6} - 1 \\ &\equiv 0 \pmod{p} \end{aligned}$$

Theorem 5.10.2 (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 5.10.3. *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 $A = \{0, 1^n, 2^n, \dots, (p-1)^n\}$ forms a compete residue system modulo p (why?). Proposition (2.3.2) says that the set $B = \{0, a^n, (2a)^n, \dots, ((p-1)a)^n\}$ also forms a complete residue system modulo p. Therefore, the sum of elements of both sets are equivalent modulo p. So

$$\begin{aligned}\sum_{k=1}^{p-1} k^n &\equiv \sum_{k=1}^{p-1} (a \cdot k)^n \\ &\equiv a^n \sum_{k=1}^{p-1} k^n \pmod{p}\end{aligned}$$

This means that

$$(a^k - 1) \sum_{k=1}^{p-1} k^n \equiv 0 \pmod{p}$$

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 $\{1, 2, \dots, p-1\}$ can be generated by g (the set $\{1, g, g^2, \dots, g^{p-2}\}$). 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

$$\begin{aligned} p^{u-1} - up^{u-2}k + \cdots + uk^{u-1} &\equiv uk^{u-1} \pmod{p} \\ k^u (p-k)^u &\equiv k^u (-k)^u \\ &\equiv (-1)^u k^{2u} \pmod{p} \end{aligned}$$

we should prove that

$$\begin{aligned} \sum_{k=1}^{p-1} \frac{uk^{u-1}}{(-1)^u k^{2u}} &\equiv \frac{u}{(-1)^u} \sum_{k=1}^{p-1} k^{-u-1} \\ &\equiv 0 \pmod{p} \end{aligned}$$

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

$$\begin{aligned} k^{-u-1} &\equiv k^{-u-1} k^{p-1} \\ &= k^{p-u-2} \pmod{p} \end{aligned}$$

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 (5.10.3) because $1 \leq p-u-2 \leq p-2$. The proof is complete. □

Problem 5.10.4. 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

$$p - \lfloor \lfloor 2p/3 \rfloor / 2 \rfloor = \lfloor 2p/3 \rfloor + 1 \tag{5.15}$$

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

$$\begin{aligned} 2 \cdot \frac{p-1}{3} &\leq \frac{2p}{3} \\ &< 2 \cdot \frac{p-1}{3} + 1 \end{aligned}$$

which means

$$\begin{aligned}\left\lfloor \frac{2p}{3} \right\rfloor &= 2 \cdot \frac{p-1}{3} \\ \left\lfloor \left\lfloor \frac{2p}{3} \right\rfloor /2 \right\rfloor &= \left\lfloor \left(2 \cdot \frac{p-1}{3} \right) /2 \right\rfloor \\ &= \frac{p-1}{3}\end{aligned}$$

Finally,

$$\begin{aligned}p - \left\lfloor \left\lfloor \frac{2p}{3} \right\rfloor /2 \right\rfloor &= p - \frac{p-1}{3} \\ &= 2 \cdot \frac{p-1}{3} + 1 \\ &= \left\lfloor \frac{2p}{3} \right\rfloor + 1\end{aligned}$$

as desired.

- If $p \equiv 2 \pmod 3$, then $\frac{p-2}{3}$ is an integer and

$$\begin{aligned}2 \cdot \frac{p-2}{3} + 1 &\le \frac{2p}{3} \\ &< \left(2 \cdot \frac{p-2}{3} + 1 \right) + 1\end{aligned}$$

This gives

$$\begin{aligned}\left\lfloor \frac{2p}{3} \right\rfloor &= 2 \cdot \frac{p-2}{3} + 1 \\ \left\lfloor \left\lfloor \frac{2p}{3} \right\rfloor /2 \right\rfloor &= \left\lfloor \left(2 \cdot \frac{p-2}{3} + 1 \right) /2 \right\rfloor \\ &= \left\lfloor \frac{p-2}{3} + \frac{1}{2} \right\rfloor \\ &= \frac{p-2}{3}\end{aligned}$$

And finally

$$\begin{aligned}p - \left\lfloor \left\lfloor \frac{2p}{3} \right\rfloor /2 \right\rfloor &= p - \frac{p-2}{3} \\ &= \left(2 \cdot \frac{p-2}{3} + 1 \right) + 1 \\ &= \left\lfloor \frac{2p}{3} \right\rfloor + 1\end{aligned}$$

The proof of equation (5.15) 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 (5.15), 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. 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

$$\begin{aligned}(10!)_5 &= 9 \times 8 \times 7 \times 6 \times 4 \times 3 \times 2 \times 1 \\ &= 72,576\end{aligned}$$

Theorem 5.11.1. *Let p be a prime number and let $(n_k n_{k-1} \cdots n_1 n_0)_p$ 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 $1, 2, \cdots, n$ are

$$\begin{array}{cccccc} 1 & 2 & \cdots & n_0 & \cdots & p-1 \\ p+1 & p+2 & \cdots & p+n_0 & \cdots & 2p-1 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ ([\frac{n}{p}]-1)p+1 & ([\frac{n}{p}]-1)p+2 & \cdots & ([\frac{n}{p}]p-1)p+n_0 & \cdots & [\frac{n}{p}]p-1 \\ [\frac{n}{p}]p+1 & [\frac{n}{p}]p+2 & \cdots & [\frac{n}{p}]p+n_0 & & \end{array}$$

Product of these numbers, $(n!)_p$ is

$$\left(\prod_{k=0}^{[\frac{n}{p}]-1} ((kp+1)\cdot(kp+2)\cdots(kp+p-1))\right) \cdot \left([\tfrac{n}{p}]p+1\right)\left([\tfrac{n}{p}]p+2\right)\ldots\left([\tfrac{n}{p}]p+n_0\right)$$

which is equal to

$$\begin{aligned}\left(\prod_{k=0}^{[\frac{n}{p}]-1} (1\cdot 2\cdots(p-1))\right) \cdot \left([\tfrac{n}{p}]p+1\right)\left([\tfrac{n}{p}]p+2\right)\ldots\left([\tfrac{n}{p}]p+n_0\right) &\equiv \left(\prod_{k=0}^{[\frac{n}{p}]-1} (-1)\right)\cdot(1\cdot 2\cdots n_0) \\ &\equiv (-1)^{[\frac{n}{p}]} n_0! \pmod{p}\end{aligned}$$

□

Proposition 5.11.2. *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

$$\begin{aligned} & a^2 \equiv 1 \pmod{p^n} \\ \implies & p^n \mid (a-1)(a+1) \end{aligned}$$

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 5.11.3. Prove that $(2^n!)_2 \equiv 1 \pmod{2^n}$.

We are ready to prove the following theorem.

Theorem 5.11.4 (Generalization of Wilson's Theorem). *Let p be a prime number and let $(n_k n_{k-1} \cdots n_1 n_0)_p$ be the representation of a positive integer n in base p. Then*

$$\frac{n!}{p^{v_p(n!)}} \equiv (-1)^{v_p(n!)} n_0! n_1! \ldots n_k! \pmod{p} \tag{5.16}$$

Proof. According to theorem (5.11.1), 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 2.12.21.

Theorem 5.11.5 (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*

$$\begin{aligned} m &= m_k p^k + m_{k-1} p^{k-1} + \cdots + m_1 p + m_0 \\ n &= k_k p^k + n_{k-1} p^{k-1} + \cdots + n_1 p + n_0 \\ r &= r_k p^k + r_{k-1} p^{k-1} + \cdots + r_1 p + r_0 \end{aligned}$$

Also, let $\ell = v_p\left(\binom{m}{n}\right)$. Then

$$\frac{1}{p^\ell} \binom{m}{n} \equiv (-1)^\ell \left(\frac{m_0!}{n_0! r_0!} \right) \left(\frac{m_1!}{n_1! r_1!} \right) \ldots \left(\frac{m_d!}{n_d! r_d!} \right) \pmod{p}$$

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 (5.11.4), 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.

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[3] stated 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:

[3]Robert Daniel Carmichael. "On Euler's φ-function". In: *Bull. Amer. Math. Soc.* 13 (1907), pp. 241–243.

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, Jr[4] pointed out 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 5.12.2. *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 5.12.3. *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 $p^2 \mid x$.*

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 $p \mid s$ and hence $p^2 \mid x$. □

Here is a very nice result that provides us with a sufficient condition for $N(x) = 1$ to happen. The result is due to Pomerance.[5]

Theorem 5.12.4 (Carl Pomerance). *Let x be a positive integer. Suppose that the following property holds for every prime p:*

$$\begin{aligned}&p - 1 \mid \varphi(x) \\ \implies\ &p^2 \mid x\end{aligned}$$

Then $N(x) = 1$. That is, if $\varphi(y) = \varphi(x)$ for some positive integer y, then $y = x$.

[4] Victor Klee Jr. "On a conjecture of Carmichael". In: *Bulletin of the American Mathematical Society* 53.12 (1947), pp. 1183–1187. DOI: 10.1090/s0002-9904-1947-08940-0.

[5] Carl Pomerance. "On Carmichael's Conjecture". In: *Proceedings of the American Mathematical Society*. 2nd ser. 43 (Apr. 1974), pp. 297–298.

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 $p-1 \mid \varphi(x)$ then $p^2 \mid x$. 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 $p - 1 \mid \varphi(y) = \varphi(x)$. So, from the assumption, $p^2 \mid x$ 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 $p^{e-1} \mid \varphi(n)$. 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 $p \mid q-1$ for any such q, those will contribute to $\nu_p(\varphi(n))$ as well. That is,

$$\nu_p(\varphi(n)) = \nu_p(n) - 1 + \sum_{q \in S(n)} \nu_p(q-1)$$

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 $\nu_p(\varphi(n))$. In other words,

$$\nu_p(\varphi(n)) = \sum_{q \in S(n)} \nu_p(q-1)$$

Combining these two results, we find out that for any prime p and any positive integer n,

$$\nu_p(\varphi(n)) = \begin{cases} \sum_{q \in S(n)} \nu_p(q-1) & \text{if } p \nmid n \\ \nu_p(n) - 1 + \sum_{q \in S(n)} \nu_p(q-1) & \text{otherwise} \end{cases}$$

Let p be a prime factor of x. Since $\varphi(x) = \varphi(y)$, for any prime p, we must have

$$\nu_p(\varphi(x)) = \nu_p(\varphi(y))$$

There are two cases to consider.

1. $p \notin S(y)$ or $p \nmid y$. Then,

$$\begin{aligned} \nu_p(x) - 1 + \sum_{q \in S(x)} \nu_p(q-1) &= \sum_{q \in S(y)} \nu_p(q-1) \\ &\le \sum_{q \in S(x)} \nu_p(q-1) \end{aligned}$$

since $S(y) \subseteq S(x)$. The latter result implies $\nu_p(x) \le 1$. But this is impossible since $\nu_p(x) \ge 2$ due to the fact that $p^2 \mid x$.

2. $p \in S(y)$. That is, $p \mid y$, or $S(x) = S(y)$. In this case we should expect to get $x = y$. One way to prove this is to show that $\nu_p(x) = \nu_p(y)$. Notice that

$$\begin{aligned}\nu_p(x) &= \nu_p(\varphi(x)) + 1 - \sum_{q \in S(x)}{}' \nu_p(q-1) \\ &= \nu_p(\varphi(y)) + 1 - \sum_{q \in S(y)}{}' \nu_p(q-1)\end{aligned}$$

since $\varphi(x) = \varphi(y)$ and $S(x) = S(y)$. So, $\nu_p(x) = \nu_p(y)$.

which was what we wanted. □

Gupta[6] 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 5.12.5 (Gupta). *Let m and n be two positive integers such that $n \in \varphi^{-1}(m)$. Then,*

$$m < n \leq m \prod_{p-1 \mid m} \frac{p}{p-1}$$

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

$$\begin{aligned}\frac{n}{\varphi(n)} &= \prod_{p \mid n} \frac{p}{p-1} \\ &\leq \prod_{p-1 \mid m} \frac{p}{p-1}\end{aligned}$$

The last line is true because if $p \mid n$ then $p - 1 \mid m$ must hold, but the converse is not true. If $p - 1 \mid m$, p may or may not divide n. □

Now we will look at the elements of $\varphi^{-1}(m)$.

Theorem 5.12.6. *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 5.12.7. *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.*

[6] Hansraj Gupta. "Euler's Totient Function And Its Inverse". In: *Indian J. Pure Appl. Math* (1981), pp. 22–30.

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 $\nu_2(\varphi(n)) \geq a - 1 + k$ and $\nu_2(2p) = 1$. 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, $1 = \nu_2(2p) = \nu_2(\varphi(n)) \geq k$, 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 5.12.8. *The number of odd elements in $\varphi^{-1}(2^k)$ is 0 or 1.*

Theorem 5.12.9. *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. 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. 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 $\pmod{20}$.

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

$$a + 1 \mid b^2 + 1$$
$$b + 1 \mid a^2 + 1$$

Prove that a and b are odd numbers.

Problem 5.13.25. Find all positive integers a and b such that

$$\frac{a^2 + b^2 + a + b + 1}{ab} \in \mathbb{N}$$

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

$$n \mid 1^n + 2^n + 3^n + \cdots + k^n$$

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

$$p^k \mid (p-2)^{2(p-1)} - (p-4)^{p-1}$$

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

$$(z+1)^x - z^y = -1$$

Part II

Problem Column

§§6 Solving Challenge Problems

> There will be plenty of time to rest in the grave.
>
> *Paul Erdős*

Problem 6.1. Prove divisibility criteria for $2, 3, 4, 5, 7, 9, 11, 13, 17, 19$, as stated in section (1.1.1).

Solution. Let n be a positive integer and it has base 10 representation $a_k \cdots a_1 a_0$. Here we show the proof for $2, 3, 4$ and then you should try the rest yourself in a similar fashion.

2: n is divisible by 2 if and only if the last digit is even. First we will prove that if n is divisible by 2, then the last digit must be even.

$$2 \mid n = 10^k a_k + \cdots + 10a_1 + a_0$$

Now, $2 \mid 10$ so $2 \mid 10^k, \cdots, 10$. In turn,

$$\begin{aligned} &2 \mid 10^k a_k + \cdots + 10a_1 \\ &2 \mid 10^k a_k + \cdots + 10a_1 + a_0 - (10^k a_k + \cdots + 10a_1) = a_0 \end{aligned}$$

This implies that 2 must divide a_0. Since a_0 is a digit, $a_0 \in \{0, 2, 4, 6, 8\}$.

Now, assume that, a_0 is even so $a_0 = 2b_0$. Then we have

$$\begin{aligned} n &= 10^k a_k + \cdots + 10a_1 + a_0 \\ &= 2(2^{k-1}5^k a_k + \cdots + 5a_1 + b_0) \end{aligned}$$

which is obviously divisible by 2.

An alternative approach would be using congruence.

$$\begin{aligned} n &\equiv 10^k a_k + \cdots + 10a_1 + a_0 \pmod 2 \\ &\equiv a_0 \pmod 2 \end{aligned}$$

since $10 \equiv 0 \pmod 2$.

3: n is divisible by 3 if and only if the sum of digits is divisible by 3.

$$\begin{aligned} n &= 10^k a_k + \cdots + 10a_1 + a_0 \\ &= (\underbrace{9\cdots 9}_{k\ 9\text{'s}} + 1)a_k + \cdots + (9+1)a_1 + a_0 \\ &= (3 \cdot \underbrace{3\cdots 9}_{k\ 3\text{'s}} + 1)a_k + \cdots + (3\cdot 3 + 1)a_1 + a_0 \\ &= 3 \cdot \left(\underbrace{3\cdots 9}_{k\ 3\text{'s}} a_k + \cdots + 3a_1 \right) + a_k + \cdots + a_1 + a_0 \end{aligned}$$

Notice that, when we divide n by 3, the term with 3 vanishes since it is divisible by 3. This is now straightforward that 3 will divide n if and only if $a_k + \cdots + a_0$ is divisible by 3. Since $a_k, \cdots, a_0$ are digits of n in base 10, the claim is proven.

4: n is divisible by 4 if and only if the number formed by the last two digits of n is divisible by 4.

$$\begin{aligned} n &= 10^k a_k + \cdots + 10a_1 + a_0 \\ &= 10^k a_k + \cdots + 100a_2 + 4l \\ &= 4\left(25 \cdot 10^{k-2} a_k + \cdots + l\right) \end{aligned}$$

This is definitely divisible by 4. The only if part is straightforward from this.

5: n is divisible by 5 if and only if the last digit of n is divisible by 5 i.e. 0 or 5. This is again straightforward since 10 is divisible by 5.

Problem 6.2. Let n be a positive integer. Show that the product of n consecutive integers is divisible by $n!$.

Before we solve this problem, let me tell you about my story when I first encountered this problem.[1] Since $n! = 1 \cdot 2 \cdots n$, the first thing that I thought was: since there are n consecutive integers, one must leave the remainder 0 modulo n. And this has to be true for all $m \leq n$. But then I immediately realized that even if we proved that the product of these n integers is divisible by all $m \leq n$ individually, we can not guarantee that their $1 \cdot 2 \cdots n$ will divide their product too! It would be a common mistake to think so. Beginners tend to make assumptions that are wrong. For example, a and b both divide c, then ab divides c too. We will see some common mistakes as we solve the problems. Be aware of them whenever you are thinking about a problem. So, to be on the safe side, if you assume something, don't think it's true until you can prove it. Appearances can be deceiving! Now, let's see a correct solution.

Solution. Let the n consecutive integers be $a, a-1, \cdots, a-n+1$ (verify that if you take n consecutive integers decreasing from a, the last integer will be $a-n+1$). See that,

$$\begin{aligned} S = a(a-1)\cdots(a-n+1) &= \frac{a(a-1)\cdots(a-n+1)\cdot(a-n)\cdots 1}{(a-n)\cdots 1} \\ &= \frac{a!}{(a-n)!} \end{aligned}$$

[1] I was a total beginner then

If we can prove that this product $\frac{S}{n!}$ is an integer, we are done.

$$\begin{aligned}\frac{S}{n!} &= \frac{a!}{(a-n)!n!} \\ &= \binom{a}{n}\end{aligned}$$

which is clearly an integer.[2]

Problem 6.3. Prove that, p^2 divides $\binom{2p}{p} - 2$.

Solution. This problem can be dealt with very easily if you know Wolstenholme's theorem which says for $p > 3$,

$$\begin{aligned}\binom{2p}{p} &\equiv \binom{2}{1} \pmod{p^3} \\ &\equiv 2 \pmod{p^3} \\ p^3 &\mid \binom{2p}{p} - 2\end{aligned}$$

For $p \leq 3$, we can check manually.

Remark. Another way to do it, if you don't know or can not remember the theorem. Use the identity:

$$\begin{aligned}\sum_{i=0}^{n} \binom{n}{i}^2 &= \binom{2n}{n} \\ \sum_{i=0}^{p} \binom{p}{i}^2 &= \binom{2p}{p}\end{aligned}$$

We already know that for $0 < i < p$, p divides $\binom{p}{i}$. So p^2 divides $\binom{p}{i}^2$ for such i and we have,

$$\begin{aligned}\sum_{i=0}^{p} \binom{p}{i}^2 &\equiv \binom{p}{0}^2 + \binom{p}{p}^2 \pmod{p^2} \\ \binom{2p}{p} &\equiv 2 \pmod{p^2} \\ p^2 &\mid \binom{2p}{p} - 2\end{aligned}$$

Problem 6.4 (Masum Billal). Find all functions $f : \mathbb{N} \to \mathbb{N}$ such that

$$(f(n+1), f(n)) = [f(n), f(n-1)]$$

holds for all $n > 1$.

[2] If $k < n$, then $\binom{n}{k} = 0$.

Solution. Let $g_n = (f(n+1), f(n))$ and $l_n = [f(n+1), f(n)]$. We have $g_{n+1} = l_n$. But note that $f(n) \mid l_n$ and $l_n = g_n \mid f(n+1)$. This gives $f(n) \mid f(n+1)$.

$$\begin{aligned} g_n &= (f(n+1), f(n)) \\ &= f(n) \\ l_n &= [f(n), f(n+1)] \\ &= f(n+1) \end{aligned}$$

This holds because if $a \mid b$, then $(a,b) = a$ and $[a,b] = b$. Since $f(n) \mid f(n+1)$, we can define a sequence $(b_i)_{i\geq 1}$ with $b_n = \dfrac{f(n+1)}{f(n)}$ and $b_1 = f(1)$, which is obviously an integer sequence.

$$\begin{aligned} f(n+1) &= b_n f(n) \\ &= b_n b_{n-1} f(n-1) \\ &= b_n b_{n-1} b_{n-2} f(n-2) \\ &\vdots \\ &= b_n b_{n-1} \cdots b_1 \\ &= \prod_{i=1}^{n} b_i \end{aligned}$$

Any positive integer sequence $(b_i)_{i\geq 1}$ works.

Sometimes we may find expression that's symmetric with respect to some variables[3] (say a, b). When you find an expression that's symmetric on a and b, you can assume $a \geq b$. That's a great advantage in many problems.

Problem 6.5 (Russia, 2000). If a and b are positive integers such that $a+b = (a,b)+[a,b]$ then one of a, b divides the other.

This is a problem that has many solutions, being a relatively easier problem. We will show two solutions here. Let $g = (a,b)$ and $l = [a,b]$ for brevity. Then the equation becomes $a + b = g + l$. Without loss of generality, we can assume $a \leq b$.

Solution (First). We know $ab = gl$ or $l = \dfrac{ab}{g}$. Substituting this into the equation:

$$\begin{aligned} a + b &= g + \frac{ab}{g} \\ g^2 + ab &= g(a+b) \\ (g-a)(g-b) &= 0 \end{aligned}$$

Since $a \leq b$, $g - a = 0$, then $(a,b) = a$ implies $a \mid b$.

[3]To see if an expression is symmetric on a, b switch places of a and b. If the expression remains the same it is symmetric, otherwise it is not. In short, we must have $f(a,b) = f(b,a)$

Solution (Second). Assume $a = gx, b = gy$ with $x \perp y$, then $l = gxy$.

$$\begin{aligned} g(x+y) &= g + gxy \\ xy + 1 &= x + y \\ (x-1)(y-1) &= 0 \end{aligned}$$

Again, since $a \leq b, x \leq y$ so $x - 1 = 0$ or $x = 1$, we have $a = g$. Same conclusion.

Problem 6.6 (Slovenia 2010). Find all primes p, q, r with $15p + 7pq + qr = pqr$.

Solution. We can write it as $p(15 + 7q) + qr = pqr$ or

$$p(qr - 15 - 7q) = qr$$

Therefore, $p \mid qr$ and since p, q, r are primes $p \mid q$ or $p \mid r$. If $p = q$, then

$$\begin{aligned} pr - 15 - 7p &= r \\ r(p-1) &= 7p + 15 \\ p - 1 \mid 7p + 15 & \end{aligned}$$

Since $p - 1 \mid 7p - 7, p - 1 \mid (7p + 15) - (7p - 7) = 22$. So $p - 1 \in \{1, 2, 11, 22\}$ which gives $p \in \{2, 3, 23\}$. But we also need $r = \dfrac{7p + 15}{p - 1}$, a prime. We get that r is a prime when $p = 2$ only when $r = 29$. The other case is $p = r$, so

$$\begin{aligned} pq - 15 - 7q &= q \\ (p-8)q &= 15 \end{aligned}$$

We have $q \in \{3, 5\}$. If $q = 3$, then $p = 13$ which is valid. If $q = 5, p = 11$ and this is a valid solution too.

Problem 6.7 (Serbia 2014). A *special* number is a positive integer n for which there exist positive integers a, b, c and d with

$$n = \frac{a^3 + 2b^3}{c^3 + 2d^3}$$

Prove that,

a. There are infinitely many special numbers.

b. 2014 is not a special number.

Solution. Proving (a) is easy since we just have to show an infinite such n. So we can choose a, b, c, d however we want, as long as they serve our purpose. Let's go with $a = ck, b = dk$, then

$$\begin{aligned} \frac{a^3 + 2b^3}{c^3 + 2d^3} &= \frac{c^3k^3 + 2d^3k^3}{c^3 + 2d^3} \\ &= k^3 \end{aligned}$$

Since we are free to choose k here, we have infinitely many n.

For part (b), let's assume

$$\begin{aligned} a^3 + 2b^3 &= 2014(c^3 + 2d^3) \\ &= 2 \cdot 19 \cdot 53(c^3 + 2d^3) \end{aligned}$$

We can consider modulo 19 in this equation. We just have to check cubes modulo 19 and the reader can verify that if $a^3 \equiv -2b^3 \pmod{19}$, then we must have $19 \mid a, b$ since $x^3 \equiv 0, \pm 1, \pm 7, \pm 8 \pmod{19}$. Say, $a = 19x, b = 19y$.

$$\begin{gathered} 19^3(x^3 + 2y^3) = 2 \cdot 19 \cdot 53(c^3 + 2d^3) \\ 19 \mid c^3 + 2d^3 \end{gathered}$$

This also shows that $19 \mid c, d$ so let $c = 19z, d = 19w$. but then

$$x^3 + 2y^3 = 2014(z^3 + w^3)$$

we get a smaller solution (x, y, z, w) which is actually infinite descent.

Problem 6.8 (Croatia 2015). Let $n > 1$ be a positive integer so that $2n - 1$ and $3n - 2$ are perfect squares. Prove that $10n - 7$ is composite.

Solution. Take $2n - 1 = x^2$ and $3n - 2 = y^2$. We need to reach $10n$ somehow here, and incidentally $10 = 12 - 2 = 3 \cdot 4 - 2 \cdot 1$. So, we do this:

$$\begin{aligned} 4(y^2) - 1(x^2) &= 4(3n - 2) - (2n - 1) \\ (2y + x)(2y - x) &= 10n - 7 \end{aligned}$$

Since $n > 1, y > 1$ so $2y - 1 > 1$. Thus $10n - 7$ is not a prime.

Problem 6.9. Find all non-negative integers m, n such that $3^m - 5^n$ is a perfect square.

Solution. Let $3^m - 5^n = a^2$. Since there are squares, we should consider modulo 4, the numbers 3, 5 also suggest us to take modulo 4. That way, we get to know about m and n. Since both sides must leave the same remainder upon division by 4,

$$(-1)^m - 1^n \equiv a^2 \equiv 0, 1 \pmod{4}$$

If m is odd then $a^2 \equiv -1 - 1 \equiv 2 \pmod{4}$, which is not possible. So m is even. If $m = 2l$, can write the equation as

$$\begin{aligned} \left(3^l\right)^2 - a^2 &= 5^n \\ (3^l + a)(3^l - a) &= 5^n \end{aligned}$$

In the right side there is nothing but 5, so we must have $3^l + a = 5^x, 3^l - a = 5^y$ for some non-negative integer x, y. If we add them

$$2 \cdot 3^l = 5^x + 5^y$$

If y is 0, then

$$2 \cdot 3^l = 5^x + 1$$

$5 + 1$ is divisible by 2 and 3, but according to Zsigmondy's theorem $5^x + 1$ will have a prime factor that is neither 2 nor 3 if $x > 1$. Clearly $x > y$ so if $y \neq 0$, then 5 divides $2 \cdot 3^l$, contradiction. So there is no such integers m, n except the trivial solutions when $x = 0$ or $x = 1$.

Problem 6.10 (Croatia 2015). Prove that there does not exist a positive integer n for which $7^n - 1$ is divisible by $6^n - 1$.

Solution. Assume to the contrary that, $6^n - 1 \mid 7^n - 1$. Due to $6^n - 1 \mid 6^n - 1$, subtraction gives

$$\begin{aligned} 6^n - 1 \mid 7^n - 1 - (6^n - 1) \\ = 7^n - 6^n \end{aligned}$$

See that left side is divisible by $6 - 1 = 5$, so right side is divisible by 5 too.

$$7^n - 6^n \equiv 2^n - 1 \pmod 5$$

The smallest positive integer for which $2^n - 1$ is divisible by 5 is $n = 4$. So, n must be divisible by 4. But then $6^4 - 1 = 37 \cdot 5 \cdot 7$ divides $6^n - 1$. So 7 divides $7^n - 6^n$, a contradiction.

Problem 6.11. Find all positive integers n such that $n^2 - 1 \mid 2^n + 1$.

Solution. Clearly $2^n + 1$ is odd, so $n^2 - 1$ must be odd as well. This means that n is even. Let $n = 2k$ for some positive integer k. Then

$$n^2 - 1 \equiv 4k^2 - 1 \equiv 3 \pmod 4.$$

By Theorem 1.5.14, every number of the form $4k + 3$ has a prime divisor of that form. Therefore, there is a prime p such that $p \mid n^2 - 1$ and $p \equiv 3 \pmod 4$. Now, according to Theorem 2.8.9, every prime divisor of $2^n + 1 = \left(2^k\right)^2 + 1$ is of the form $4k + 1$. This is a contradiction because $p \mid n^2 - 1 \mid 2^n + 1$. Thus no such n exists.

Note. Although some problems seem difficult at first sight, they are pretty easy if you think in a proper way.

Problem 6.12. Find all $m, n \in \mathbb{N}$ such that $2^n - 1 \mid m^2 + 9$.

Solution. $n = 1$ is obviously a solution (which works for any m), so let's look at $n > 1$ only. Note that $m^2 + 9 = m^2 + 3^2$, if $m \perp 3$, then $m^2 + 3^2$ is a bisquare. Therefore, if $n > 1$ then $2^n - 1 \equiv -1 \pmod 4$, so $m^2 + 9$ will have a prime divisor of the form $4k + 3$. But we know that, no bisquare has a prime divisor of this form. Therefore, m must be divisible by 3. If $m = 3k$,

$$2^n - 1 \mid 9(k^2 + 1)$$

Now, no matter what k is, $k^2 + 1$ is always a bisquare. Therefore, it can not have any divisors of the form $4k + 3$. So, $2^n - 1 \mid 9$, checking with $2^n - 1 = 1, 3, 9$, we get that $n = 1, 2$ are the solutions.

You never know what's coming next until you think clearly!

Problem 6.13. If $n > 1$, prove that $n^2 - 1$ divides $2^{n!} - 1$ for even n.

Solution. If we set $m = n + 1$, then we need to prove $m(m-2)$ divides $2^{(m-1)!} - 1$. Since n is even, m is odd so m is co-prime to 2.

$$\begin{aligned} 2^{\varphi(m)} &\equiv 1 \pmod{m} \\ 2^{\varphi(m-2)} &\equiv 1 \pmod{m-2} \end{aligned}$$

Since $\varphi(m) < m$ and $\varphi(m-2) \leq m-2$, $\varphi(m)$ and $\varphi(m-2)$ divides $(m-1)!$. Therefore,

$$\begin{aligned} 2^{(m-1)!} &\equiv 1 \pmod{m} \\ 2^{(m-1)!} &\equiv 1 \pmod{m-2} \end{aligned}$$

This implies $m \mid 2^{(m-1)!} - 1$ and $m - 2 \mid 2^{(m-1)!} - 1$. Since $m \perp m - 2$ for odd m, we have $m(m-2) \mid 2^{(m-1)!} - 1$.

Problem 6.14. Prove that n divides $2^n + 1$ for infinitely many $n \in \mathbb{N}$.

Solution. One can easily observe that $n = 3$ works since n is odd, so we could take $n = 3k$. Then we see that $2^{3k} + 1 = 8^k + 1$ is divisible by 9 since k is odd. This suggests us to take $n = 3^k$. Indeed, it works because due to LTE, $3^{k+1} \| 2^{3^k} + 1$, so $n = 3^k$ gives us infinitely such n.

Problem 6.15 (Croatia 2015). Determine all positive integers n for which there exists a divisor d of n such that $dn + 1 \mid d^2 + n^2$.

Solution. Let $n = dk$ where $k \in \mathbb{N}$. The equation becomes

$$\begin{aligned} d^2k + 1 &\mid d^2 + d^2k^2 \\ d^2k + 1 &\mid d^2k^2 + k \\ d^2k + 1 &\mid d^2k^2 + d^2 - (d^2k^2 + k) \\ &= d^2 - k \end{aligned}$$

If $d^2 > k$ then $d^2k + 1 \mid d^2 - k$ but clearly $d^2 - k < d^2 < d^2k + 1$, contradiction. If $k > d^2$, then $k - d^2 < k < kd^2 + 1$. Thus, $d^2 - k = 0$ or $k = d^2$. We get $n = dk = d^3$.

Problem 6.16 (IMO Shortlist 2013, N1, Proposed by Malaysia). Find all functions $f : \mathbb{N} \to \mathbb{N}$ such that

$$m^2 + f(n) \mid mf(m) + n$$

Arithmetic functional equations or divisibility problems are really popular for IMO or Shortlist. Anyway, let's see how we can solve this one. We say it beforehand that, it can be solved in many ways, being an easy problem. So if you try yourself you should be able to do it.

Solution (First). There are two variables in this divisibility. Sometimes reducing to one variable and then working on it alone suffices for some problems. By the way, you have probably guessed already, $f(n) = n$ is the solution.

First let's play with some values of m and n. To remove two variables, set $m = n$.

$$\begin{aligned} n^2 + f(n) \mid nf(n) + n \\ nf(n) + n \geq n^2 + f(n) \\ (n-1)(f(n) - n) \geq 0 \end{aligned}$$

Since $n \geq 1$, we have $f(n) - n \geq 0$ so $f(n) \geq n$. If we can prove now that $f(n) \leq n$, we will have $f(n) = n$. Set $n = 2$ in the divisibility.

$$\begin{aligned} 4 + f(2) \mid 2f(2) + 2 \\ 4 + f(2) \mid 8 + 2f(2) \\ 4 + f(2) \mid 8 + 2f(2) - (2f(2) + 2) \\ 4 + f(2) \mid 6 \end{aligned}$$

Since $4 + f(2) \geq 5$, we must have $4 + f(2) = 6$ or $f(2) = 2$. Now, using $n = 2$ in the original divisibility,

$$\begin{aligned} m^2 + f(2) \mid mf(m) + 2 \\ m^2 + 2 \mid mf(m) + 2 \\ m^2 + 2 \leq mf(m) + 2 \\ m^2 \leq mf(m) \\ m \leq f(m) \end{aligned}$$

And we are done!

Solution (Second). This one uses another great idea. This kind of technique is useful in many cases. Another example of choosing a special prime.

Set $m = f(n)$ in the divisibility, and it gives us

$$\begin{aligned} f(n)^2 + f(n) \mid f(n)f(f(n)) + n \\ f(n)(f(n) + 1) \mid f(n)f(f(n)) + n \end{aligned}$$

Thus, $f(n) \mid f(n)f(f(n)) + n$ or $f(n) \mid n$, so $f(n) \leq n$. Now, we will explain our main idea. We will make the right side a prime (think what the benefit of doing so). But we need to understand if that's achievable. It is, since we can take n as we please, and there is a free n on the right side. Let $p = mf(m) + n$ for a prime $p > mf(m)$. In fact, we take a prime $p > m^2$, that way we also ensure $p > mf(m)$ since $f(m) \leq n$. So, for that m,

$$m^2 + f(n) \mid mf(m) + n = p$$

This forces us to $m^2 + f(n) = p$ since $m^2 + f(n) \geq 2$.

$$\begin{aligned} p - m^2 = f(n) &\leq n \\ &= p - mf(m) \end{aligned}$$

which gives $m \leq f(m)$. So $f(n) = n$.

Problem 6.17 (IMO 1990, Problem 3). Find all $n \in \mathbb{N}$ for which $n^2 \mid 2^n + 1$.

Solution. Let's see if we can determine the smallest prime factor again. If p is the smallest prime divisor of n,

$$\begin{aligned} 2^n &\equiv -1 \pmod{p} \\ 2^{2n} &\equiv 1 \pmod{p} \end{aligned}$$

And from Fermat's little theorem, $2^p \equiv 1 \pmod{p}$. So we get

$$2^{(2n,p-1)} \equiv 1 \pmod{p}$$

Using the same argument as before, $n \perp p-1$, so $(2n, p-1) = (2, p-1) = 2$ because p is odd. This gives us $2^2 \equiv 1 \pmod{p}$ or $p = 3$. What do we do now? We only have the smallest prime. So, we can assume $n = 3^\alpha k$ where k is not divisible by 3. Think yourself about the reason to do this. It would be certainly fruitful to find out what values α can assume. This is where Lifting the Exponent lemma comes to the rescue! But first we need to make sure we can actually apply LTE. In this case, we can because $2 + 1 = 3$, divisible by 3 and $2 \perp 1$. We have

$$\begin{aligned} \nu_3(n^2) &= \nu_3(3^{2\alpha}k^2) \\ &= \nu_3(3^{2\alpha}) + \nu_3(k^2) \\ &= 2\alpha \end{aligned}$$

On the other hand, from LTE,

$$\begin{aligned} \nu_3(2^{3^\alpha} + 1) &= \nu_3(2+1) + \nu_3(3^\alpha) \\ &= 1 + \alpha \end{aligned}$$

$n^2 \mid 2^n + 1$ implies that

$$\begin{aligned} \nu_3(2^n + 1) &\geq \nu_3(n^2) \\ 1 + \alpha &\geq 2\alpha \\ 1 &\geq \alpha \end{aligned}$$

Since α is a positive integer, we have $\alpha = 1$. So $n = 3k$ with $3 \nmid k$. The problem is now finding k with

$$k^2 \mid 8^k + 1$$

Here, we again try to determine the smallest prime divisor of k, we call it q. Then $8^k \equiv -1 \pmod{q}$.

$$\begin{aligned} 8^{2k} &\equiv 1 \pmod{q} \\ 8^{q-1} &\equiv 1 \pmod{q} \\ 8^{(2k,q-1)} &\equiv 1 \pmod{q} \\ 8^2 &\equiv 1 \pmod{q} \end{aligned}$$

We hope the lines above don't need a second explanation. This way, $q \mid 63 = 3^2 \cdot 7$. Since $3 \perp q$, we can only have $q = 7$. But,

$$8^k + 1 \equiv 1^k + 1 \equiv 2 \pmod 7$$

This is impossible, which means k doesn't have any prime divisor i.e. $k = 1$. The only solution we have is $n = 1, 3$.

Note. This is a fantastic problem which uses couple of techniques at the same time. Worthy of being a problem 3 at the IMO!

Problem 6.18 (All Russian Olympiad 2014, Day 2). Define $m(n)$ to be the greatest proper natural divisor of $n \in\in N$. Find all n such that $n + m(n)$ is a power of 10.

Solution. Let $n + m(n) = 10^a$. If n is a prime then $m(n)$ is clearly 1. In that case,

$$\begin{aligned} p + 1 &= 10^a \\ p &= 10^a - 1 \end{aligned}$$

Right side is divisible by $10 - 1 = 9$, so p can not be prime. Now, if $n > 1$ and not a prime, then n has a smallest prime divisor. Then the greatest proper divisor of n will be $\frac{n}{p}$, let's say $n = pk$. Be careful here, p is the smallest prime does not mean that k is not divisible by p. For example, $12 = 2^2 \cdot 3$ so $k = 6$. Take $k = p^r l$ where all prime factors of l must be greater than p and $r \geq 0$.

$$\begin{aligned} n + m(n) &= 10^a \\ pk + k &= 10^a \\ p^r l(p + 1) &= 10^a \end{aligned}$$

If $r \geq 1$ then p divides 10. So $p = 2$ or $p = 5$. If $p = 2$, then $p + 1 = 3$ divides 10^a, contradiction. If $p = 5$, $p + 1 = 6$ divides 10^a, again contradiction. So $r = 0$ and $l(p + 1) = 10^a$. It is clear that l is odd, otherwise $2 \mid l$ and hence $p < 2$ since all prime factors of l are greater than p. This also provides with $p + 1 \leq l$. Since l is odd, $l = 5^x$ for some $1 \leq x \leq a$. Since p is less than all prime factors of l, we must have $p = 3$.

$$5^x \cdot 4 = 2^a 5^a$$

which immediately gives $a = 2$, so $x = a = 2$. Thus, $n = pk = 3 \cdot 5^2 = 75$.

Problem 6.19 (Czech Slovakia 1996). Find all positive integers x, y such that $p^x - y^p = 1$ where p is a prime.

Solution. If $p = 2$, then $2^x = y^2 + 1$. If $x \geq 2$, then $x^2 \equiv -1 \pmod 4$, which is impossible. So $x = 1$ and now p is odd. Then $p^x = y^p + 1 = (y + 1)S$ for some integer S. Obviously $y + 1$ is divisible by p but $y^p + 1$ has a primitive divisor unless $y = 2, p = 1$.

Problem 6.20 (China 2001, Problem 4). We are given three integers a, b, c such that $a, b, c, a + b - c, a + c - b, b + c - a$, and $a + b + c$ are seven distinct primes. Let d be the difference between the largest and smallest of these seven primes. Suppose that $800 \in \{a + b, b + c, c + a\}$. Determine the maximum possible value of d.

Solution. Observation: all of a, b, c are odd prime. In cases like this, show a contradiction that the other case can not happen. So let's assume that $a = 2$ and b, c are odd. Then $a+b-c$ is even since $b-c$ is even, so not a prime unless $a+b-c = 2$ but then $b = c$ which contradicts that b, c are distinct primes. We leave the other cases for the reader.

From what we just proved, the smallest prime of a, b, c (namely $c \geq 3$) must be at least 3. What other information is there for us to use? $800 \in \{a+b, b+c, c+a\}$, but we don't need to analyze every case since they are symmetric over a, b, c. Without loss of generality, take $a + b = 800$. $a + b - c > 0$ is a prime too, so $c < a + b = 800$ or $c \leq 799$, a prime. We can check that 17 divides 799, so $c \leq 797$, inferring $a + b + c \leq 800 + 797 = 1597$. And by luck, 1597 is a prime (well, that's how the problem creator created the problem). So if we can find a, b so that all are primes, we are done and in that case, $d = a + b + c - 3 = 1594$ since $a + b + c$ is the largest prime and 3 is the smallest prime. a must be greater than or equal to 5, but since $a + b = 800$, a can not be 5. Let's check starting from $a = 7, b = 793$. With some tedious calculations, we can find that $a = 13, b = 787$ satisfies all the conditions. Other primes would be $23, 1571$.

Problem 6.21. Find the number of positive integers d so that for a given positive integer n, d divides $a^n - a$ for all integer a.

Solution. Let's focus only on $n > 1$. How do we understand the nature of d? Surely we should take a prime divisor of d, say p. If we can find the values of p and the exponent of p in d, we can find d. So we get $p \mid a^n - a$ for all $p \mid d$. What should we use to get a clue on the exponents? We can set different values of a. And it seems wise to use $a = p$. This shows that $p \mid p^n - p$. Now, if $p^2 \mid d$ then we would have $p^2 \mid p^n - p$ which would breed a contradiction $p^2 \mid p$ because $p^2 \mid p^n$ for $n > 1$. Therefore, for any prime $p \mid d$, p^2 can't divide d and so d is square-free.

Now, we only need to find the valid values of p. This is where it gets tricky. For any integer a, either $p \mid a$ or $a \perp p$. It's safe to work only for $a \perp p$ since the problem asks for all values of a. In that case, from Fermat's little theorem, $a^{p-1} \equiv 1 \pmod{p}$. And from the problem statement, we have $a(a^{n-1} - 1)$ is divisible by p. Since $a \perp p$, we get $a^{n-1} - 1$ is divisible by p, or $a^{n-1} \equiv 1 \pmod{p}$. This almost tells us to infer that we must have $p - 1 \mid n - 1$. That is the case indeed, however, we have to prove that $p - 1$ must be the order of a for some integer a. You should think on this more and get to the point where you understand: we should set $a = g$ where g is a primitive root of p. So that, we can tell $g^{p-1} \equiv 1 \pmod{p}$ and $\mathrm{ord}_p(g) = p - 1$. Therefore, from $g^{n-1} \equiv 1 \pmod{p}$, we get $p - 1 \mid n - 1$.

Notice that, if $D = \prod_{p-1 \mid n-1} p$, then any $d \mid D$ satisfies the condition of the problem. Therefore the number of such positive integer d is $\tau(D)$. If the number of primes $p \mid n$ for which $p - 1 \mid n - 1$ is $t(n)$ i.e.

$$t(n) = \sum_{\substack{p \mid n \\ p-1 \mid n-1}} 1$$

then $\tau(D) = 2^{t(n)}$.

Note. The following approach works too. Consider $a \perp d$ so we have $d \mid a^{n-1} - 1$. Using Theorem 2.13.3, we get $\lambda(n) \mid n - 1$.

Problem 6.22. For rational a, b and all prime p, $a^p - b^p$ is an integer. Prove that, a and b must be integer.

Solution. Since a, b are rational, we can assume that $a = \frac{m}{d}, b = \frac{n}{d}$ with $m \perp d, n \perp d$. Otherwise, if $\gcd(m, d) > 1$ we can divide by the common factor. Moreover, we can assume $m \perp n$. Indeed, if not, say r is a prime factor of d. Then we must have $r \nmid \gcd(m, n)$. Otherwise the condition $m \perp d$ would be broken. Therefore, without loss of generality, $m \perp n$. Let q be a prime factor of d. Thus,

$$q^p \mid m^p - n^p$$

for all p, and e be the smallest positive integer such that

$$m^e \equiv n^e \pmod{q}$$

We can say that $e \mid p$ for all prime p. But this impossible except for $e = 1$. Hence, $q \mid m - n$. Now, take a prime $p \neq q$, and from Exponent GCD lemma we have

$$\begin{aligned} \gcd\left(m - n, f(m, n, p)\right) &\mid p \\ q &\nmid f(m, n, p) \end{aligned}$$

This gives us, $q^p \mid m - n$ for all prime $p \neq q$ which leaves a contradiction inferring that d can't have a prime factor i.e. d must be 1. And then, a and b both are integers.

Problem 6.23. Prove that, $\sigma(n) = n + k$ has a finite number of solutions for a fixed positive integer k.

Solution. We can easily show that $\sigma(n) > n + \sqrt{n}$ which says $k > \sqrt{n}$. In other words, n is bounded above so it can not have arbitrary number of solutions.

Note. We can use some sharper inequalities to get a upper bound of k. Try to sharpen the inequality as much as you can.

Problem 6.24. Prove that, for a positive integer n,

$$\binom{2n}{n} \mid [1, 2, \cdots, 2n]$$

Solution. When proving divisibility like this, you should consider Theorem 1.4.13. The idea is that if we can show the exponent in the left side of the divisibility is less than or equal to the exponent in the right side for a prime p, we are done. It is clear that no side of divisibility will have a prime $p > 2n$. So we should consider only primes $p < 2n$, since $2n$ is not a prime for $n > 1$. Using Theorem 1.5.12, if for a prime p, $\alpha = \log_p(2n)$,

$$\nu_p([1, 2, \cdots, 2n]) = \alpha$$

On the other hand, from Legendre's theorem, if $N = \binom{2n}{n}$,

$$\begin{aligned}
\nu_p(N) &= \sum_{i=1}^{\infty} \left\lfloor \frac{2n}{p^i} \right\rfloor - 2\left\lfloor \frac{n}{p^i} \right\rfloor \\
&= \sum_{i=1}^{\log_p(2n)} \left\lfloor \frac{2n}{p^i} \right\rfloor - 2\left\lfloor \frac{n}{p^i} \right\rfloor \\
&\leq \sum_{i=1}^{a} 1 \text{ since } \lfloor 2x \rfloor - 2\lfloor x \rfloor \in \{0, 1\} \\
&= \alpha \\
\nu_p(N) &\leq \nu_p([1, 2, \cdots, 2n])
\end{aligned}$$

This is exactly what we needed to prove.

Problem 6.25 (Italy TST 2003). Find all triples of positive integers (a, b, p) such that $2^a + p^b = 19^a$.

Solution. Rewrite the equation as $p^b = 19^a - 2^a$. Right side is divisible by $19 - 2 = 17$ which is a prime. Therefore, $p = 17$, $17^b = 19^a - 2^a$. But if $a > 1$ then $19^a - 2^a$ has a prime factor other than 17, contradiction. Thus, the only solution is $(a, b) = (1, 1,)$.

Problem 6.26 (APMO 2012 - Problem 3). Find all pairs of (n, p) so that $\dfrac{n^p + 1}{p^n + 1}$ is a positive integer where n is a positive integer and p is a prime number.

Solution. We can re-state the relation as

$$p^n + 1 \mid n^p + 1$$

Firstly, we exclude the case $p = 2$. In this case,

$$2^n + 1 \mid n^2 + 1$$

Obviously, we need

$$n^2 + 1 \geq 2^n + 1 \Rightarrow n^2 \geq 2^n$$

But, using induction we can easily say that for $n > 4$, $2^n > n^2$ giving a contradiction. Checking $n = 1, 2, 3, 4$ we easily get the solutions:

$$(n, p) = (2, 2), (4, 2)$$

We are left with p odd. So, $p^n + 1$ is even, and hence $n^p + 1$ as well. This forces n to be odd. Say, q is an arbitrary prime factor of $p + 1$. If $q = 2$, then $q \mid n + 1$ and since

$$n^p + 1 = (n + 1)(n^{p-1} - .... + 1)$$

and p odd, there are p terms in the right factor, therefore odd. So, we infer that $2^k \mid n+1$ where k is the maximum power of 2 in $p + 1$.

We will use the following theorem from elementary calculus, which can also be proved elementarily.

Theorem 6.27.

$$\lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n = e$$

where e is the Euler constant.

Now, we prove the following lemmas.

Lemma 6.28. *If $p \geq 3$ is an odd number (not necessarily prime), then $p^n \leq n^p$ for $p \leq n$.*

Proof. We will proceed by induction. The result is true for $n = 1$. Suppose that $n > 1$ is an integer such that $p^n \leq n^p$ holds for all $3 \leq p \leq n$. We want to show that $p^{n+1} \leq (n+1)^p$ for all $3 \leq p \leq n+1$. If $p = n+1$, we have the equality case. So, suppose that $3 \leq p < n+1$. Then, since $p \leq n$, we have

$$(pn+p)^p \leq (pn+n)^p,$$

which gives (after dividing both sides by $(np)^p$)

$$\left(1+\frac{1}{n}\right)^p \leq \left(1+\frac{1}{p}\right)^p.$$

Therefore, since we assumed $n^p \leq p^n$,

$$\begin{aligned}(n+1)^p &= n^p\left(1+\frac{1}{n}\right)^p \\ &\leq p^n\left(1+\frac{1}{p}\right)^p \\ &\leq p^n \cdot e \\ &< p^{n+1}\end{aligned}$$

since $e < 3$. □

Back to the problem. Assume that q is odd.

$$q \mid p^n + 1 \mid n^p + 1$$

Write them using congruence. And we have,

$$n^p \equiv -1 \pmod{q}$$

$$\Rightarrow n^{2p} \equiv 1 \pmod{q}$$

Suppose, $e = \mathrm{ord}_q(n)$ i.e. e is the smallest positive integer such that

$$n^e \equiv 1 \pmod{q}$$

Then, $e \mid 2p$ and $e \mid q-1$ from Theorem 2.12.1.

Also, from Fermat's theorem,

$$n^{q-1} \equiv 1 \pmod{q}$$

Therefore,

$$n^{(2p,q-1)} \equiv 1 \pmod{q}$$

From p odd and $q \mid p+1, p > q$ and so p and $q-1$ are co-prime. Thus,

$$(2p, q-1) = (2, q-1) = 2$$

This gives us, $e \mid (2p, q-1)$ and so we must have $e = 2$. Again, since p odd, if $p = 2r+1$,

$$n^{2r+1} \equiv n \pmod{q}$$

Hence, $q \mid n+1$. If $q \mid \frac{n^p+1}{n+1}$, then by the Theorem 5.4.1 we get

$$q \mid \gcd\left(n+1, \frac{n^p+1}{n+1}\right) \mid p$$

which would imply $q = 1$ or p. Both of the cases are impossible. So, if s is the maximum power of q so that $q^s \mid p+1$, then we have $q^s \mid n+1$ too for every prime factor q of $p+1$. This leads us to the conclusion $p+1 \mid n+1$ or $p \leq n$ which gives $p^n \geq n^p$ by lemma 2.5. But from the given relation,

$$p^n + 1 \leq n^p + 1 \Rightarrow p^n \leq n^p$$

Combining these two, $p = n$ is the only possibility to happen. Thus, the solutions are $(n, p) = (4, 2), (p, p)$.

Problem 6.29. Prove that $a^{\varphi(n)}(a^{\varphi(n)} - 1)$ is always divisible by n for all positive integers a and n.

Solution. Let p be any prime divisor of n. Suppose that that $p^k \mid n$ but $p^{k+1} \nmid n$, where $k \geq 1$ is an integer. Consider two possible cases:

1. $p \nmid a$. Note that by Corollary (3.2.12), since $p^k \mid n$, we have $\varphi(p^k) \mid \varphi(n)$. Then by Euler's theorem and Theorem 1.5.21,

$$\begin{aligned} p^k &\mid a^{\varphi(p^k)} - 1 \\ a^{\varphi(p^k)} - 1 &\mid a^{\varphi(n)} - 1 \end{aligned}$$

2. $p \mid a$. We know that $\varphi(p^k) = p^{k-1}(p-1)$, which is clearly bigger than k. Thus

$$\begin{aligned} p^k &\mid a^k \\ a^k &\mid a^{\varphi(p^k)} \\ a^{\varphi(p^k)} &\mid a^{\varphi(a^n)} \end{aligned}$$

Therefore in both cases we have $p^k \mid a^{\varphi(n)}(a^{\varphi(n)} - 1)$ which results in $n \mid a^{\varphi(n)}(a^{\varphi(n)} - 1)$.

Problem 6.30 (Serbian Mathematical Olympiad 2014, Day 2). We call a natural number n nutty if there exist natural numbers $a > 1$ and $b > 1$ such that $n = a^b + b$. Do there exist 2014 consecutive natural numbers, exactly 2012 of which are nutty?

Solution. Let's say n is nutty for (a,b) if $n=a^b+b$ for $a,b>1$. We need 2014 consecutive natural numbers with $b>1$ among which 2012 will be nutty. Let say those numbers are $a^1+1, a^2+2, \cdots, a^{2014}+2014$. Crucial observation: If n is nutty for a,b then n is nutty for a^k,b where k is a positive integer. Since there are integers $1,2,3,\cdots,2014$ associated and we are free to choose a as long as $a>1$, it makes sense to take the exponent 2014!. But we can not change b, therefore, we must introduce this factorial within a. So, let's take a positive integer $x>1$ and look at the numbers

$$x^{2014!}+1, x^{2014!}+2, \cdots, x^{2014!}+2014$$
$$x^{2014!}+1, \left(x^{\frac{2014!}{2}}\right)^2+2, \cdots, \left(x^{\frac{2014!}{2014}}\right)^{2014}+2014$$

All of them are nutty except the first one (probably). But we need exactly two to be not nutty. A way to do that is to divide 2014! by a number and hope it doesn't remain nutty. Let's say this number is k, that is, we are looking at the numbers

$$x^{\frac{2014!}{k}}+1, \left(x^{\frac{2014!}{2k}}\right)^2+2, \cdots, \left(x^{\frac{2014!}{2014k}}\right)^{2014}+2014$$

We can see that there are only two numbers which can be candidates to be not nutty. $x^{\frac{2014!}{k}}+1$ and $\left(x^{\frac{2014!}{k^2}}\right)^k+k$. Essentially we don't want the case k^2 divides 2014!. This is a hint to using primes! If we take a prime $p>1007$, $p^2\nmid 2014!$. Now we that have 2012 numbers nutty for sure, we just need to find x,p so that those two numbers become not nutty.

$$x^{\frac{2014!}{p}}+1=a^b+b$$
$$x^{\frac{2014!}{p}}+p=a^b+b$$

Take $N=\frac{2014!}{p}$. If we find x,p so that the equations $x^N+1=a^b+b$ and $x^N+p=a^b+b$ don't have solutions, we are done. Let's try with $x=2$ since $a\geq 2$, we might be able to use inequalities. For $b\geq N$,

$$\begin{aligned}2^N+p&=a^b+b\\&\geq 2^b+b\\&\geq 2^N+N\\&>2^N+p\end{aligned}$$

So $b<N$. This also means we are in the right track to solve the problem. And $b>p$ too must hold. Otherwise,

$$\begin{aligned}p-b&=a^b-2^N\\&=a^b-\left(2^{\frac{N}{b}}\right)^b\\&=\left(a-2^{\frac{N}{b}}\right)\left(a^{b-1}+\cdots+2^{\frac{N(b-1)}{b}}\right)\\&>p\\0&>b\end{aligned}$$

contradiction. Now , if a is even, let $a = 2u$.

$$b - p = 2^N - 2^b u^b$$

Since $b < N$, $2^b \mid b - p$ but clearly $b - p < 2^b$. Thus, a is odd. If b is even with $b = 2v$,

$$\begin{aligned} b - p &= \left(2^{\frac{N}{2}}\right)^2 - (2^v)^2 \\ &= \left(2^{\frac{N}{2}} + 2^v\right)\left(2^{\frac{N}{2}} - 2^v\right) \\ &> b \end{aligned}$$

again contradiction. Try to do the same with $2^N + 1$.

Problem 6.31 (Columbia 2010). Find the smallest $n \in \mathbb{N}$ such that $n!$ is divisible by n^{10}.

Solution. Let p be a prime divisor of n and p-base representation of n is $n = a_k p^k + \cdots + a_1 p + a_0$. Then

$$\nu_p(n!) = \frac{n - (a_k + \cdots + a_0)}{p - 1}$$

If $\nu_p(n) = \alpha$ then the last α digits of n in base p is 0.

$$\begin{aligned} \nu_p(n!) &= \frac{n - (a_k + \cdots + a_\alpha)}{p - 1} \text{ and} \\ \nu_p(n^{10}) &= \nu_p(p^{10\alpha}) = 10\alpha \end{aligned}$$

We must have $\nu_p(n!) \geq \nu_p(n^{10}) = 10\alpha$.

$$\frac{n - (a_k + \cdots + a_\alpha)}{p - 1} \geq 10\alpha$$

where $\alpha \leq \log_p(n)$. Remember that, we are looking for the smallest n, not all n. Therefore, we should first consider the case $n = p^\alpha$ first. Then In base p,

$$n = (1\underbrace{0 \cdots 0}_{\alpha \text{ zeros}})_p$$

$\nu_p(n!) = \dfrac{p^\alpha - 1}{p - 1}$ and so,

$$\frac{p^\alpha - 1}{p - 1} \geq 10\alpha$$

We need to find such p, α such that p^α is minimum. Therefore, p must be 2. Now we need the smallest α for which $2^\alpha - 1 \geq 10\alpha$. See that $\alpha = 6$ works. But can we minimize n even further? Since $n!$ must be divisible by n^{10}, so we need to look at primes for which we get the exponent at least 10. If $p^2 \mid n$ for some prime p, we need $\nu_p(n!) \geq 20$ for some $n < 64$. The minimum n for which $n!$ is divisible by 3^{10} is 24. For $n < 64$,

$$\begin{aligned} \nu_3(n!) &\leq \frac{63}{3} + \frac{63}{9} + \left\lfloor \frac{63}{27} \right\rfloor \\ &= 21 + 7 + 2 = 30 \end{aligned}$$

And we see that $n = 63$ is in fact a solution because $\nu_7(63!) = \frac{63}{7} + \left\lfloor \frac{63}{49} \right\rfloor = 10$. The minimum n for which $\nu_5(n!) \geq 10$ is $n = 45$. Using the arguments we made already, show that we can not minimize n further.

Problem 6.32 (Greece National Mathematical Olympiad, 2015). Find all triplets (x, y, p) of positive integers such that p is a prime number and

$$\frac{xy^3}{x+y} = p$$

Solution. This equation does not suggest it, but we will take $(x, y) = g$ and $x = ga, y = gb$ where $a \perp b$. Because that way, we can reduce the equation or extract more information.

$$\begin{aligned} \frac{gag^3b^3}{g(a+b)} &= p \\ g^3ab^3 &= p(a+b) \end{aligned}$$

Now this equation talks more than the previous one. Since $a \perp b$, $a+b \perp a, a+b \perp b$ and $b^3 \perp a+b$. Therefore, $a \mid p(a+b)$ gives us $a \mid p$ and $b^3 \mid p(a+b)$ gives $b^3 \mid p$. From this, $b = 1$ since $b = p$ is not possible. If $a = p$, then

$$\begin{aligned} g^3b^3 &= b + p \\ p &= b(g^3b^2 - 1) \\ &= g^3 - 1 \end{aligned}$$

This equation gives p is divisible by $g - 1$, which is not possible unless $g = 2$. Then $a = p = 7$ and $x = ga = 14, y = gb = 2$. We are left with $a = 1$ which gives $g^3 = 2p$ but this is not possible since right side can not be a cube.

Problem 6.33 (Korea 2010). A prime p is called a *nice* prime if there exists a sequence of positive integers $(n_1, \cdots, n_k)$ satisfying following conditions for infinitely positive integers k, but not for $k = 1$.

- For $1 \leq i \leq k, n_i \geq \frac{p+1}{2}$.
- For $1 \leq i \leq k$, $p^{n_i} - 1$ is a multiple of n_{i+1} and $\frac{p^{n_i} - 1}{n_{i+1}}$ is co-prime to n_{i+1}. Set $n_{k+1} = n_1$.

Show that 2 is not a nice prime, but any odd prime is.

Solution. Let's deal with the case $p = 2$ first. We will show that there does not exist infinitely many k for which there exist $n_2, \cdots, n_k$ with $n_{i+1} \mid 2^{n_i} - 1$. For $i > 1$, n_i is odd, and fix k. Consider all prime factors of n_i for $i > 1$, let the smallest of them be q. If $q \mid n_l$ Then $2^{n_{l-1}} \equiv 1 \pmod{q}$ and $2^{q-1} \equiv 1 \pmod{q}$. If $d = \text{ord}_q(2)$, then we can say $d \mid q-1$ and $d \mid n_{l-1}$. If $d \neq 1$, then we get a smaller divisor than q since $d \leq q - 1$. This shows that $d = 1$ but then $q \mid 2^1 - 1 = 1$, contradiction.

Now we consider $p \geq 3$. We have to take care of the $k = 1$ case first, since it was explicitly mentioned, and it seems the easier part. We need to prove that, for no positive integer n,

$$n \mid p^n - 1$$
$$\left(n, \frac{p^n - 1}{n}\right) = 1$$

does not hold. Again, we assume that q is the smallest prime divisor of n. Clearly $q \neq p$, and $q \perp p$.

$$\begin{aligned} p^n &\equiv 1 \pmod q \\ p^{q-1} &\equiv 1 \pmod q \\ p^{(n,q-1)} &\equiv \pmod q \\ p &\equiv 1 \pmod q \end{aligned}$$

since $n \perp q-1 < q$.[4] From this, you should be able to tell, you can invoke LTE! Because $q \mid p - 1$, from LTE,

$$\begin{aligned} \nu_q\left(\frac{p^n - 1}{n}\right) &= \nu_q\left(p^n - 1\right) - \nu_q(n) \\ &= \nu_q(p-1) + \nu_q(n) - \nu_q(n) \\ &= \nu_q(p-1) \\ &\geq 1 \end{aligned}$$

Therefore q divides $\dfrac{p^n - 1}{n}$ and $q \mid n$, contradiction. Such n does not exist for $k = 1$.

We just have to find a construction for such $(n_1, n_2, \cdots, n_k)$. First think on the condition $\left(n_{i+1}, \dfrac{p^{n_i} - 1}{n_{i+1}}\right) = 1$. This clearly means for any odd prime divisor[5] q of n_{i+1}, q does not divide $\dfrac{p^{n_i} - 1}{n_{i+1}}$.

$$\nu_q\left(\frac{p^{n_i} - 1}{n_{i+1}}\right) = 0$$
$$\nu_q(p^{n_i} - 1) - \nu_q(n_{i+1}) = 0$$

This suggests us to take n_1 so that $n_1 = p - 1$ and $p - 1 \geq \dfrac{p+1}{2}$ is obvious for odd p. Then we have $n_2 \mid p^{p-1} - 1$. If $q^e \| p - 1$, then $q^{2e} \| p^{p-1} - 1$ according to LTE. Then $q \nmid \dfrac{p^{p-1} - 1}{q^2}$ for any $q \mid p - 1$. So we should include $n_2 = q^{2e}$. You should understand that we have to define n_3 the same way. Let q be a prime divisor of $p - 1$. Then

$$e_i = \nu_q\left(p^{n_i} - 1\right)$$
$$n_{i+1} = q^{e_i}$$

[4] we already argued the same way before

[5] we won't show the case $q = 2$ here, do that yourself in the same fashion

The only thing left to do is ensure that $n_i \geq \frac{p+1}{2}$. Note that the sequence $(e_i)_{i\geq 1}$ is increasing for a fixed q. Therefore, there will be an index r for which $n_r \geq \frac{p+1}{2}$ must hold. We leave it to the reader to verify that they satisfy the conditions of the problem.

Problem 6.34 (IMO Shortlist 2013, Problem 4, Proposed by Belgium). Prove that there exist infinitely many positive integers n such that the largest prime divisor of n^4+n^2+1 is equal to the largest prime divisor of $(n+1)^4+(n+1)^2+1$.

Solution. Let $a_n = n^4+n^2+1$, and p_n be the largest prime divisor of a_n. The problem asks to prove there are infinite n for which $p_n = p_{n+1}$.

$$(n^4+n^2+1) = (n^2+n+1)(n^2-n+1) \tag{6.1}$$

This identity tells us to consider the numbers $b_n = n^2+n+1$, and the largest prime divisor of b_n is q_n. Then $a_n = b_{n^2}$ and $p_n = q_{n^2}$. From equation (6.1), $p_n = \max(q_n, q_{n-1})$ since $b_{n-1} = (n-1)^2+n-1+1 = n^2-n+1$. By Euclidean Algorithm

$$\begin{aligned}(n^2+n+1, n^2-n+1) &= (n^2-n+1, 2n)\\ &= (n^2-n+1, 2)\\ &= 1\end{aligned}$$

Therefore $b_n \perp b_{n-1}$, implying $q_n \neq q_{n-1}$. Up until now, all we have done was self implicating. But what will allow us to prove that $p_n = p_{n+1}$ happens for infinite n? $p_n = \max(q_n, q_{n-1})$ and $p_{n+1} = \max(q_{n+1}, q_n)$. The problem requires $p_n = p_{n+1}$ or $\max(q_{n-1}, q_n) = \max(q_{n+1}, q_n)$. This provides us a hint what we need to do. We will focus on q_n. That means, we will try to prove that for infinite n, $q_n = \max(q_n, q_{n-1})$ and $q_n = \max(q_{n+1}, q_n)$. In short, we have to prove $q_n > q_{n+1}$ and $q_n > q_{n-1}$ holds true for infinite n. First we need to check that at least one such q_n exists. $q_2 = 7, q_3 = 13, q_4 = 7$, so $n = 3$ gives us such a q_n.

Assume to the contrary that, only for finite n, $q_n > q_{n-1}$ and $q_n > q_{n+1}$. Then there is a largest value of n for which this condition holds true, say it is N. Let's think if it is possible that $q_i > q_{i+1}$ for all $i \geq N$. But that would give us an infinite set of decreasing positive integers, which is impossible. So there is an $i > N$ for which $q_i < q_{i+1}$ (remember that $q_i \neq q_{i+1}$). Then is it possible to have an infinite chain of $q_i < q_{i+1} < q_{i+2} < \cdots$? No, because $q_{(i+1)^2} = p_{i+1} = \max(q_{i+1}, q_i) = q_{i+1}$. Therefore, we must have an j for which $q_j > q_{j+1}$. For that j, we have $q_j > q_{j-1}$, so it is a contradiction. Thus, there are infinite such n.

Problem 6.35. Let p be an odd prime. If $g_1, \cdots, g_{\phi(p-1)}$ are the primitive roots $\pmod p$ in the range $1 < g \leq p-1$, prove that

$$\sum_{i=1}^{\phi(p-1)} g_i \equiv \mu(p-1) \pmod p$$

Solution. Note the following.

$$\begin{aligned}\sum_i g_i &= \sum_{d|p-1} \mu(d) \sum_{k=1}^{(p-1)/d} g^{kd} \\ &= \mu(p-1)\end{aligned}$$

Because $\sum_{k=1}^{(p-1)/d} g^{kd} = 0 \mod p$, when $d < p-1$.

Problem 6.36 (IMO Shortlist 2014, N4, Proposed by Hong Kong, also used at Bangladesh TST 2015). Let n be a given integer. Define the sequence $(a_k)_{k\geq 1}$ by:

$$a_k = \left\lfloor \frac{n^k}{k} \right\rfloor$$

Prove that this sequence has infinitely many odd terms.

Solution. If n is odd, then we set $k = n^i$, so that k divides n^k and $a_k = \dfrac{n^k}{k}$ is an odd integer. Now we concentrate on even n.

When $n > 2$ is even, a prime divisor p of $n-1$ is odd. Take $p \mid n-1$ then from LTE,

$$\begin{aligned}\nu_p\left(n^{p^k}-1\right) &= \nu_p(n-1) + \nu_p(p^k) \\ &= \nu_p(n-1) + k\end{aligned}$$

Thus, p^k divides $n^{p^k}-1$, so $\dfrac{n^{p^k}-1}{p^k}$ is an integer. We have

$$\begin{aligned}a_{p^j} &= \left\lfloor \frac{n^{p^j}}{p^j} \right\rfloor \\ &= \frac{n^{p^j}-1}{p^j}\end{aligned}$$

which is an odd integer. If $n = 2$, then $a_k = \left\lfloor \dfrac{2^k}{k} \right\rfloor$. Note that, $2^m - 1$ is divisible by 3 for even m. Therefore, we should consider $k = 2 \cdot 3^i$. From LTE, $3^{i+1} \| 2^{2\cdot 3^i} - 1$. But if k is even it won't divide any odd integer. No worries, we will just borrow a power of 2.

$$\begin{aligned}a_{3\cdot 4^j} &= \left\lfloor \frac{2^{3\cdot 4^j}}{3\cdot 4^j} \right\rfloor \\ &= \frac{2^{3\cdot 4^j} - 4^j}{3\cdot 4^j}\end{aligned}$$

is an odd integer since 4^j clearly divides $2^{3\cdot 4^j}$ and $3 \cdot 4^j > j$. Show why 3 divides the numerator yourself.

Problem 6.37 (IMO Shortlist 2014, N5, Proposed by Belgium, also used at Bangladesh TST 2015). Find all triples (p,x,y) consisting of a prime number p and two positive integers x and y such that $x^{p-1}+y$ and $x+y^{p-1}$ are both powers of p.

Solution. Let $y+x^{p-1}=p^a$ and $x+y^{p-1}=p^b$ and $y>x$ without loss of generality (so $b>a$ too). If $p=2$, then $x+y=2^a$ so $(x,y)=(x,2^a-x)$ works with any $a\in\mathbb{N}, x<2^a$.

We need to deal with odd p now. Let $g=(x,y)$ and $x=gm, y=gn$ with $m\perp n$. We intend to prove that $x\perp y$. If not, $g=p^s$ for some s.

$$\begin{aligned} p^s n+p^{s(p-1)}m^{p-1}&=p^a\\ p^s m+p^{s(p-1)}n^{p-1}&=p^b \end{aligned}$$

If $s\neq 0$, the dividing the equations by p^s we get,

$$\begin{aligned} n+p^{s(p-2)}m^{p-1}&=p^{a-s}\\ m+p^{s(p-2)}n^{p-2}&=p^{b-s} \end{aligned}$$

Since $p>2$, p divides $p^{s(p-2)}, p^{a-s}$ and p^{b-s}, hence p divides both m and n. But this contradicts the fact that $m\perp n$. Therefore, $s=0$, and $(x,p)=(y,p)=(x,y)=1$. From FLT,

$$\begin{aligned} x+y^{p-1}&\equiv x+1 \pmod p\\ x^{p-1}+y&\equiv y+1 \pmod p \end{aligned}$$

Thus, $p\mid x+1-(y+1)=x-y$. You must understand by now that we are just trying to set this up for applying LTE. Without loss of generality, let's take $a<b$.

$$\begin{aligned} &p^a\mid x+y^{p-1}\\ &p^a\mid y+x^{p-1}\\ &p^a\mid x(x^{p-1}+y)-y(x+y^{p-1})\\ &p^a\mid x^p-y^p \end{aligned}$$

Since $x\perp y$ and $p\mid x-y$, if $p^\alpha\| x-y$, using LTE,

$$\begin{aligned} \nu_p(x^p-y^p)&=\nu_p(x-y)+\nu_p(p)\\ &=\alpha+1 \end{aligned}$$

We get $\alpha+1\geq a$, so $p^{a-1}\mid x-y$. Since $y>x$, assume that $y-x=p^{a-1}k$.

$$\begin{aligned} x^{p-1}+y&=p^a\\ y-x&=p^{a-1}k\\ x^{p-1}+y-(y+x)&p^a-p^{a-1}k\\ x^{p-1}+x&=p^{a-1}(p-k)\\ x(x^{p-2}+1)&=p^{a-1}(p-k) \end{aligned}$$

Because $x \perp p$, $x \mid p-k$ which implies $p-k \geq x$ or $p \geq x+k \geq x+1$. On the other hand, we had $p \mid x+1$ or $x+1 \geq p$. Combining these two, $x+1=p$ or $x=p-1$ and $k=1$. Finally,

$$\begin{aligned} y &= x + p^{a-1} \\ &= p - 1 + p^{a-1} \end{aligned}$$

But from the given condition,

$$\begin{aligned} x^{p-1} + y &= p^a \\ (p-1)^{p-1} + p^{a-1} + p - 1 &= p^a \\ (p-1)^{p-1} + p - 1 &= p^{a-1}(p-1) \\ (p-1)^{p-2} + 1 &= p^{a-1} \\ (p-1)^{p-2} &= p^{a-1} - 1 \end{aligned}$$

Since p is odd, if $a-1>1$, then according to Zsigmondy's theorem, $p^{a-1}-1$ has a prime divisor that does not divide $p-1$. So $a-1=1$ or $a=2$ and $p=3$. Thus, $x=2$ and $y=x+p^{a-1}=5$. By symmetry, $(5,2)$ is also a solution.

Problem 6.38 (Russia 2000). Do there exist three distinct pairwise co-prime integers a, b, c such that $a \mid 2^b+1$, $b \mid 2^c+1$ and $c \mid 2^a+1$?

Solution. Let p be the smallest prime divisor of a. Then $p \mid 2^b+1$, so $2^b \equiv -1 \pmod{p}$.

$$\begin{aligned} 2^{2b} &\equiv 1 \pmod{p} \\ 2^{p-1} &\equiv 1 \pmod{p} \\ 2^{(2b,p-1)} &\equiv 1 \pmod{p} \end{aligned}$$

Without loss of generality, we can assume that $p<q,r$ where q and r are the smallest prime divisors of b and c (even if it is not, we can just switch the places of p and q, or r). Therefore, $(2b, p-1)=2$ and $p \mid 2^2-1=3$ so $p=3$. Let $a=3x$. We can see that $3 \nmid x$, because otherwise 9 divides 2^b+1, which would be possible only if $b=3y$ meaning that $(a,b) \geq 3$.

Again we are out of information. In order to dig out some information, let's take the smallest prime divisor of x, b and c and call it q. If $q \mid x$, then $q \mid 2^b+1$ and again q is smaller than the smallest prime divisor of b and c. But this again gives that $q=3$, which gives the contradiction that x is divisible by 3. Thus, we can say q divides b or c. If $q \mid c$, then

$$\begin{aligned} 2^{3x} &\equiv -1 \pmod{q} \\ 8^{2x} &\equiv 1 \pmod{q} \\ 8^{q-1} &\equiv 1 \pmod{q} \\ 8^{(2x,q-1)} &\equiv 1 \pmod{q} \end{aligned}$$

Here, x must have no smaller prime divisor than q, otherwise that would have been the smallest prime divisor instead of q. So, $(2x, q-1)=2$ and $q \mid 8^2-1=3^2 \cdot 7$. Since q is

co-prime to $a = 3x, q \neq 3$. So $q = 7$ but then $7 \mid 2^a + 1 = 8^x + 1$, which is a contradiction due to

$$8^x + 1 \equiv 1 + 1 \pmod 7$$

Thus, q must be the smallest prime divisor of b, and so c does not have any prime divisor less than or equal to q. Similarly,

$$\begin{aligned} 2^c &\equiv -1 \pmod q \\ 2^{2c} &\equiv 1 \pmod q \\ 2^{q-1} &\equiv 1 \pmod q \\ 2^{(2c, q-1)} &\equiv 1 \pmod q \\ 2^2 &\equiv 1 \pmod q \end{aligned}$$

which gives us $q = 3$ but then $3 \mid b$, a contradiction. Therefore, b can not have any prime divisor, $b = 1$. We also have $c \mid 2^3 + 1 = 9$, so $c \in \{1, 3, 9\}$. But if $c = 1$, it would collide with $b = 1$. If $c = 3$ or $c = 9$, it would not be co-prime with a. Therefore, no such a, b, c exist.

Problem 6.39 (Austria 2010). Let

$$f(n) = 1 + n + \cdots + n^{2010}$$

For every integer m with $2 \leq m \leq 2010$, there is no non-negative integer n such that $f(n)$ is divisible by m.

Solution. We can write $f(n)$ as

$$f(n) = \frac{n^{2011} - 1}{n - 1}$$

Let p be a prime factor of $f(n)$. Then if $p \mid n - 1$, we have $n \equiv 1 \pmod p$. Take $d = \text{ord}_p(n)$. If $p \perp (n - 1)$, then

$$\begin{aligned} n^{2011} &\equiv 1 \pmod p \\ n^d &\equiv 1 \pmod p \end{aligned}$$

We have $d \mid 2011$, if $d = 1$.

$$\begin{aligned} 1 + n + \cdots + n^{2010} &\equiv 1 + 1 + \cdots + 1 \pmod p \\ f(n) &\equiv 2011 \pmod p \end{aligned}$$

This gives us $p \mid 2011$. Moreover, from FLT, we also have

$$n^{p-1} \equiv 1 \pmod p$$

so $d \mid p - 1$. If $d = 2011$, then $p \equiv 1 \pmod{2011}$. But for $1 < m < 2011$, there is no m for which m has a prime divisor p so that $2011 \mid p$ or $p \equiv 1 \pmod{2011}$ because $p \geq 2011 > m$.

Remark. We can make a general result. Every prime divisor q of

$$f(n) = 1 + n + \cdots + n^{p-1}$$

must be either p or $q \equiv 1 \pmod{p}$, where p is a prime.

Problem 6.40 (APMO 2014, Problem 3). Find all positive integers n such that for any integer k there exists an integer a for which $a^3 + a - k$ is divisible by n.

Solution. Make sense of the problem before you try it. It can be rephrased this way: find all n such that the set $a^3 + a$ for $a = 1, 2, \cdots, n$ we get a complete residue class modulo n. Or, for no two $1 \leq a < b \leq n$,

$$a^3 + a \equiv b^3 + b \pmod{n}$$

In order to understand the values of n, see some examples with smaller values first. A pattern follows, $n = 1, 3, 9$ works. So may be the condition holds if and only if $n = 3^k$.

Checking the if part is easy.

$$\begin{aligned} a^3 + a &\equiv b^3 + b \pmod{3^k} \\ a^3 - b^3 + a - b &\equiv 0 \pmod{3^k} \\ (a-b)(a^2 + ab + b^2 + 1) &\equiv 0 \pmod{3^k} \end{aligned}$$

For $a \not\equiv b \pmod{3}$, we can see that $3 \nmid a^2+ab+b^2+1$. So we must have $a \equiv b \pmod{3^k}$. Now we need to prove that if $n \neq 3^k$, the condition does not hold. If n has a prime divisor p for which the condition doesn't hold, then the same is true for n as well, so let's just look at the primes.

If $p \equiv 1 \pmod{4}$ is a prime, we know that -1 is a quadratic residue of p, so there is an x for which

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

If we choose $y = 0$,

$$x^3 + x \equiv y^3 + y \pmod{p}$$

So, n can not have any prime factor $\equiv 1 \pmod{4}$. Let $p \equiv 3 \pmod{4}$ be a prime. We must have

$$\begin{aligned} (1^3 + 1) \cdot (2^3 + 2) \cdots ((p-1)^3 + p - 1) &\equiv 1 \cdot 2 \cdots (p-1) \pmod{p} \\ 1 \cdot 2 \cdots (p-1) \prod_{k=1}^{p-1} (k^2 + 1) &\equiv 1 \cdot 2 \cdots (p-1) \pmod{p} \\ \prod_{k=1}^{p-1} (k^2 + 1) &\equiv 1 \pmod{p} \\ \prod_{k=1}^{p-1} (k + i)(k - i) &\equiv 1 \pmod{p} \end{aligned}$$

Note that, using Lagrange's theorem, we can imply,

$$\begin{aligned}\prod_{k=1}^{p-1}(k+i)\prod_{k=1}^{p-1}(k-i) &\equiv 1 \pmod p\\ (k^{p-1}-1)(k^{p-1}-1) &\equiv 1 \pmod p\\ (k^{p-1})^2 - 2k^{p-1} + 1 &\equiv 1 \pmod p\\ 2 - 2k^{p-1} &\equiv 1 \pmod p\end{aligned}$$

Here, $k^{p-1} \equiv \pm 1 \pmod p$, so we have $2-(\pm 2) \equiv 1 \pmod p$ or $p = 3$. Hence, proven.

Problem 6.41 (Croatia 2014). Do there exist positive integers m and n such that m^2+n and n^2+m are squares of positive integers?

This is a problem where we use another technique, we will call it *squeezing between squares*. The name is due to *Dan Schwarz*, who was a problem solver and creator from Romania, and a user on Art of Problem Solving. He used the handle *mavropnevma* and taught many people many things through the forum. In a solution of a similar problem, he used the words squeezing between squares. So, out of respect we named this.

Solution. Due to symmetry, we can assume $m \geq n$ without loss of generality.

$$\begin{aligned}m^2 + n \geq m^2 + m &> m^2\\ m^2 + 2m + 1 &> m^2 + m\\ m^2 < m^2 + m &< (m+1)^2\end{aligned}$$

This says that m^2+m resides between two squares, so it can not be a perfect square. Therefore, no such (m,n).

Problem 6.42 (Turkey 2011). Let $a_{n+1} = a_n^3 - 2a_n^2 + 2$ for all $n \geq 1$ and $a_1 = 5$. Prove that if $p \equiv 3 \pmod 4$ and p is a divisor of $a_{2011}+1$, then $p = 3$.

Solution. The recursion is a cheeky one.

$$\begin{aligned}a_{n+1} - 2 &= a_n^2(a_n - 2)\\ &= a_n^2 a_{n-1}^2(a_{n-1} - 2)\\ &\vdots\\ &= a_n^2 a_{n-1}^2 \cdots a_2(a_1 - 2)\\ &= 3a_2^2 \cdots a_n^2\\ a_{n+1} + 1 &= 3(a_2^2 \cdots a_n^2 + 1)\end{aligned}$$

If $p \mid a_{n+1}+1$, then p divides 3 or p divides $a_2^2 \cdots a_n^2 + 1$. But we know that $p \equiv 3 \pmod 4$ can not divide a bisquare. Thus, p must divide 3, or $p = 3$.

Problem 6.43 (IMO Shortlist 2004, N2). For $n \in \mathbb{N}$ let,

$$f(n) = \sum_{i=1}^{n} \gcd(i,n)$$

(a) Prove that $f(mn) = f(m)f(n)$ for all $m \perp n$.

(b) Prove that, for all a, there is a solution to $f(an) = an$.

Solution. Since we are required to prove that f is multiplicative, it may be better if $f(n)$ can be written in terms of divisors of n. Since we are facing this kind of problem for the first time, let's show a manipulation. It is clear that $f(10) = \sum_{i=1}^{10}(i, 10)$, which is

$$= (1,10) + (2,10) + (3,10) + (4,10) + (5,10) + (6,10) \\ + (7,10) + (8,10) + (9,10) + (10,10)$$

and hence,

$$\begin{aligned} f(10) &= 1+2+1+2+5+2+1+2+1+10 \\ &= 1\cdot 4 + 2\cdot 4 + 5\cdot 1 + 10\cdot 1 \end{aligned}$$

First of all, $1, 2, 5, 10$ are divisors of 10. Since (i, n) will be a divisor of n, it makes sense. Now we just need to figure out how to determine those numbers $4, 4, 1, 1$ for $1, 2, 5, 10$ respectively. Let's think about the case when divisor, $d = 2$. We want $(i, 10) = d$ so we can write $i = dj$ and $10 = dm$ where $(j, m) = 1$. Since we are counting all such possible j, it is simply the number of j less than or equal to m, which are co-prime to m. In other words, the coefficient of i is $\varphi(m) = \varphi\left(\frac{10}{d}\right)$. Now, let's prove it formally.

$$\begin{aligned} f(n) &= \sum_{i=1}^{n}(i, n) \\ &= \sum_{i=1}^{n}(dj, dm) \\ &= \sum_{d|n}\sum_{\substack{j=1 \\ j\perp m}}^{m} d(j, m) \\ &= \sum_{d|n} d\varphi(m) \\ &= \sum_{d|n} d\varphi\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \frac{n}{d}\varphi(d) \\ &= n\sum_{d|n}\frac{\varphi(d)}{d} \end{aligned}$$

Let's concentrate on proving the claims now.

(a) Let $m \perp n$.

$$\begin{aligned} f(mn) &= \sum_{d \mid mn} d\varphi\left(\frac{mn}{d}\right) \\ &= \sum_{\substack{d=ef \\ e \mid m \\ f \mid n}} ef\varphi\left(\frac{mn}{ef}\right) \\ &= \sum_{\substack{e \mid m \\ f \mid n}} ef\varphi\left(\frac{m}{e}\right)\varphi\left(\frac{n}{f}\right) \\ &= \sum_{e \mid m} e\varphi\left(\frac{m}{e}\right) \sum_{f \mid n} f\left(\frac{n}{f}\right) \\ &= f(m)f(n) \end{aligned}$$

We could also prove it using Dirichlet product. If $f(n) = n$ and $g(n) = \varphi(n)$, then both f and g are multiplicative. So, their Dirichlet product would be multiplicative as well.

$$\begin{aligned} f * g &= \sum_{d \mid n} f(d)g\left(\frac{n}{d}\right) \\ &= \sum_{d \mid n} d\varphi\left(\frac{n}{d}\right) \end{aligned}$$

must be multiplicative then!

(b) $f(an) = an$ means

$$\sum_{d \mid an} d\varphi\left(\frac{an}{d}\right) = an$$

But clearly the sum on the left side is hard to deal with. It would be better if we could have another representation, probably a closed form instead of a summation. Let's determine $f(p^i)$ first.

$$\begin{aligned} f(p^e) &= p^e \sum_{d \mid p^e} \frac{\varphi(d)}{d} = p^e \sum_{i=0}^{e} \frac{\varphi(p^i)}{p^i} \\ &= p^e \left(1 + \sum_{i=1}^{e} \frac{p^{i-1}(p-1)}{p^i}\right) \\ &= p^e \left(1 + \sum_{i=1}^{e} \frac{p-1}{p}\right) \\ &= p^e \left(1 + \frac{e(p-1)}{p}\right) \end{aligned}$$

From the given condition, $f(n) = an$, so for $n = p^e$, it implies

$$p^e\left(1 + \frac{e(p-1)}{p}\right) = ap^e$$

and so,

$$1 + \frac{e(p-1)}{p} = a$$

Here, a is integer, so $\frac{e(p-1)}{p}$ is an integer too. Since $p \perp p-1$, we must have $p \mid e$. Let $e = pk$ so that

$$a = 1 + k(p-1)$$

If this has to be true for any a, we should assume $p = 2$, and we get $a = 1 + k$ or $k = a - 1, e = 2(a-1)$. This gives us an infinite solution for $n = 2^{2(a-1)}$.

Problem 6.44 (IMO 2006). Find all integers x and y which satisfy the equation

$$1 + 2^x + 2^{2x+1} = y^2$$

Solution. Obviously, $x \geq 0$. If $x = 0$, then $y = \pm 2$. Suppose that $x \geq 1$. Clearly, y is an odd number, so assume that $y = 2k + 1$. Now:

$$\begin{aligned} 1 + 2^x + 2^{2x+1} &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \end{aligned}$$

Removing 1 from both sides and then dividing by 4, one can write the above equation as

$$2^{x-2}(2^{x+1} + 1) = k(k+1) \tag{6.2}$$

We consider two cases:

1. k is even. So $k + 1$ is odd and $(2^{x-2}, k+1) = 1$. Then $2^{x-2} \mid k(k+1)$ reduces to $2^{x-2} \mid k$. Let $k = 2^{x-2} \cdot t$ and rewrite equation (6.2) to achieve

   $$2^{x+1} + 1 = t(2^{x-2} \cdot t + 1)$$

   So, t is odd. If $t = 1$, we have $2^{x+1} = 2^{x-2}$, which is absurd. Thus $t \geq 3$ and

   $$\begin{aligned} t(2^{x-2} \cdot t + 1) &= 2^{x-2} \cdot t^2 + t \\ &\geq 9 \cdot 2^{x-2} + 3 \\ &> 2^{x+1} + 1 \end{aligned}$$

   and no solutions in this case.

2. k is odd. So $k+1$ is even and $\gcd(2^{x-2}, k) = 1$. Then $2^{x-2} \mid k(k+1)$ reduces to $2^{x-2} \mid k+1$. Let $k+1 = 2^{x-2} \cdot m$ and rewrite equation (6.2) as

$$2^{x+1} + 1 = m(2^{x-2} \cdot m - 1)$$

So m is odd. $m = 1$ gives no solutions, so $m \geq 3$. For $m = 3$, we have

$$\begin{aligned} 2^{x+1} + 1 &= 3(2^{x-2} \cdot 3 - 1) \\ \implies 4 &= 9 \cdot 2^{x-2} - 2^{x+1} \\ \implies 4 &= 2^{x-2}(9-8) \\ \implies x &= 4 \end{aligned}$$

Thus for $m = 3$, we have $k = 2^{x-2} \cdot m - 1 = 11$ and so $y = 2k + 1 = 23$, and $(x, y) = (4, 23)$ is a solution. If (x, y) is a solution, obviously $(x, -y)$ is a solution too. So $(x, y) = (4, -23)$ is also a solution.

We will show that $m \geq 5$ gives no solutions. Note that

$$\begin{aligned} m(2^{x-2} \cdot m - 1) &\geq 5(2^{x-2} \cdot 5 - 1) \\ &= 25 \cdot 2^{x-2} - 5 \\ &= (8 + 16 + 1) \cdot 2^{x-2} - 5 \\ &= 2^{x+1} + 2^{x+2} + 2^{x-2} - 5 \\ &> 2^{x+1} + 1 \end{aligned}$$

So $m(2^{x-2} \cdot m - 1) > 2^{x+1} + 1$ for $m \geq 5$ and no solutions.

Hence the solutions are: $(x, y) = \{(0, 2), (0, -2), (4, 23), (4, -23)\}$.

§§7 Practice Challenge Problems

Problem 7.1. Show that the ratio $\frac{\sigma(n)}{n}$ can be arbitrarily large for infinitely many n.

Problem 7.2. Prove that for all positive integers n, there exists an n-digit prime.

Problem 7.3. There are n points on a circle with $n > 10$, and each point is given a number that is equal to the average of the numbers of its two nearest neighbors. Show that all the numbers must be equal.

Problem 7.4. Let $F(n)$ be the nth Fibonacci number, show that for some $n > 1$, $F(n)$ ends with 2007 zeros.

Problem 7.5. Let $N = .23571113...$ where N consists of all prime numbers concatenated together after the decimal. Determine if N is rational or irrational.

Problem 7.6. Prove that there exists a positive integer n such that the four leftmost digits of the decimal representation of $2n$ is 2007.

Problem 7.7. The only sets of $N-1$ (distinct) integers, with no non-empty subset having its sum of elements divisible by N, are those where all integers are congruent to a same residue modulo N, relatively prime with N.

Problem 7.8 (Austrian Mathematical Olympiad, 2016). Determine all composite positive integers n with the following property: If $1 = d_1 < d_2 < \cdots < d_k$ are the divisors of n then

$$d_2 - d_1 : d_3 - d_2 : \cdots : d_k - d_{k-1} = 1 : 2 : \cdots k - 1$$

Problem 7.9 (Belarus 2009). Find all $m, n \in \mathbb{N}$ such that $m! + n! = m^n$.

Problem 7.10. Integer $n > 2$ is given. Find the biggest integer d, for which holds, that from any set S consisting of n integers, we can find three different (but not necessarily disjoint) nonempty subsets, such that sum of elements of each of them is divisible by d.

Problem 7.11. Consider the set $M = \{1, 2, 3, ..., 2007\}$. Prove that in any way we choose the subset X with 15 elements of M there exist two disjoint subsets A and B in X such that the sum of the members of A is equal to the sum of the members of B.

Problem 7.12 (India 2014). Let $n \in \mathbb{N}$. Show that,

$$\left\lfloor \frac{n}{1} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor + ... + \left\lfloor \frac{n}{n} \right\rfloor + \lfloor \sqrt{n} \rfloor$$

is even.

Problem 7.13. Given 101 distinct non-negative integers less than 5050 show that one can choose four a, b, c, d such that $a + b - c - d$ is a multiple of 5050.

Problem 7.14 (Bulgarian Mathematical Olympiad, 2016). Find all positive integers m and n such that $\left(2^{2^m} + 1\right)\left(2^{2^n} + 1\right)$ is divisible by mn.

Problem 7.15 (Slovenia 2010). Find all prime numbers p, q and r such that $p > q > r$ and the numbers $p - q, p - r$ and $q - r$ are also prime.

Problem 7.16 (Croatia Mathematical Olympiad, First Round, 2016). Determine the number of positive integers smaller than 1000000, that are also perfect squares and give a remainder 4 when divided by 8.

Problem 7.17. Prove that among 81 natural numbers whose prime divisors are in the set $\{2, 3, 5\}$ there exist four numbers whose product is the fourth power of an integer.

Problem 7.18. We chose $n+2$ numbers from set $\{1, 2, ...3n\}$. Prove that there are always two among the chosen numbers whose difference is more than n but less than $2n$.

Problem 7.19 (India 2014). Let a, b be natural numbers with $ab > 2$. Suppose that the sum of their greatest common divisor and least common multiple is divisble by $a + b$. Prove that the quotient is at most $\frac{a+b}{4}$. When is this quotient exactly equal to $\frac{a+b}{4}$?

Problem 7.20. The integers $1, ..., n$ are arranged in any order. In one step any two neighboring integers may be interchanged. Prove that the initial order can never be reached after an odd number of steps.

Problem 7.21. A palindrome is a number or word that is the same when read forward and backward, for example, 176671 and *civic*. Can the number obtained by writing the numbers from 1 to n in order (for some $n > 1$) be a palindrome?

Problem 7.22 (IMO Shortlist N2, Proposed by Jorge Tipe, Peru). A positive integer N is called balanced, if $N = 1$ or if N can be written as a product of an even number of not necessarily distinct primes. Given positive integers a and b, consider the polynomial P defined by $P(x) = (x + a)(x + b)$.

(a) Prove that there exist distinct positive integers a and b such that all the number $P(1), P(2),..., P(50)$ are balanced.

(b) Prove that if $P(n)$ is balanced for all positive integers n, then $a = b$.

Problem 7.23. Let n be an integer. Prove that if the equation $x^2 + xy + y^2 = n$ has a rational solution, then it also has an integer solution.

Problem 7.24 (Iran Olympiad, Third Round). Let p be a prime number. Prove that, there exists integers x, y such that $p = 2x^2 + 3y^2$ if and only if $p \equiv 5, 11 \pmod{24}$.

Problem 7.25 (Polish Math Olympiad). Let S be a set of all positive integers which can be represented as $a^2 + 5b^2$ for some integers a, b such that $a \perp b$. Let p be a prime number such that $p = 4n + 3$ for some integer n. Show that if for some positive integer k the number kp is in S, then $2p$ is in S as well.

Problem 7.26. Prove that the equation $x^3 - x + 9 = 5y^2$ has no solution in integers.

Problem 7.27 (India TST). 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 colour than T.

Problem 7.28. Prove that, for any positive integer k, there are positive integers $a, b > 1$ such that

$$k = \frac{a^2 + b^2 - 1}{ab}$$

Problem 7.29. Let a, b, and c be positive integers such that $0 \leq a^2 + b^2 - abc \leq c$. Prove that $a^2 + b^2 - abc$ is a perfect square.

Problem 7.30. Let the n^{th} Lemur set, L_n, be the set composed of all positive integers that are equal to the sum of the squares of their first n divisors. For example, $L_1 = \{1\}$, $L_2 = \{\}$, and $L_4 = \{130\}$.

a Find L_3, L_5, and L_6.

b Describe all n for which L_n is empty.

c Describe all n for which L_n is infinite.

d Provide a method for finding members of non-empty Lemur sets.

Problem 7.31 (IMO 2007, Problem 5). Let a and b be positive integers so that $4ab - 1$ divides $(4a^2 - 1)^2$. Prove that $a = b$.

Problem 7.32. Let $a_1, a_2, \ldots, a_n$ be positive integers such that $a_1 < a_2 < \cdots < a_n$. Prove that

$$\sum_{i=1}^{n-1} \frac{1}{[a_i, a_{i-1}]} < 1$$

Problem 7.33. Let $N = 2^{p_1 \cdots p_n} + 1$ where p_i are distinct primes greater than 2 and $\tau(N)$ is the number of divisors of N. Maximize $\tau(N)$.

Problem 7.34 (Masum Billal). Let $n \geq 3, a, d$ be positive integers so that $a, a+d, \ldots, a+(n-1)d$ are all primes. If $\lambda(n)$ is the number of primes *strictly less than* n, prove that,

$$N = 2^{\lfloor \frac{d}{2} \rfloor} + 1$$

has at least $2^{2^{\lambda(n)-2}-1}$ divisors.

Problem 7.35. For $n \geq 2$,

$$F_n^{\frac{F_{n+m}-1}{2}} \equiv 1 \pmod{F_{n+m}}$$

Problem 7.36. Let $f(x) = x^3 + 17$. Prove that for each natural number $n \geq 2$, there is a natural number x for which $f(x)$ is divisible by 3^n but not 3^{n+1}.

Problem 7.37 (Boylai). Show that every Fermat prime is of the form $6k - 1$.

Problem 7.38 (Iran TST 2015). We are given three natural numbers a_1, a_2, a_3. For $n \geq 3$,

$$a_{n+1} = [a_{n-1}, a_n] - [a_{n-1}, a_{n-2}]$$

Prove that there exists an index $k \leq a_3 + 4$ such that $a_k \leq 0$.

Problem 7.39 (Bosnia Olympiad 2013, Second Day). Find all primes p and q such that $p \mid 30q - 1$ and $q \mid 30p - 1$.

Problem 7.40 (IMO Shortlist 2004, N3, Proposed by Iran). f is a function with $f : \mathbb{N} \to \mathbb{N}$ so that

$$f^2(m) + f(n) \mid (m^2 + n)^2$$

Show that $f(n) = n$.

Problem 7.41 (Columbia 2010). Find all pairs of positive integers (m, n) such that $m^2 + n^2 = (m+1)(n+1)$.

Problem 7.42 (AMOC 2014, Senior Section). For which integers $n \geq 2$ is it possible to separate the numbers $1, 2, \ldots, n$ into two sets such that the sum of the numbers in one of the sets is equal to the product of the numbers in the other set?

Problem 7.43 (Greece). Determine all triples (p, m, n) of positive integers such that p is a prime number and $p^m - 8 = n^3$.

Problem 7.44 (Canadian Students Math Olympiad 2011). For a fixed positive integer k, prove that there exist infinitely many primes p such that there is an integer w, where $w^2 - 1$ is not divisible by p, and the order of w modulo p is the same as the order of w modulo p^k.

Problem 7.45 (China TST 2009). Let $a > b > 1$ and b be an odd integer, $n \in \mathbb{N}$. If $b^n \mid a^n - 1$, then prove that $a^b > \dfrac{3^n}{n}$.

Problem 7.46 (Kazakhstan 2015). Solve in positive integers: $x^y y^x = (x+y)^z$.

Problem 7.47 (Kazakhstan 2015). $P_k(n)$ is the product of all divisors of n that are divisible by k (in empty case it is 1). Prove that, $P_1(n) \cdot P_2(n) \cdots P_n(n)$ is a perfect square.

Problem 7.48 (Russia 2000). If a perfect number greater than 6 is divisible by 3, it is also divisible by 9. If a perfect number greater than 28 is divisible by 7, it is also divisible by 49.

Problem 7.49 (Croatia 2014). For a positive integer n denote by $s(n)$ the sum of all positive divisors of n and by $d(n)$ the number of positive divisors of n. Determine all positive integers n such that

$$s(n) = n + d(n) + 1$$

Problem 7.50 (IMO 2003, Problem 2, N3). Find all pairs of positive integers (a, b) such that

$$\frac{a^2}{2ab^2 - b^3 + 1}$$

is a positive integer.

Problem 7.51. Show that $n = \varphi(n) + \tau(n)$ if and only if n is a prime.

Problem 7.52 (IMO Shortlist 2004, N2 Part (c)). Find all n for which $f(n) = an$ has a unique solution where,

$$f(n) = \sum_{i=1}^{n} (i, n)$$

Problem 7.53. Let k be a positive integer. Find all positive integers n such that $3^k \mid 2^n - 1$.

Problem 7.54. Let a, b be distinct real numbers such that the numbers

$$a - b,\ a^2 - b^2,\ a^3 - b^3, \ldots$$

are all integers. Prove that a, b are both integers.

Problem 7.55 (MOSP 2001). Find all quadruples of positive integers (x, r, p, n) such that p is a prime number, $n, r > 1$ and $x^r - 1 = p^n$.

Problem 7.56 (China TST 2009). Let $a > b > 1$ be positive integers and b be an odd number, let n be a positive integer. If $b^n \mid a^n - 1$, then show that $a^b > \frac{3^n}{n}$.

Problem 7.57 (Romanian Junior Balkan TST 2008). Let p be a prime number, $p \neq 3$, and integers a, b such that $p \mid a+b$ and $p^2 \mid a^3+b^3$. Prove that $p^2 \mid a+b$ or $p^3 \mid a^3+b^3$.

Problem 7.58. Let m and n be positive integers. Prove that for each odd positive integer b there are infinitely many primes p such that $p^n \equiv 1 \pmod{b^m}$ implies $b^{m-1} \mid n$.

Problem 7.59. Find all positive integers n such that

$$\frac{2^{n-1}+1}{n}$$

is an integer.

Problem 7.60. Find all primes p, q such that $\dfrac{(5^p-2^p)(5^q-2^q)}{pq}$ is an integer.

Problem 7.61. For some natural number n let a be the greatest natural number for which $5^n - 3^n$ is divisible by 2^a. Also let b be the greatest natural number such that $2^b \leq n$. Prove that $a \leq b+3$.

Problem 7.62. Determine all sets of non-negative integers x, y and z which satisfy the equation

$$2^x + 3^y = z^2$$

Problem 7.63 (IMO ShortList 2007). Find all surjective functions $f : \mathbb{N} \to \mathbb{N}$ such that for every $m, n \in \mathbb{N}$ and every prime p, the number $f(m+n)$ is divisible by p if and only if $f(m)+f(n)$ is divisible by p.

Problem 7.64 (Romania TST 1994). Let n be an odd positive integer. Prove that $((n-1)^n+1)^2$ divides $n(n-1)^{(n-1)^n+1}+n$.

Problem 7.65. Find all positive integers n such that $3^n - 1$ is divisible by 2^n.

Problem 7.66 (Romania TST 2009). Let $a, n \geq 2$ be two integers, which have the following property: there exists an integer $k \geq 2$, such that n divides $(a-1)^k$. Prove that n also divides $a^{n-1} + a^{n-2} + \cdots + a + 1$.

Problem 7.67. Find all the positive integers a such that $\frac{5^a+1}{3^a}$ is a positive integer.

Problem 7.68. Find all primes p, q such that $pq \mid 5^p + 5^q$.

Problem 7.69. Find all primes p, q such that $pq \mid 2^p + 2^q$.

Problem 7.70 (APMO 2016). A positive integer is called *fancy* if it can be expressed in the form

$$2^{a_1} + 2^{a_2} + \cdots + 2^{a_{100}}$$

where $a_1, a_2, \cdots, a_{100}$ are non-negative integers that are not necessarily distinct. Find the smallest positive integer n such that no multiple of n is a fancy number.

Problem 7.71 (Argentina Intercollegiate Olympiad First Level 2016). Find all positive integers a, b, c, and d, all less than or equal to 6, such that

$$\frac{a}{b} = \frac{c}{d} + 2$$

Problem 7.72 (Argentina Intercollegiate Olympiad Second Level 2016). Find all positive integers x and y which satisfy the following conditions:

1. x is a 4—digit palindromic number, and
2. $y = x + 312$ is a 5—digit palindromic number.

Note. A palindromic number is a number that remains the same when its digits are reversed. For example, 16461 is a palindromic number.

Problem 7.73 (Argentina Intercollegiate Olympiad Third Level 2016). Find a number with the following conditions:

1. it is a perfect square,
2. when 100 is added to the number, it equals a perfect square plus 1, and
3. when 100 is again added to the number, the result is a perfect square.

Problem 7.74 (Argentina Intercollegiate Olympiad Third Level 2016). Let $a_1, a_2, \ldots, a_{15}$ be an arithmetic progression. If the sum of all 15 terms is twice the sum of the first 10 terms, find $\frac{d}{a_1}$, where d is the common difference of the progression.

Problem 7.75 (Austria Federal Competition for Advanced Students Final Round 2016). Determine all composite positive integers n with the following property: If $1 = d_1 < d_2 < \cdots < d_k = n$ are all the positive divisors of n, then

$$(d_2 - d_1) : (d_3 - d_2) : \cdots : (d_k - d_{k-1}) = 1 : 2 \cdots : (k-1)$$

Problem 7.76 (Austria National Competition Final Round 2016). Let a, b, and c be integers such that

$$\frac{ab}{c} + \frac{ac}{b} + \frac{bc}{a}$$

is an integer. Prove that each of the numbers

$$\frac{ab}{c}, \frac{ac}{b}, \text{ and } \frac{bc}{a}$$

is an integer.

Problem 7.77 (Austria Beginners' Competition 2016). Determine all non-negative integers n having two distinct positive divisors with the same distance from $n/3$.

Problem 7.78 (Austria Regional Competition 2016). Determine all positive integers k and n satisfying the equation

$$k^2 - 2016 = 3^n$$

Problem 7.79 (Azerbaijan TST 2016). The set A consists of natural numbers such that these numbers can be expressed as $2x^2 + 3y^2$, where x and y are integers. $(x^2 + y^2 \neq 0)$

1. Prove that there is no perfect square in the set A.

2. Prove that multiple of odd number of elements of the set A cannot be a perfect square.

Problem 7.80 (Azerbaijan Junior Mathematical Olympiad 2016). Given

$$34! = 295232799039a041408476186096435b0000000$$

in decimal representation, find the numbers a and b.

Problem 7.81 (Azerbaijan Junior Mathematical Olympiad 2016). Prove that if for a real number a, $a + \frac{1}{a}$ is integer then $a^n + \frac{1}{a^n}$ is also integer for any positive integer n.

Problem 7.82 (Azerbaijan Junior Mathematical Olympiad 2016). A quadruple (p, a, b, c) of positive integers is called a *good quadruple* if

(a) p is odd prime,

(b) a, b, c are distinct,

(c) $ab + 1, bc + 1$, and $ca + 1$ are divisible by p.

Prove that for all good quadruple $p + 2 \leq \frac{a+b+c}{3}$, and show the equality case.

Problem 7.83 (Balkan 2016). Find all monic polynomials f with integer coefficients satisfying the following condition: there exists a positive integer N such that p divides $2(f(p)!) + 1$ for every prime $p > N$ for which $f(p)$ is a positive integer.
Note: A monic polynomial has a leading coefficient equal to 1.

Problem 7.84 (Bay Area Olympiad 2016). Let $A = 2^k - 2$ and $B = 2^k \cdot A$, where k is an integer ($k \geq 2$). Show that, for every integer k greater than or equal to 2,

1. A and B have the same set of distinct prime factors.

2. $A + 1$ and $B + 1$ have the same set of distinct prime factors.

Problem 7.85 (Bay Area Olympiad 2016). Find a positive integer N and $a_1, a_2, \cdots, a_N$ where $a_k = 1$ or $a_k = -1$, for each $k = 1, 2, \cdots, N$, such that

$$a_1 \cdot 1^3 + a_2 \cdot 2^3 + a_3 \cdot 3^3 \cdots + a_N \cdot N^3 = 20162016$$

or show that this is impossible.

Problem 7.86 (Belgium Flanders Math Olympiad Final Round 2016). Find the smallest positive integer n which does not divide 2016!.

Problem 7.87 (Belgium National Olympiad Final Round 2016). Solve the equation

$$2^{2m+1} + 9 \cdot 2^m + 5 = n^2$$

for integers m and n.

Problem 7.88 (Benelux 2016). Find the greatest positive integer N with the following property: there exist integers $x_1, \ldots, x_N$ such that $x_i^2 - x_i x_j$ is not divisible by 1111 for any $i \neq j$.

Problem 7.89 (Benelux 2016). Let n be a positive integer. Suppose that its positive divisors can be partitioned into pairs (i.e. can be split in groups of two) in such a way that the sum of each pair is a prime number. Prove that these prime numbers are distinct and that none of these are a divisor of n.

Problem 7.90 (Bosnia and Herzegovina TST 2016). For an infinite sequence $a_1 < a_2 < a_3 < \ldots$ of positive integers we say that it is nice if for every positive integer n holds $a_{2n} = 2a_n$. Prove the following statements:

(a) If there is given a nice sequence and prime number $p > a_1$, there exist some term of the sequence which is divisible by p.

(b) For every prime number $p > 2$, there exist a nice sequence such that no terms of the sequence are divisible by p.

Problem 7.91 (Bosnia and Herzegovina TST 2016). Determine the largest positive integer n which cannot be written as the sum of three numbers bigger than 1 which are pairwise relatively prime.

Problem 7.92 (Bulgaria National Olympiad 2016). Find all positive integers m and n such that $\left(2^{2^m}+1\right)\left(2^{2^n}+1\right)$ is divisible by mn.

Problem 7.93 (Bulgaria National Olympiad 2016). Determine whether there exists a positive integer $n < 10^9$ such that n can be expressed as a sum of three squares of positive integers by more than 1000 distinct ways.

Problem 7.94 (Canadian Mathematical Olympiad Qualification 2016).

(a) Find all positive integers n such that $11 \mid (3^n + 4^n)$.

(b) Find all positive integers n such that $31 \mid (4^n + 7^n + 20^n)$.

Problem 7.95 (Canadian Mathematical Olympiad Qualification 2016). Determine all ordered triples of positive integers (x, y, z) such that $\gcd(x+y, y+z, z+x) > \gcd(x, y, z)$.

Problem 7.96 (Canada National Olympiad 2016). Find all polynomials $P(x)$ with integer coefficients such that $P(P(n) + n)$ is a prime number for infinitely many integers n.

Problem 7.97 (CCA Math Bonanza 2016). Let $f(x) = x^2+x+1$. Determine the ordered pair (p, q) of primes satisfying $f(p) = f(q) + 242$.

Problem 7.98 (CCA Math Bonanza 2016). Let $f(x) = x^2+x+1$. Determine the ordered pair (p, q) of primes satisfying $f(p) = f(q) + 242$.

Problem 7.99 (CCA Math Bonanza 2016). Compute

$$\sum_{k=1}^{420} \gcd(k, 420)$$

Problem 7.100 (CCA Math Bonanza 2016). Pluses and minuses are inserted in the expression

$$\pm 1 \pm 2 \pm 3 \cdots \pm 2016$$

such that when evaluated the result is divisible by 2017. Let there be N ways for this to occur. Compute the remainder when N is divided by 503.

Problem 7.101 (CCA Math Bonanza 2016). What is the largest integer that must divide $n^5 - 5n^3 + 4n$ for all integers n?

Problem 7.102 (CCA Math Bonanza 2016). Determine the remainder when

$$2^6 \cdot 3^{10} \cdot 5^{12} - 75^4 \left(26^2 - 1\right)^2 + 3^{10} - 50^6 + 5^{12}$$

is divided by 1001.

Problem 7.103 (CentroAmerican 2016). Find all positive integers n that have 4 digits, all of them perfect squares, and such that n is divisible by 2, 3, 5, and 7.

Problem 7.104 (CentroAmerican 2016). We say a number is *irie* if it can be written in the form $1+\frac{1}{k}$ for some positive integer k. Prove that every integer $n \geq 2$ can be written as the product of r distinct irie numbers for every integer $r \geq n-1$.

Problem 7.105 (Chile 2016). Determine all triples of positive integers (p, n, m) with p a prime number, which satisfy the equation:

$$p^m - n^3 = 27$$

Problem 7.106 (Chile 2016[1]). Find all prime numbers that do not have a multiple ending in 2015.

Problem 7.107 (Chile 2016). Find the number of different numbers of the form $\lfloor \frac{i^2}{2015} \rfloor$, where $i = 1, 2, \ldots, 2015$.

Problem 7.108 (China Girls Mathematical Olympiad 2016). Let m and n are relatively prime integers and $m > 1, n > 1$. Show that there are positive integers a, b, c such that $m^a = 1 + n^b c$, and n and c are relatively prime.

Problem 7.109 (China National Olympiad 2016). Let p be an odd prime and $a_1, a_2, \ldots, a_p$ be integers. Prove that the following two conditions are equivalent:

1. There exists a polynomial $P(x)$ with degree $\leq \frac{p-1}{2}$ such that $P(i) \equiv a_i \pmod{p}$ for all $1 \leq i \leq p$.
2. For any natural $d \leq \frac{p-1}{2}$,

$$\sum_{i=1}^{p} (a_{i+d} - a_i)^2 \equiv 0 \pmod{p}$$

where indices are taken modulo p.

[1]Thanks to Kamal Kamrava and Behnam Sajadi for translating the problem.

Problem 7.110 (China South East Mathematical Olympiad 2016). Let n be a positive integer and let D_n be the set of all positive divisors of n. Define $f(n) = \sum_{d \in D_n} \frac{1}{1+d}$. Prove that for any positive integer m,

$$\sum_{i=1}^{m} f(i) < m$$

Problem 7.111 (China South East Mathematical Olympiad 2016). Let $\{a_n\}$ be a sequence consisting of positive integers such that $n^2 \mid \sum_{i=1}^{n} a_i$ and $a_n \leq (n+2016)^2$ for all $n \geq 2016$. Define $b_n = a_{n+1} - a_n$. Prove that the sequence $\{b_n\}$ is eventually constant.

Problem 7.112 (China South East Mathematical Olympiad 2016). Define the sets

$$A = \{a^3 + b^3 + c^3 - 3abc : a, b, c \in \mathbb{N}\}$$
$$B = \{(a+b-c)(b+c-a)(c+a-b) : a, b, c \in \mathbb{N}\}$$
$$P = \{n : n \in A \cap B, 1 \leq n \leq 2016\}$$

Find the number of elements of P.

Problem 7.113 (China TST2016). Let $c, d \geq 2$ be positive integers. Let $\{a_n\}$ be the sequence satisfying $a_1 = c, a_{n+1} = a_n^d + c$ for $n = 1, 2, \ldots$. Prove that for any $n \geq 2$, there exists a prime number p such that $p \mid a_n$ and $p \nmid a_i$ for $i = 1, 2, \ldots, n-1$.

Problem 7.114 (China TST 2016). Set positive integer $m = 2^k \cdot t$, where k is a non-negative integer, t is an odd number, and let $f(m) = t^{1-k}$. Prove that for any positive integer n and for any positive odd number $a \leq n$, $\prod_{m=1}^{n} f(m)$ is a multiple of a.

Problem 7.115 (China TST 2016). Does there exist two infinite positive integer sets S, T, such that any positive integer n can be uniquely expressed in the form

$$n = s_1 t_1 + s_2 t_2 + \ldots + s_k t_k$$

where k is a positive integer dependent on n, $s_1 < s_2 < \cdots < s_k$ are elements of S, $t_1, \ldots, t_k$ are elements of T?

Problem 7.116 (China TST 2016). Let a, b, b', c, m, q be positive integers, where $m > 1, q > 1, |b - b'| \geq a$. It is given that there exist a positive integer M such that

$$S_q(an + b) \equiv S_q(an + b') + c \pmod{m}$$

holds for all integers $n \geq M$. Prove that the above equation is true for all positive integers n. (Here $S_q(x)$ is the sum of digits of x taken in base q).

Problem 7.117 (China Western Mathematical Olympiad 2016). For an n-tuple of integers, define a transformation to be:

$$(a_1, a_2, \ldots, a_{n-1}, a_n) \to (a_1 + a_2, a_2 + a_3, \ldots, a_{n-1} + a_n, a_n + a_1)$$

Find all ordered pairs of integers (n, k) with $n, k \geq 2$, such that for any n-tuple of integers $(a_1, a_2, \ldots, a_{n-1}, a_n)$, after a finite number of transformations, every element in the of the n-tuple is a multiple of k.

Problem 7.118 (China Western Mathematical Olympiad 2016). Prove that there exist infinitely many positive integer triples (a, b, c) such that a, b, c are pairwise relatively prime ,and $ab + c, bc + a, ca + b$ are pairwise relatively prime.

Problem 7.119 (Croatia First Round Competition 2016). Can the sum of squares of three consecutive integers be divisible by 2016?

Problem 7.120 (Croatia First Round Competition 2016). Let $a = 123456789$ and $N = a^3 - 2a^2 - 3a$. Prove that N is a multiple of 540.

Problem 7.121 (Croatia First Round Competition 2016). Find all pairs (a, b) of positive integers such that $1 < a, b \leq 100$ and

$$\frac{1}{\log_a 10} + \frac{1}{\log_b 10}$$

is a positive integer.

Problem 7.122 (Croatia First Round Competition 2016). A sequence (a_n) is given: $a_1 = a_2 = 1$, and

$$a_{n+1} = \frac{a_2^2}{a_1} + \frac{a_3^2}{a_2} + \cdots + \frac{a_n^2}{a_{n-1}}$$

for $n \geq 2$. Find a_{2016}.

Problem 7.123 (Croatia First Round Competition 2016). Let a, b, and c be integers. If $4a + 5b - 3c$ is divisible by 19, prove that $6a - 2b + 5c$ is also divisible by 19.

Problem 7.124 (Croatia First Round Competition 2016). Determine all pairs of positive integers (x, y) such that $x^2 - y! = 2016$.

Problem 7.125 (Croatia Second Round Competition 2016).

(a) Prove that there are no two positive integers such that the difference of their squares is 987654.

(b) Prove that there are no two positive integers such that the difference of their cubes is 987654.

Problem 7.126 (Croatia Second Round Competition 2016). How many ordered pairs (m, k) of positive integers satisfy the following?

$$20m = k(m - 15k)$$

Problem 7.127 (Croatia Second Round Competition 2016). Determine all pairs (a, b) of positive integers such that

$$a^3 - 3b = 15$$
$$b^2 - a = 13$$

Problem 7.128 (Croatia Second Round Competition 2016). Prove that, for every positive integer $n > 3$, there are n different positive integers whose reciprocals add up to 1.

Problem 7.129 (Croatia Second Round Competition 2016). Determine all pairs (a, b) of integers such that $(7a - b)^2 = 2(a-1)b^2$.

Problem 7.130 (Croatia Final Round National Competition 2016). Determine the sum

$$\frac{2^2+1}{2^2-1} + \frac{3^2+1}{3^2-1} + \cdots + \frac{100^2+1}{100^2-1}$$

Problem 7.131 (Croatia Final Round National Competition 2016). Let a, b, and c be positive integers such that

$$c = a + \frac{b}{a} - \frac{1}{b}$$

Prove that c is the square of an integer.

Problem 7.132 (Croatia Final Round National Competition 2016). Determine all pairs (m, n) of positive integers for which exist integers a, b, and c that satisfy

$$a + b + c = 0$$
$$a^2 + b^2 + c^2 = 2^m \cdot 3^n$$

Problem 7.133 (Croatia Final Round National Competition 2016). Prove that there does not exist a positive integer k such that $k + 4$ and $k^2 + 5k + 2$ are cubes of positive integers.

Problem 7.134 (Croatia Final Round National Competition 2016). Determine all triples (m, n, k) of positive integers such that $3^m + 7^n = k^2$.

Problem 7.135 (Croatian Mathematical Olympiad 2016). Find all pairs (p, q) of prime numbers such that

$$p(p^2 - p - 1) = q(2q + 3)$$

Problem 7.136 (Croatian TST for MEMO 2016, Sweden 2014). Find all pairs (m, n) of positive integers such that

$$3 \cdot 5^m - 2 \cdot 6^n = 3$$

Problem 7.137 (Croatia IMO TST 2016). Prove that for every positive integer n there exist integers a and b such that n divides $4a^2 + 9b^2 - 1$.

Problem 7.138 (Croatia IMO TST 2016, Bulgaria TST 2016). Let $p > 10^9$ be a prime number such that $4p+1$ is also prime. Prove that the decimal expansion of $\frac{1}{4p+1}$ contains all the digits $0, 1, \ldots, 9$.

Problem 7.139 (Denmark Georg Mohr Contest Second Round 2016). Find all possible values of the number

$$\frac{a+b}{c}+\frac{a+c}{b}+\frac{b+c}{a}$$

where a, b, and c are positive integers, and $\frac{a+b}{c}$, $\frac{a+c}{b}$, and $\frac{b+c}{a}$ are also positive integers.

Problem 7.140 (ELMO 2016). Cookie Monster says a positive integer n is *crunchy* if there exist $2n$ real numbers $x_1, x_2, \ldots, x_{2n}$, not all equal, such that the sum of any n of the x_i's is equal to the product of the other n of the x_i's. Help Cookie Monster determine all crunchy integers.

Problem 7.141 (ELMO 2016). Big Bird has a polynomial P with integer coefficients such that n divides $P(2^n)$ for every positive integer n. Prove that Big Bird's polynomial must be the zero polynomial.

Problem 7.142 (Estonia IMO TST First Stage 2016). Let p be a prime. Find all integers (not necessarily positive) a, b, and c such that

$$a^b b^c c^a = p$$

Problem 7.143 (Estonia IMO TST First Stage 2016). Prove that for every positive integer $n \geq 3$,

$$2 \cdot \sqrt{3} \cdot \sqrt[3]{4} \ldots \sqrt[n-1]{n} > n$$

Problem 7.144 (Estonia IMO TST Second Stage 2016). Find all positive integers n such that

$$(n^2+11n-4) \cdot n! + 33 \cdot 13^n + 4$$

is a perfect square.

Problem 7.145 (Estonia National Olympiad Tenth Grade 2016). Find all pairs of integers (a, b) which satisfy

$$3(a^2+b^2) - 7(a+b) = -4$$

Problem 7.146 (Estonia National Olympiad Eleventh Grade 2016). Find the greatest positive integer n for which $3^{2016} - 1$ is divisible by 2^n.

Problem 7.147 (Estonia National Olympiad Eleventh Grade 2016). Let n be a positive integer. Let $\delta(n)$ be the number of positive divisors of n and let $\sigma(n)$ be their sum. Prove that

$$\sigma(n) > \frac{(\delta(n))^2}{2}$$

Problem 7.148 (Estonia Regional Olympiad Tenth Grade 2016). Does the equation

$$x^2+y^2+z^2+w^2 = 3+xy+yz+zw$$

has a solution in which x, y, z, and w are different integers?

Problem 7.149 (Estonia Regional Olympiad Twelfth Grade 2016). Determine whether the logarithm of 6 in base 10 is larger or smaller than $\frac{7}{9}$.

Problem 7.150 (Estonia Regional Olympiad Twelfth Grade 2016). Find the largest positive integer n so that one can select n primes $p_1, p_2, \dots, p_n$ (not necessarily distinct) such that

$$p_1, p_1 + p_2, \dots, p_1 + p_2 + \cdots + p_n$$

are all primes.

Problem 7.151 (European Girls' Mathematical Olympiad 2016). Let S be the set of all positive integers n such that n^4 has a divisor in the range $n^2 + 1, n^2 + 2, \dots, n^2 + 2n$. Prove that there are infinitely many elements of S of each of the forms $7m, 7m+1, 7m+2, 7m+5, 7m+6$ and no elements of S of the form $7m+3$ and $7m+4$, where m is an integer.

Problem 7.152 (European Mathematical Cup Seniors 2016). $A = \{a, b, c\}$ is a set containing three positive integers. Prove that we can find a set $B \subset A$, say $B = \{x, y\}$, such that for all odd positive integers m and n,

$$10 \mid x^m y^n - x^n y^m$$

Problem 7.153 (European Mathematical Cup Juniors 2016). Let $d(n)$ denote the number of positive divisors of n. For a positive integer n we define $f(n)$ as

$$f(n) = d(k_1) + d(k_2) + \cdots + d(k_m)$$

where $1 = k_1 < k_2 < \cdots < k_m = n$ are all divisors of the number n. We call an integer $n > 1$ *almost perfect* if $f(n) = n$. Find all almos perfect numbers.

Problem 7.154 (Finland MAOL Competition 2016). Let n be a positive integer. Find all pairs (x, y) of positive integers such that

$$(4a - b)(4b - a) = 1770^n$$

Problem 7.155 (Germany National Olympiad First Round Ninth/Tenth Grade, 2016).

(A) Prove that there exists an integer $a > 1$ such that the number

$$82 \cdot (a^8 - a^4)$$

is divisible by the product of three consecutive positive integers each of which has at least two digits.

(B) Determine the smallest prime number a with at least two digits such that the number

$$82 \cdot (a^8 - a^4)$$

is divisible by the product of three consecutive positive integers each of which has at least two digits.

(C) Determine the smallest integer $a > 1$ such that the number

$$82 \cdot (a^8 - a^2)$$

is divisible by the product of three consecutive positive integers each of which has at least two digits.

Problem 7.156 (Germany National Olympiad First Round Eleventh/Twelfth Grade, 2016). Consider the following system of equations:

$$\begin{aligned} 2(z-1) - x &= 55 \\ 4xy - 8z &= 12 \\ a(y+z) &= 11 \end{aligned}$$

Find two largest real values for a for which there are positive integers x, y, and z that satisfy the system of equations. In each of these solutions, determine xyz.

Problem 7.157 (Germany National Olympiad First Round Eleventh/Twelfth Grade, 2016). Find all pairs (a, b) of positive integers for which $(a+1)(b+1)$ is divisible by ab.

Problem 7.158 (Germany National Olympiad Second Round Tenth Grade, 2016). For each of the following cases, determine whether there exist prime numbers x, y, and z such that the given equality holds

(a) $y = z^2 - x^2$.

(b) $x^2 + y = z^4$.

(c) $x^2 + y^3 = z^4$.

Problem 7.159 (Germany National Olympiad Second Round Eleventh/Twelfth Grade, 2016). The sequence $x_1, x_2, x_3, \ldots$ is defined as $x_1 = 1$ and

$$x_{k+1} = x_k + y_k$$

where y_k is the last digit of decimal representation of x_k. Prove that the sequence $x_1, x_2, x_3, \ldots$ contains all powers of 4. That is, for every positive integer n, there exists some natural k for which $x_k = 4^n$.

Problem 7.160 (Germany National Olympiad Third Round Eleventh/Twelfth Grade, 2016). Find all positive integers a and b which satisfy

$$\binom{ab+1}{2} = 2ab(a+b)$$

Problem 7.161 (Germany National Olympiad Third Round Eleventh/Twelfth Grade, 2016). Let m and n be two positive integers. Prove that for every positive integer k, the following statements are equivalent:

1. $n + m$ is a divisor of $n^2 + km^2$.

2. $n+m$ is a divisor of $k+1$.

Problem 7.162 (Germany National Olympiad Fourth Round Ninth Grade, 2016). Find all triples (a,b,c) of integers which satisfy

$$\begin{aligned} a^3+b^3 &= c^3+1 \\ b^2-a^2 &= a+b \\ 2a^3-6a &= c^3-4a^2 \end{aligned}$$

Problem 7.163 (Germany National Olympiad Fourth Round Tenth Grade, 2016[2]). A sequence of positive integers $a_1, a_2, a_3, \ldots$ is defined as follows: a_1 is a 3 digit number and a_{k+1} (for $k \geq 1$) is obtained by

$$a_{k+1} = a_k + 2 \cdot Q(a_k)$$

where $Q(a_k)$ is the sum of digits of a_k when represented in decimal system. For instance, if one takes $a_1 = 358$ as the initial term, the sequence would be

$$\begin{aligned} a_1 &= 358, \\ a_2 &= 358 + 2 \cdot 16 = 390 \\ a_3 &= 390 + 2 \cdot 12 = 414 \\ a_4 &= 414 + 2 \cdot 9 = 432 \\ &\vdots \end{aligned}$$

Prove that no matter what we choose as the starting number of the sequence,

(a) the sequence will not contain 2015.

(b) the sequence will not contain 2016.

Problem 7.164 (Germany National Olympiad Fourth Round Eleventh Grade, 2016). Find all positive integers m and n with $m \leq 2n$ which satisfy

$$m \cdot \binom{2n}{n} = \binom{m^2}{2}$$

Problem 7.165 (Germany TST 2016). The positive integers $a_1, a_2, \ldots, a_n$ are aligned clockwise in a circular line with $n \geq 5$. Let $a_0 = a_n$ and $a_{n+1} = a_1$. For each $i \in \{1, 2, \ldots, n\}$ the quotient

$$q_i = \frac{a_{i-1} + a_{i+1}}{a_1}$$

is an integer. Prove that

$$\begin{aligned} 2n &\leq q_1 + q_2 + \cdots + q_n \\ &< 3n \end{aligned}$$

[2]Thanks to Arian Saffarzadeh for translating the problem.

Problem 7.166 (Germany TST 2016, Taiwan TST First Round 2016). Determine all positive integers M such that the sequence $a_0, a_1, a_2, \cdots$ defined by

$$\begin{aligned} a_0 &= M + \frac{1}{2} \\ a_{k+1} &= a_k \lfloor a_k \rfloor \\ &\vdots \end{aligned}$$

contains at least one integer term.

Problem 7.167 (Greece 2016). Find all triplets of non-negative integers (x, y, z) and $x \leq y$ such that

$$x^2 + y^2 = 3 \cdot 2016^z + 77$$

Problem 7.168 (Greece TST 2016). Given is the sequence $(a_n)_{n \geq 0}$ which is defined as follows:$a_0 = 3$ and $a_{n+1} - a_n = n(a_n - 1)$, $\forall n \geq 0$. Determine all positive integers m such that $\gcd(m, a_n) = 1$ for all $n \geq 0$.

Problem 7.169 (Harvard-MIT Math Tournament 2016). Denote by $\mathbb{N}$ the positive integers. Let $f : \mathbb{N} \to \mathbb{N}$ be a function such that, for any $w, x, y, z \in \mathbb{N}$,

$$f(f(f(z)))f(wxf(yf(z))) = z^2 f(xf(y))f(w)$$

Show that $f(n!) \geq n!$ for every positive integer n.

Problem 7.170 (Hong Kong (China) Mathematical Olympiad 2016). Find all integral ordered triples (x, y, z) such that

$$\sqrt{\frac{2015}{x+y}} + \sqrt{\frac{2015}{y+z}} + \sqrt{\frac{2015}{x+z}}$$

are positive integers.

Problem 7.171 (Hong Kong Preliminary Selection Contest 2016). Find the remainder when

$$19^{17^{15^{\cdot^{\cdot^{\cdot^{3^1}}}}}}$$

is divided by 100.

Problem 7.172 (Hong Kong Preliminary Selection Contest 2016). Let k be an integer. If the equation

$$kx^2 + (4k-2)x + (4k-7) = 0$$

has an integral root, find the sum of all possible values of k.

Problem 7.173 (Hong Kong Preliminary Selection Contest 2016). Let n be a positive integer. If the two numbers $(n+1)(2n+15)$ and $n(n+5)$ have exactly the same prime factors, find the greatest possible value of n.

Problem 7.174 (Hong Kong Preliminary Selection Contest 2016). An arithmetic sequence with 10 terms has common difference $d > 0$. If the absolute value of each term is a prime number, find the smallest possible value of d.

Problem 7.175 (Hong Kong Preliminary Selection Contest 2016). Let $a_1 = \frac{2}{3}$ and

$$a_{n+1} = \frac{a_n}{4} + \sqrt{\frac{24a_n + 9}{256}} - \frac{9}{48}$$

for all integers $n \geq 1$. Find the value of

$$a_1 + a_2 + a_3 + \ldots$$

Problem 7.176 (Hong Kong TST 2016). Find all natural numbers n such that n, n^2+10, $n^2 - 2, n^3 + 6$, and $n^5 + 36$ are all prime numbers.

Problem 7.177 (Hong Kong TST 2016). Find all triples (m, p, q) such that

$$2^m p^2 + 1 = q^7$$

where p and q are primes and m is a positive integer.

Problem 7.178 (Hong Kong TST 2016). Find all prime numbers p and q such that $p^2 \mid q^3 + 1$ and $q^2 \mid p^6 - 1$.

Problem 7.179 (Hong Kong TST 2016). Let p be a prime number greater than 5. Suppose there is an integer k satisfying that $k^2 + 5$ is divisible by p. Prove that there are positive integers m and n such that $p^2 = m^2 + 5n^2$.

Problem 7.180 (IberoAmerican 2016). Find all prime numbers p, q, r, k such that $pq + qr + rp = 12k + 1$.

Problem 7.181 (IberoAmerican 2016). Let k be a positive integer and $a_1, a_2, \ldots, a_k$ digits. Prove that there exists a positive integer n such that the last $2k$ digits of 2^n are, in the following order, $a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_k$, for certain digits $b_1, b_2, \ldots, b_k$.

Problem 7.182 (IMO Shortlist 2015, India TST 2016, Taiwan TST Second Round 2016, Croatian Mathematical Olympiad 2016, Switzerland TST 2016). Let m and n be positive integers such that $m > n$. Define

$$x_k = \frac{m + k}{n + k}$$

for $k = 1, 2, \ldots, n + 1$. Prove that if all the numbers $x_1, x_2, \ldots, x_{n+1}$ are integers, then $x_1 x_2 \ldots x_{n+1} - 1$ is divisible by an odd prime.

Problem 7.183 (IMO 2016). A set of postive integers is called fragrant if it contains at least two elements and each of its elements has a prime factor in common with at least one of the other elements. Let $P(n) = n^2 + n + 1$. What is the least possible positive integer value of b such that there exists a non-negative integer a for which the set

$$\{P(a + 1), P(a + 2), \ldots, P(a + b)\}$$

is fragrant?

Problem 7.184 (India IMO Training Camp 2016). Given that n is a natural number such that the leftmost digits in the decimal representations of 2^n and 3^n are the same, find all possible values of the leftmost digit.

Problem 7.185 (India IMO Practice Test 2016). We say a natural number n is perfect if the sum of all the positive divisors of n is equal to $2n$. For example, 6 is perfect since its positive divisors $1, 2, 3, 6$ add up to $12 = 2 \times 6$. Show that an odd perfect number has at least 3 distinct prime divisors.

Problem 7.186 (India TST 2016). Let n be a natural number. We define sequences $\langle a_i \rangle$ and $\langle b_i \rangle$ of integers as follows. We let $a_0 = 1$ and $b_0 = n$. For $i > 0$, we let

$$(a_i, b_i) = \begin{cases} (2a_{i-1} + 1, b_{i-1} - a_{i-1} - 1) & \text{if } a_{i-1} < b_{i-1} \\ (a_{i-1} - b_{i-1} - 1, 2b_{i-1} + 1) & \text{if } a_{i-1} > b_{i-1} \\ (a_{i-1}, b_{i-1}) & \text{if } a_{i-1} = b_{i-1} \end{cases}$$

Given that $a_k = b_k$ for some natural number k, prove that $n + 3$ is a power of two.

Problem 7.187 (India TST 2016). Let $\mathbb{N}$ denote the set of all natural numbers. Show that there exists two nonempty subsets A and B of $\mathbb{N}$ such that

1. $A \cap B = \{1\}$;
2. every number in $\mathbb{N}$ can be expressed as the product of a number in A and a number in B;
3. each prime number is a divisor of some number in A and also some number in B;
4. one of the sets A and B has the following property: if the numbers in this set are written as $x_1 < x_2 < x_3 < \cdots$, then for any given positive integer M there exists $k \in \mathbb{N}$ such that $x_{k+1} - x_k \geq M$;
5. Each set has infinitely many composite numbers.

Problem 7.188 (India National Olympiad 2016). Let $\mathbb{N}$ denote the set of natural numbers. Define a function $T : \mathbb{N} \to \mathbb{N}$ by $T(2k) = k$ and $T(2k + 1) = 2k + 2$. We write $T^2(n) = T(T(n))$ and in general $T^k(n) = T^{k-1}(T(n))$ for any $k > 1$.

(i) Show that for each $n \in \mathbb{N}$, there exists k such that $T^k(n) = 1$.

(ii) For $k \in \mathbb{N}$, let c_k denote the number of elements in the set $\{n : T^k(n) = 1\}$. Prove that $c_{k+2} = c_{k+1} + c_k$, for $k \geq 1$.

Problem 7.189 (India National Olympiad 2016). Consider a non-constant arithmetic progression $a_1, a_2, \cdots, a_n, \cdots$. Suppose there exist relatively prime positive integers $p > 1$ and $q > 1$ such that a_1^2, a_{p+1}^2 and a_{q+1}^2 are also the terms of the same arithmetic progression. Prove that the terms of the arithmetic progression are all integers.

Problem 7.190 (Iran Third Round National Olympiad 2016). Let F be a subset of the set of positive integers with at least two elements and P be a polynomial with integer coefficients such that for any two elements of F like a and b, the following two conditions hold

(i) $a+b \in F$, and

(ii) $\gcd(P(a), P(b)) = 1$.

Prove that $P(x)$ is a constant polynomial.

Problem 7.191 (Iran Third Round National Olympiad 2016). Let P be a polynomial with integer coefficients. We say P is *good* if there exist infinitely many prime numbers q such that the set

$$X = \{P(n) \mod q : \quad n \in \mathbb{N}\}$$

has at least $\frac{q+1}{2}$ members. Prove that the polynomial $x^3 + x$ is good.

Problem 7.192 (Iran Third Round National Olympiad 2016). Let m be a positive integer. The positive integer a is called a *golden residue* modulo m if $\gcd(a, m) = 1$ and $x^x \equiv a \pmod{m}$ has a solution for x. Given a positive integer n, suppose that a is a golden residue modulo n^n. Show that a is also a golden residue modulo n^{n^n}.

Problem 7.193 (Iran Third Round National Olympiad 2016). Let p, q be prime numbers (q is odd). Prove that there exists an integer x such that

$$q \mid (x+1)^p - x^p$$

if and only if

$$q \equiv 1 \pmod{p}$$

Problem 7.194 (Iran Third Round National Olympiad 2016). We call a function g *special* if $g(x) = a^{f(x)}$ (for all x) where a is a positive integer and f is polynomial with integer coefficients such that $f(n) > 0$ for all positive integers n.

A function is called an *exponential polynomial* if it is obtained from the product or sum of special functions. For instance, $2^x 3^{x^2+x-1} + 5^{2x}$ is an exponential polynomial.

Prove that there does not exist a non-zero exponential polynomial $f(x)$ and a non-constant polynomial $P(x)$ with integer coefficients such that

$$P(n) \mid f(n)$$

for all positive integers n.

Problem 7.195 (Iran Third Round National Olympiad 2016). A sequence $P = \{a_n\}_{n=1}^{\infty}$ is called a *permutation* of natural numbers if for any natural number m, there exists a unique natural number n such that $a_n = m$.

We also define $S_k(P)$ as $S_k(P) = a_1 + a_2 + \cdots + a_k$ (the sum of the first k elements of the sequence).

Prove that there exists infinitely many distinct permutations of natural numbers like $P_1, P_2, \ldots$ such that for all k and $i < j$,

$$S_k(P_i) \mid S_k(P_j)$$

Problem 7.196 (Iran TST 2016). Let $p \neq 13$ be a prime number of the form $8k+5$ such that 39 is a quadratic non-residue modulo p. Prove that the equation

$$x_1^4 + x_2^4 + x_3^4 + x_4^4 \equiv 0 \pmod{p}$$

has a solution in integers such that $p \nmid x_1x_2x_3x_4$.

Problem 7.197 (Italy National Olympiad 2016). Determine all pairs of positive integers (a, n) with $a \geq n \geq 2$ for which $(a+1)^n + a - 1$ is a power of 2.

Problem 7.198 (Japan Mathematical Olympiad Preliminary 2016). For $1 \leq n \leq 2016$, how many integers n satisfying the condition: the reminder divided by 20 is smaller than the one divided by 16.

Problem 7.199 (Japan Mathematical Olympiad Preliminary 2016). Determine the number of pairs (a, b) of integers such that $1 \leq a, b \leq 2015$, a is divisible by $b+1$, and $2016-a$ is divisible by b.

Problem 7.200 (Japan Mathematical Olympiad Finals 2016). Let p be an odd prime number. For positive integer k satisfying $1 \leq k \leq p-1$, the number of divisors of $kp+1$ between k and p exclusive is a_k. Find the value of $a_1 + a_2 + \ldots + a_{p-1}$.

Problem 7.201 (Junior Balkan Mathematical Olympiad 2016). Find all triplets of integers (a, b, c) such that the number

$$N = \frac{(a-b)(b-c)(c-a)}{2} + 2$$

is a power of 2016.

Problem 7.202 (Korea Summer Program Practice Test 2016). A infinite sequence $\{a_n\}_{n\geq 0}$ of real numbers satisfy $a_n \geq n^2$. Suppose that for each $i, j \geq 0$ there exist k, l with $(i, j) \neq (k, l), l-k = j-i$, and $a_l - a_k = a_j - a_i$. Prove that $a_n \geq (n+2016)^2$ for some n.

Problem 7.203 (Korea Summer Program Practice Test 2016). A finite set S of positive integers is given. Show that there is a positive integer N dependent only on S, such that any $x_1, \ldots, x_m \in S$ whose sum is a multiple of N, can be partitioned into groups each of whose sum is exactly N. (The numbers $x_1, \ldots, x_m$ need not be distinct.)

Problem 7.204 (Korea Winter Program Practice Test 2016). $p(x)$ is an irreducible polynomial with integer coefficients, and q is a fixed prime number. Let a_n be a number of solutions of the equation $p(x) \equiv 0 \mod q^n$. Prove that we can find M such that $\{a_n\}_{n\geq M}$ is constant.

Problem 7.205 (Korea Winter Program Practice Test 2016). Find all $\{a_n\}_{n\geq 0}$ that satisfies the following conditions.

1. $a_n \in \mathbb{Z}$,
2. $a_0 = 0, a_1 = 1$,

3. For infinitely many m, $a_m = m$, and
4. For every $n \geq 2$,

$$\{2a_i - a_{i-1} | i = 1, 2, 3, \cdots, n\} \equiv \{0, 1, 2, \cdots, n-1\} \pmod{n}$$

Problem 7.206 (Korea Winter Program Practice Test 2016). Find all positive integers a, b, m, and n such that

$$a^2 + b^2 = m^2 - n^2$$
$$ab = 2mn$$

Problem 7.207 (Korea Winter Program Practice Test 2016). Find all pairs of positive integers (n, t) such that $6^n + 1 = n^2 t$, and $(n, 29 \times 197) = 1$.

Problem 7.208 (Korea National Olympiad Final Round 2016). Prove that for all rationals x, y, $x - \frac{1}{x} + y - \frac{1}{y} = 4$ is not true.

Problem 7.209 (Kosovo TST 2016). Show that for any $n \geq 2$, the number $2^{2^n} + 1$ ends with 7.

Problem 7.210 (Latvia National Olympiad 2016).

1. Given positive integers x and y such that xy^2 is a perfect cube, prove that $x^2 y$ is also a perfect cube.
2. Given that x and y are positive integers such that xy^{10} is perfect 33rd power of a positive integer, prove that $x^{10} y$ is also a perfect 33rd power.
3. Given that x and y are positive integers such that xy^{433} is a perfect 2016-power of a positive integer, prove that $x^{433} y$ is also a perfect 2016-power.
4. Given that x, y and z are positive integers such that $x^3 y^5 z^6$ is a perfect 7th power of a positive integer, show that also $x^5 y^6 z^3$ is a perfect 7th power.

Problem 7.211 (Latvia National Olympiad 2016). Prove that among any 18 consecutive positive 3 digit numbers, there is at least one that is divisible by the sum of its digits.

Problem 7.212 (Latvia National Olympiad 2016). Two functions are defined by equations: $f(a) = a^2 + 3a + 2$ and $g(b, c) = b^2 - b + 3c^2 + 3c$. Prove that for any positive integer a there exist positive integers b and c such that $f(a) = g(b, c)$.

Problem 7.213 (Macedonian National Olympiad 2016). Solve the equation in the set of natural numbers $1 + x^z + y^z = \text{lcm}(x^z, y^z)$.

Problem 7.214 (Macedonian National Olympiad 2016). Solve the equation in the set of natural numbers $xyz + yzt + xzt + xyt = xyzt + 3$.

Problem 7.215 (Macedonian Junior Mathematical Olympiad 2016). Solve the equation

$$x_1^4 + x_2^4 + \cdots + x_{14}^4 = 2016^3 - 1$$

in the set of integers.

Problem 7.216 (Macedonian Junior Mathematical Olympiad 2016). Solve the equation

$$x + y^2 + (\gcd(x,y))^2 = xy \cdot \gcd(x,y)$$

in the set of positive integers.

Problem 7.217 (Mediterranean Mathematics Olympiad 2016). Determine all integers $n \geq 1$ for which the number $n^8 + n^6 + n^4 + 4$ is prime.

Problem 7.218 (Middle European Mathematical Olympiad 2016). Find all $f : \mathbb{N} \to \mathbb{N}$ such that $f(a) + f(b)$ divides $2(a + b - 1)$ for all $a, b \in \mathbb{N}$.

Problem 7.219 (Middle European Mathematical Olympiad 2016). A positive integer n is Mozart if the decimal representation of the sequence $1, 2, \ldots, n$ contains each digit an even number of times. Prove that:

1. All Mozart numbers are even.
2. There are infinitely many Mozart numbers.

Problem 7.220 (Middle European Mathematical Olympiad 2016). For a positive integer n, the equation $a^2 + b^2 + c^2 + n = abc$ is given in the positive integers. Prove that:

1. There does not exist a solution (a, b, c) for $n = 2017$.
2. For $n = 2016$, a is divisible by 3 for all solutions (a, b, c).
3. There are infinitely many solutions (a, b, c) for $n = 2016$.

Problem 7.221 (Netherlands TST 2016). Find all positive integers k for which the equation:

$$\operatorname{lcm}(m,n) - \gcd(m,n) = k(m-n)$$

has no solution in integers positive (m, n) with $m \neq n$.

Problem 7.222 (Nordic Mathematical Competition 2016). Determine all sequences $(a_n)_{n=1}^{2016}$ of non-negative integers such that all sequence elements are less than or equal to 2016 and

$$i + j \mid ia_i + ja_j$$

for all $i, j \in \{1, 2, \ldots, 2016\}$.

Problem 7.223 (Norway Niels Henrik Abel Mathematics Competition Final Round 2016).

(a) Find all positive integers a, b, c, and d with $a \leq b$ and $c \leq d$ such that

$$a + b = cd$$
$$c + d = ab$$

(b) Find all non-negative integers x, y, and z such that

$$x^3 + 2y^3 + 4z^3 = 9!$$

Problem 7.224 (Pan-African Mathematical Olympiad 2016). For any positive integer n, we define the integer $P(n)$ by

$$P(n) = n(n+1)(2n+1)(3n+1)\ldots(16n+1)$$

Find the greatest common divisor of the integers $P(1), P(2), P(3), \ldots, P(2016)$.

Problem 7.225 (Philippine Mathematical Olympiad Area Stage 2016). Let a, b, and c be three consecutive even numbers such that $a > b > c$. What is the value of $a^2 + b^2 + c^2 - ab - bc - ac$?

Problem 7.226 (Philippine Mathematical Olympiad Area Stage 2016). Find the sum of all the prime factors of 27,000,001.

Problem 7.227 (Philippine Mathematical Olympiad Area Stage 2016). Find the largest number N so that

$$\sum_{n=5}^{N} \frac{1}{n(n-2)} < \frac{1}{4}$$

Problem 7.228 (Philippine Mathematical Olympiad Area Stage 2016). Let s_n be the sum of the digits of a natural number n. Find the smallest value of $\frac{n}{s_n}$ if n is a four-digit number.

Problem 7.229 (Philippine Mathematical Olympiad Area Stage 2016). The 6 digit number $\overline{739ABC}$ is divisible by 7, 8, and 9. What values can A, B, and C take?

Problem 7.230 (Polish Mathematical Olympiad 2016). Let p be a certain prime number. Find all non-negative integers n for which polynomial $P(x) = x^4 - 2(n+p)x^2 + (n-p)^2$ may be rewritten as product of two quadratic polynomials $P_1,\ P_2 \in \mathbb{Z}[X]$.

Problem 7.231 (Polish Mathematical Olympiad 2016). Let k, n be odd positive integers greater than 1. Prove that if there a exists natural number a such that $k \mid 2^a + 1,\ n \mid 2^a - 1$, then there is no natural number b satisfying $k \mid 2^b - 1,\ n \mid 2^b + 1$.

Problem 7.232 (Polish Mathematical Olympiad 2016). There are given two positive real number $a < b$. Show that there exist positive integers $p,\ q,\ r,\ s$ satisfying following conditions:

1. $a < \frac{p}{q} < \frac{r}{s} < b$.

2. $p^2+q^2=r^2+s^2$.

Problem 7.233 (Romania Danube Mathematical Competition 2016). Determine all positive integers n such that all positive integers less than or equal to n and prime to n are pairwise relatively prime.

Problem 7.234 (Romania Danube Mathematical Competition 2016). Given an integer $n \geq 2$, determine the numbers that can be written in the form

$$\sum_{i=2}^{k} a_{i-1}a_i$$

where k is an integer greater than or equal to 2, and $a_1, a_2, \ldots, a_k$ are positive integers that add up to n.

Problem 7.235 (Romania Imar Mathematical Competition 2016). Determine all positive integers expressible, for every integer $n \geq 3$, in the form

$$\frac{(a_1+1)(a_2+1)\ldots(a_n+1)-1}{a_1a_2\ldots a_n}$$

where $a_1, a_2, \ldots, a_n$ are pairwise distinct positive integers.

Problem 7.236 (Romanian Masters in Mathematics 2016). A *cubic sequence* is a sequence of integers given by $a_n = n^3+bn^2+cn+d$, where b, c and d are integer constants and n ranges over all integers, including negative integers.

(a) Show that there exists a cubic sequence such that the only terms of the sequence which are squares of integers are a_{2015} and a_{2016}.

(b) Determine the possible values of $a_{2015} \cdot a_{2016}$ for a cubic sequence satisfying the condition in part (a).

Problem 7.237 (Romanian Mathematical Olympiad District Round Grade 5, 2016). Find all three-digit numbers which decrease 13 times when the tens' digit is suppressed.

Problem 7.238 (Romanian Mathematical Olympiad District Round Grade 5, 2016). If A and B are positive integers, then $\overline{AB}$ will denote the number obtained by writing, in order, the digits of B after the digits of A. For instance, if $A = 193$ and $B = 2016$, then $\overline{AB} = 1932016$. Prove that there are infinitely many perfect squares of the form $\overline{AB}$ in each of the following situations:

(a) A and B are perfect squares;

(b) A and B are perfect cubes;

(c) A is a perfect cube and B is a perfect square;

(d) A is a perfect square and B is a perfect cube.

Problem 7.239 (Romanian Mathematical Olympiad District Round Grade 6, 2016). The positive integers m and n are such that $m^{2016} + m + n^2$ is divisible by mn.

(a) Give an example of such m and n, with $m > n$.

(b) Prove that m is a perfect square.

Problem 7.240 (Romanian Mathematical Olympiad District Round Grade 7, 2016). Find all pairs of positive integers (x, y) such that

$$x + y = \sqrt{x} + \sqrt{y} + \sqrt{xy}$$

Problem 7.241 (Romanian Mathematical Olympiad District Round Grade 7, 2016). Let

$$M = \{x_1 + 2x_2 + 3x_3 + \cdots + 2015x_{2015} : x_1, x_2, \ldots, x_{2015} \in \{-2, 3\}\}$$

Prove that $2015 \in M$ but $2016 \notin M$.

Problem 7.242 (Romanian Mathematical Olympiad District Round Grade 8, 2016). For each positive integer n denote x_n the number of the positive integers with n digits, divisible by 4, formed with digits $2, 0, 1$, or 6.

(a) Compute x_1, x_2, x_3, and x_4;

(b) Find n so that

$$1 + \left\lfloor \frac{x_2}{x_1} \right\rfloor + \left\lfloor \frac{x_3}{x_2} \right\rfloor + \cdots + \left\lfloor \frac{x_{n+1}}{x_n} \right\rfloor = 2016$$

Problem 7.243 (Romanian Mathematical Olympiad District Round Grade 8, 2016).

(a) Prove that, for every integer k, the equation $x^3 - 24x + k = 0$ has at most one integer solution.

(b) Prove that the equation $x^3 + 24x - 2016 = 0$ has exactly one integer solution.

Problem 7.244 (Romanian Mathematical Olympiad District Round Grade 9, 2016). Let a and n be positive integers such that

$$\left\{\sqrt{n + \sqrt{n}}\right\} = \{\sqrt{a}\}$$

where $\{\cdot\}$ denotes the fractional part. Prove that $4a + 1$ is a perfect square.

Problem 7.245 (Romanian Mathematical Olympiad District Round Grade 9, 2016). Let $a \geq 2$ be an integer. Prove that the following statements are equivalent:

(a) One can find positive integers b and c such that $a^2 = b^2 + c^2$.

(b) One can find a positive integer d such that the equations $x^2 - ax + d = 0$ and $x^2 - ax - d = 0$ have integer roots.

Problem 7.246 (Romanian Mathematical Olympiad Final Round Grade 5, 2016). Two positive integers x and y are such that

$$\begin{aligned}\frac{2010}{2011} &< \frac{x}{y} \\ &< \frac{2011}{2012}\end{aligned}$$

Find the smallest possible value of the sum $x+y$.

Problem 7.247 (Romanian Mathematical Olympiad Final Round Grade 5, 2016). Find all the positive integers a, b, and c with the property $a+b+c=abc$.

Problem 7.248 (Romanian Mathematical Olympiad Final Round Grade 6, 2016). We will call a positive integer *exquisite* if it is a multiple of the number of its divisors (for instance, 12 is exquisite because it has 6 divisors and 12 is a multiple of 6).

(a) Find the largest exquisite two digit number.

(b) Prove that no exquisite number has its last digit 3.

Problem 7.249 (Romanian Mathematical Olympiad Final Round Grade 6, 2016). Find all positive integers a and b so that $\frac{a+1}{b}$ and $\frac{b+2}{a}$ are simultaneously positive integers.

Problem 7.250 (Romanian Mathematical Olympiad Final Round Grade 6, 2016). Let a and b be positive integers so that there exists a prime number p with the property $[a, a+p]=[b, b+p]$. Prove that $a=b$. Here, $[x, y]$ denotes the least common multiple of x and y.

Problem 7.251 (Romanian Mathematical Olympiad Final Round Grade 7, 2016). Find all non-negative integers n such that

$$\sqrt{n+3}+\sqrt{n+\sqrt{n+3}}$$

is an integer.

Problem 7.252 (Romanian Mathematical Olympiad Final Round Grade 7, 2016). Find all the positive integers p with the property that the sum of the first p positive integers is a four-digit positive integer whose decomposition into prime factors is of the form $2^m 3^n (m+n)$, where m and n are non-negative integers.

Problem 7.253 (Romanian Mathematical Olympiad Final Round Grade 8, 2016). Let n be a non-negative integer. We will say that the non-negative integers $x_1, x_2, \ldots, x_n$ have property (P) if

$$x_1 x_2 \ldots x_n = x_1 + 2x_2 + \cdots + nx_n$$

(a) Show that for every non-negative integer n, there exists n positive integers with property (P).

(b) Find all integers $n \geq 2$ so that there exists n positive integers $x_1, x_2, \ldots, x_n$ with $x_1 < x_2 < \cdots < x_n$, having property (P).

Problem 7.254 (Romanian Mathematical Olympiad Final Round Grade 9, 2016).

(a) Prove that 7 cannot be written as a sum of squares of three rational numbers.

(b) Let a be a rational number that can be written as a sum of squares of three rational numbers. Prove that a^m can be written as a sum of squares of three rational numbers, for any positive integer m.

Problem 7.255 (Romanian National Mathematical Olympiad Small Juniors Shortlist, 2016). Find all non-negative integers n so that n^2-4n+2, $n^2-3n+13$ and $n^2-6n+19$ are simultaneously primes.

Problem 7.256 (Romanian National Mathematical Olympiad Small Juniors Shortlist, 2016). We will call a number good if it is a positive integer with at least two digits and by removing one of its digits we get a number which is equal to the sum of its initial digits (for instance, 109 is good: remove 9 to get $10 = 1 + 0 + 9$).

(a) Find the smallest good number.

(b) Find how many numbers are good.

Problem 7.257 (Romanian National Mathematical Olympiad Small Juniors Shortlist, 2016). Four positive integers a, b, c, and d are not divisible by 5 and the sum of their squares is divisible by 5. Prove that

$$N = (a^2+b^2)(a^2+c^2)(a^2+d^2)(b^2+c^2)(b^2+d^2)(c^2+d^2)$$

is divisible by 625.

Problem 7.258 (Romanian National Mathematical Olympiad Small Juniors Shortlist, 2016). For a positive integer n denote $d(n)$ the number of its positive divisors and $s(n)$ their sum. It is known that $n+d(n) = s(n)+1$, $m+d(m) = s(m)+1$, and $nm+d(nm)+2016 = s(nm)$. Find n and m.

Problem 7.259 (Romanian National Mathematical Olympiad Small Juniors Shortlist, 2016). Prove that there are no positive integers of the form

$$n = \underbrace{\overline{aa\ldots a}}_{k \text{ times}} + 5a$$

divisible by 2016 where $k > 1$.

Problem 7.260 (Romanian National Mathematical Olympiad Small Juniors Shortlist, 2016). Find the smallest positive integer of the form

$$n = \underbrace{\overline{aa\ldots a}}_{k \text{ times}} + a(a-2)^2$$

divisible by 2016 where $k > 1$.

Problem 7.261 (Romanian National Mathematical Olympiad Small Juniors Shortlist, 2016). A positive integer k will be called of *type* n ($n \neq k$) if n can be obtained by adding to k the sum or the product of the digits of k.

(a) Show that there are at least two numbers of type 2016.

(b) Find all numbers of type 216.

Problem 7.262 (Romanian National Mathematical Olympiad Juniors Shortlist, 2016).

(a) Prove that $2^n + 3^n + 5^n + 8^n$ is not a perfect square for any positive integer n.

(b) Find all positive integers n so that

$$1^n + 4^n + 6^n + 7^n = 2^n + 3^n + 5^n + 8^n$$

Problem 7.263 (Romanian National Mathematical Olympiad Juniors Shortlist, 2016).

(a) Find all perfect squares of the form $\overline{aabcc}$.

(b) Let n be a given positive integer. Prove that there exists a perfect square of the form

$$\overline{aab\underbrace{cc\cdots c}_{2n \text{ times}}}$$

Problem 7.264 (Romanian National Mathematical Olympiad Juniors Shortlist, 2016). Prove that $2n^2 + 27n + 91$ is a perfect square for infinitely many positive integers n.

Problem 7.265 (Romanian National Mathematical Olympiad Seniors Shortlist, 2016). Let p be a prime number and $n_1, n_2, \ldots, n_k \in \{1, 2, \ldots, p-1\}$ be positive integers. Show that the equation

$$x_1^{n_1} + x_2^{n_2} + \cdots + x_k^{n_k} = x_{k+1}^p$$

has infinitely many positive integer solutions.

Problem 7.266 (Romanian National Mathematical Olympiad Seniors Shortlist, 2016). Let $n \geq 4$ be a positive integer and define $A_n = \{1, 2, \ldots, n-1\}$. Find the number of solutions in the set $A_n \times A_n \times A_n \times A_n$ of the system

$$\begin{cases} x + z &= 2y \\ y + t &= 2z \end{cases}$$

Problem 7.267 (Romanian Stars of Mathematics Junior Level 2016). Show that there are positive odd integers $m_1 < m_2 < \ldots$ and positive integers $n_1 < n_2 < \ldots$ such that m_k and n_k are relatively prime, and $m_k^k - 2n_k^4$ is a perfect square for each index k.

Problem 7.268 (Romanian Stars of Mathematics Junior Level 2016). Given an integer $n \geq 3$ and a permutation $a_1, a_2, \ldots, a_n$ of the first n positive integers, show that at least $\sqrt{n}$ distinct residue classes modulo n occur in the list

$$a_1, a_1 + a_2, \ldots, a_1 + a_2 + \cdots + a_n$$

Problem 7.269 (Romanian Stars of Mathematics Senior Level 2016). Let n be a positive integer and let $a_1, a_2, \ldots, a_n$ be n positive integers. Show that

$$\sum_{k=1}^{n} \frac{\sqrt{a_k}}{1 + a_1 + a_2 + \cdots + a_k} < \sum_{k=1}^{n^2} \frac{1}{k}$$

Problem 7.270 (Romania TST for Junior Balkan Mathematical Olympiad 2016). Let M be the set of natural numbers k for which there exists a natural number n such that

$$3^n \equiv k \pmod{n}$$

Prove that M has infinitely many elements.

Problem 7.271 (Romania TST for Junior Balkan Mathematical Olympiad 2016). Let n be an integer greater than 2 and consider the set

$$A = \{2^n - 1, 3^n - 1, \ldots, (n-1)^n - 1\}$$

Given that n does not divide any element of A, prove that n is a square-free number. Does it necessarily follow that n is a prime?

Problem 7.272 (Romania TST for Junior Balkan Mathematical Olympiad 2016). Let n be a positive integer and consider the system

$$S(n): \begin{cases} x^2 + ny^2 = z^2 \\ nx^2 + y^2 = t^2 \end{cases}$$

where x, y, z, and t are naturals. If

- $M_1 = \{n \in \mathbb{N} : \text{system } S(n) \text{ has infinitely many solutions}\}$, and
- $M_1 = \{n \in \mathbb{N} : \text{system } S(n) \text{ has no solutions}\}$,

prove that

(a) $7 \in M_1$ and $10 \in M_2$.

(b) sets M_1 and M_2 are infinite.

Problem 7.273 (Romania TST 2016). Let n be a positive integer and let $a_1, a_2, \ldots, a_n$ be pairwise distinct positive integers. Show that

$$\sum_{k=1}^{n} \frac{1}{[a_1, a_2, \ldots, a_k]} < 4$$

where $[a_1, a_2, \ldots, a_k]$ is the least common multiple of the integers $a_1, a_2, \ldots, a_k$.

Problem 7.274 (Romania TST 2016). Determine the integers $k \geq 2$ for which the sequence

$$\binom{2n}{n} \pmod{k}$$

is eventually periodic where $0 \leq k \leq 2n$.

Problem 7.275 (Romania TST 2016). Given positive integers k and m, show that m and $\binom{n}{k}$ are relatively prime for infinitely many integers $n \geq k$.

Problem 7.276 (Romania TST 2016). Prove that:

(a) If $(a_n)_{n\geq 1}$ is a strictly increasing sequence of positive integers such that $(a_{2n-1} + a_{2n})/a_n$ is constant as n runs through all positive integers, then this constant is an integer greater than or equal to 4; and

(b) Given an integer $N \geq 4$, there exists a strictly increasing sequence $(a_n)_{n\geq 1}$ of positive integers such that $(a_{2n-1} + a_{2n})/a_n = N$ for all indices n.

Problem 7.277 (Romaina TST 2016). Given a positive integer k and an integer $a \equiv 3 \pmod 8$, show that $a^m + a + 2$ is divisible by 2^k for some positive integer m.

Problem 7.278 (Romaina TST 2016). Given a positive integer n, show that for no set of integers modulo n, whose size exceeds $1 + \sqrt{n+4}$, is it possible that the pairwise sums of unordered pairs be all distinct.

Problem 7.279 (Romania TST 2016). Given a prime p, prove that the sum

$$\sum_{k=1}^{\lfloor q/p \rfloor} k^{p-1}$$

is not divisible by q for all but finitely many primes q.

Problem 7.280 (Romania TST 2016). Determine the positive integers expressible in the form $\frac{x^2+y}{xy+1}$, for at least two pairs (x, y) of positive integers.

Problem 7.281 (All-Russian Olympiads 2016, Grade 11). Let n be a positive integer and let $k_0, k_1, \ldots, k_{2n}$ be nonzero integers such that

$$k_0 + k_1 + \cdots + k_{2n} \neq 0$$

Is it always possible to a permutation $(a_0, a_1, \ldots, a_{2n})$ of $(k_0, k_1, \ldots, k_{2n})$ so that the equation

$$a_{2n}x^{2n} + a_{2n-1}x^{2n-1} + \cdots + a_0 = 0$$

has not integer roots?

Problem 7.282 (San Diego Math Olympiad 2016). Let a, b, c, d be four integers. Prove that

$$(b-a)(c-a)(d-a)(d-c)(d-b)(c-b)$$

is divisible by 12.

Problem 7.283 (San Diego Math Olympiad 2016). Quadratic equation $x^2+ax+b+1=0$ have 2 positive integer roots, for integers a, b. Show that a^2+b^2 is not a prime.

Problem 7.284 (Saudi Arabia Pre-selection Test 2016). Let p be a given prime. For each prime r, we define

$$F(r) = \frac{(p^{rp}-1)(p-1)}{(p^r-1)(p^p-1)}$$

1. Show that $F(r)$ is a positive integer for any prime $r \neq p$.
2. Show that $F(r)$ and $F(s)$ are relatively prime for any primes r and s such that $r \neq p, s \neq p$ and $r \neq s$.
3. Fix a prime $r \neq p$. Show that there is a prime divisor q of $F(r)$ such that $p \mid q-1$ but $p^2 \nmid q-1$.

Problem 7.285 (Saudi Arabia Pre-selection Test 2016). Let u and v be positive rational numbers with $u \neq v$. Assume that there are infinitely many positive integers n with the property that $u^n - v^n$ is an integer. Prove that u and v are integers.

Problem 7.286 (Saudi Arabia Pre-selection Test 2016). Let a and b be two positive integers such that

$$b+1 \mid a^2+1$$
$$a+1 \mid b^2+1$$

Prove that both a and b are odd.

Problem 7.287 (Saudi Arabia Pre-selection Test 2016).

1. Prove that there are infinitely many positive integers n such that there exists a permutation of $1, 2, 3, \ldots, n$ with the property that the difference between any two adjacent numbers is equal to either 2015 or 2016.
2. Let k be a positive integer. Is the statement in part 1 still true if we replace the numbers 2015 and 2016 by k and $k+2016$, respectively?

Problem 7.288 (Saudi Arabia Pre-selection Test 2016). Let n be a given positive integer. Prove that there are infinitely many pairs of positive integers (a, b) with $a, b > n$ such that

$$\prod_{i=1}^{2015} (a+i) \mid b(b+2016)$$
$$\prod_{i=1}^{2015} (a+i) \nmid b$$
$$\prod_{i=1}^{2015} (a+i) \nmid (b+2016)$$

Problem 7.289 (Saudi Arabia TST for Gulf Mathematical Olympiad 2016). Find all positive integer n such that there exists a permutation $(a_1, a_2, \ldots, a_n)$ of $(1, 2, 3, \ldots, n)$ satisfying the condition:

$$k \mid a_1 + a_2 + \ldots + a_k$$

for $1 \leq k \leq n$.

Problem 7.290 (Saudi Arabia TST for Balkan Mathematical Olympiad 2016). Show that there are infinitely many positive integers n such that n has at least two prime divisors and $20^n + 16^n$ is divisible by n^2.

Problem 7.291 (Saudi Arabia TST for Balkan Mathematical Olympiad 2016). Let m and n be odd integers such that (n^2-1) is divisible by m^2+1-n^2. Prove that $|m^2+1-n^2|$ is a perfect square.

Problem 7.292 (Saudi Arabia TST for Balkan Mathematical Olympiad 2016). Let $a > b > c > d$ be positive integers such that

$$a^2 + ac - c^2 = b^2 + bd - d^2$$

Prove that $ab + cd$ is a composite number.

Problem 7.293 (Saudi Arabia TST for Balkan Mathematical Olympiad 2016). For any positive integer n, show that there exists a positive integer m such that n divides $2016^m + m$.

Problem 7.294 (Saudi Arabia TST for Balkan Mathematical Olympiad 2016). Let d be a positive integer. Show that for every integer S, there exist a positive integer n and a sequence $a_1, a_2, \ldots, a_n \in \{-1, 1\}$ such that

$$S = a_1(1+d)^2 + a_2(1+2d)^2 + \cdots + a_n(1+nd)^2$$

Problem 7.295 (Saudi Arabia TST for Balkan Mathematical Olympiad 2016). Let p and q be given primes and the sequence $(p_n)_{n\geq 1}$ defined recursively as follows: $p_1 = p$, $p_2 = q$, and p_{n+2} is the largest prime divisor of the number $(p_n + p_{n+1} + 2016)$ for all $n \geq 1$. Prove that this sequence is bounded. That is, there exists a positive real number M such that $a_n < M$ for all positive integers n.

Problem 7.296 (Saudi Arabia IMO TST 2016). Let $n \geq 3$ be an integer and let $x_1, x_2, \ldots, x_n$ be n distinct integers. Prove that

$$(x_1 - x_2)^2 + (x_2 - x_3)^2 + \cdots + (x_n - x_1)^2 \geq 4n - 6$$

Problem 7.297 (Saudi Arabia IMO TST 2016). Let k be a positive integer. Prove that there exist integers x and y, neither of which divisible by 7, such that

$$x^2 + 6y^2 = 7^k$$

Problem 7.298 (Saudi Arabia IMO TST 2016). Define the sequence $a_1, a_2, \ldots a_s$ follows: $a_1 = 1$, and for every $n \geq 2$, $a_n = n - 2$ if $a_{n-1} = 0$ and $a_n = a_{n-1} - 1$, otherwise. Find the number of $1 \leq k \leq 2016$ such that there are non-negative integers r and s and a positive integer n satisfying $k = r + s$ and $a_{n+r} = a_n + s$.

Problem 7.299 (Saudi Arabia IMO TST 2016). Let a be a positive integer. Find all prime numbers p with the following property: there exist exactly p ordered pairs of integers (x, y), with $0 \leq x, y \leq p - 1$, such that p divides $y^2 - x^3 - a^2x$.

Problem 7.300 (Saudi Arabia IMO TST 2016). Find the number of permutations $(a_1, a_2, \ldots, a_{2016})$ of the first 2016 positive integers satisfying the following two conditions:

1. $a_{i+1} - a_i \leq 1$ for all $i = 1, 2, \ldots, 2015$, and
2. There are exactly two indices $i < j$ with $1 \leq i < j \leq 2016$ such that $a_i = i$ and $a_j = j$.

Problem 7.301 (Saudi Arabia IMO TST 2016). Call a positive integer $N \geq 2$ *special* if for every k such that $2 \leq k \leq N$, N can be expressed as a sum of k positive integers that are relatively prime to N (although not necessarily relatively prime to each other). Find all special positive integers.

Problem 7.302 (Serbia Additional TST 2016). Let $w(x)$ be largest odd divisor of x. Let a, b be natural numbers such that $(a, b) = 1$ and $a + w(b+1)$ and $b + w(a+1)$ are powers of two. Prove that $a + 1$ and $b + 1$ are powers of two.

Problem 7.303 (Serbia National Olympiad 2016). Let $n > 1$ be an integer. Prove that there exist $m > n^n$ such that

$$\frac{n^m - m^n}{m + n}$$

is a positive integer.

Problem 7.304 (Serbia National Olympiad 2016). Let $a_1, a_2, \ldots, a_{2^{2016}}$ be positive integers not bigger than 2016. We know that for each $n \leq 2^{2016}$, $a_1 a_2 \ldots a_n + 1$ is a perfect square. Prove that for some i , $a_i = 1$.

Problem 7.305 (Serbia TST for Junior Balkan Mathematical Olympiad 2016). Find minimal number of divisors that can number $|2016^m - 36^n|$ have,where m and n are natural numbers.

Problem 7.306 (Slovakia Domestic Category B Mathematical Olympiad 2016). Let k, l, and m be positive integers such that

$$\frac{k + m + klm}{lm + 1} = \frac{2051}{44}$$

Find all possible values for klm.

Problem 7.307 (Slovakia Domestic Category B Mathematical Olympiad 2016). A positive integer has the property that the number of its even divisors is 3 more than the number of its odd divisors. What is the ratio of sum of all even divisors over the sum of all odd divisors of this number? Find all possible answers.

Problem 7.308 (Slovakia Domestic Category C Mathematical Olympiad 2016). Find all possible values for the product pqr, where p, q, and r are primes satisfying

$$p^2 - (q+r)^2 = 637$$

Problem 7.309 (Slovakia School Round Category C Mathematical Olympiad 2016). Find all four digit numbers $\overline{abcd}$ such that

$$\overline{abcd} = 20 \cdot \overline{ab} + 16 \cdot \overline{cd}$$

Problem 7.310 (Slovakia Regional Round Category B Mathematical Olympiad 2016). Determine all positive integers k, l, and m such that

$$\frac{3l+1}{3kl+k+3} = \frac{lm+1}{5lm+m+5}$$

Problem 7.311 (Slovakia Regional Round Category C Mathematical Olympiad 2016). Find the least possible value of

$$3x^2 - 12xy + y^4$$

where x and y are non-negative integers.

Problem 7.312 (Slovakia National Round Category A Mathematical Olympiad 2016). Let $p > 3$ be a prime. Determine the number of all 6—tuples (a, b, c, d, e, f) of positive integers with sum $3p$ such that

$$\frac{a+b}{c+d}, \frac{b+c}{d+e}, \frac{c+d}{e+f}, \frac{d+e}{f+a}, \frac{e+f}{a+b}$$

are all integers.

Problem 7.313 (Slovakia TST 2016). Let n be a positive integer and let S_n be the set of all positive divisors of n (including 1 and n). Prove that the rightmost digit of more than half of the elements of S_n is 3.

Problem 7.314 (Slovakia TST 2016). Find all odd integers M for which the sequence $a_0, a_1, a_2, \ldots$ defined by $a_0 = \frac{1}{2}(2M+1)$ and $a_{k+1} = a_k \lfloor a_k \rfloor$ for $k = 0, 1, 2, \ldots$ contains at least one integer.

Problem 7.315 (South Africa National Olympiad 2016). Let k and m be integers with $1 < k < m$. For a positive integer i, let L_i be the least common multiple of $1, 2, \ldots, i$. Prove that k is a divisor of

$$L_i \cdot \left[\binom{m}{i} - \binom{m-k}{i} \right]$$

for all $i \geq 1$.

Problem 7.316 (Slovenia National Math Olympiad First Grade 2016). Find all relatively prime integers x and y that solve the equation

$$4x^3 + y^3 = 3xy^2$$

Problem 7.317 (Slovenia National Math Olympiad Fourth Grade 2016). Find all integers a, b, c, and d that solve the equation

$$a^2 + b^2 + c^2 = d + 13$$
$$a + 2b + 3c = \frac{d}{2} + 13$$

Problem 7.318 (Slovenia IMO TST 2016). Let

$$N = 2^{15} \cdot 2015$$

How many divisors of N^2 are strictly smaller than N and do not divide N?

Problem 7.319 (Slovenia IMO TST 2016, Philippine 2015). Prove that for all positive integers $n \geq 2$,

$$\frac{1}{2} + \sqrt{\frac{1}{2}} + \sqrt[3]{\frac{2}{3}} + \cdots + \sqrt[n]{\frac{n-1}{n}} < \frac{n^2}{n+1}$$

Problem 7.320 (Slovenia IMO TST 2016, Romania JBMO TST 2015). Find all positive integers a, b, c, and d such that

$$4^a \cdot 5^b - 3^c \cdot 11^d = 1$$

Problem 7.321 (Spain National Olympiad 2016). Two real number sequences are guiven, one arithmetic $(a_n)_{n\in\mathbb{N}}$ and another geometric sequence $(g_n)_{n\in\mathbb{N}}$ none of them constant. Those sequences verifies $a_1 = g_1 \neq 0$, $a_2 = g_2$ and $a_{10} = g_3$. Find with proof that, for every positive integer p, there is a positive integer m, such that $g_p = a_m$.

Problem 7.322 (Spain National Olympiad 2016). Given a positive prime number p. Prove that there exist a positive integer α such that $p \mid \alpha(\alpha - 1) + 3$, if and only if there exist a positive integer β such that $p \mid \beta(\beta - 1) + 25$.

Problem 7.323 (Spain National Olympiad 2016). Let m be a positive integer and a and b be distinct positive integers strictly greater than m^2 and strictly less than $m^2 + m$. Find all integers d such that $m^2 < d < m^2 + m$ and d divides ab.

Problem 7.324 (Switzerland Preliminary Round 2016). Determine all natural numbers n such that for all positive divisors d of n,

$$d + 1 \mid n + 1$$

Problem 7.325 (Switzerland Final Round 2016). Find all positive integers n for which primes p and q exist such that

$$p(p + 1) + q(q + 1) = n(n + 1)$$

Problem 7.326 (Switzerland Final Round 2016). Let a_n be a sequence of positive integers defined by $a_1 = m$ and $a_n = a_{n-1}^2 - 1$ for $n = 2, 3, 4, \ldots$. A pair (a_k, a_l) is called *interesting* if

(i) $0 < l - k < 2016$, and

(ii) a_k divides a_l.

Prove that there exists a positive integer m such that the sequence a_n contains no interesting pair.

Problem 7.327 (Switzerland TST 2016). Let n be a positive integer. We call a pair of natural numbers *incompatible* if their greatest common divisor is equal to 1. Find the minimum value of incompatible pairs when one divides the set $\{1, 2, \dots, 2n\}$ into n pairs.

Problem 7.328 (Switzerland TST 2016). Let n be a positive integer. Show that $7^{7^n} + 1$ has at least $2n + 3$ prime divisors (not necessarily distinct).

Problem 7.329 (Switzerland TST 2016). Find all positive integers n such that

$$\sum_{\substack{d \mid n \\ 1 \le d \le n}} d^2 = 5(n+1)$$

Problem 7.330 (Syria Central Round First Stage 2016). A positive integer $n \geq 2$ is called *special* if n^2 can be written as sum of n consecutive positive integers (for instance, 3 is special since $3^2 = 2 + 3 + 4$).

(i) Prove that 2016 is not special.

(ii) Prove that the product of two special numbers is also special.

Problem 7.331 (Syria Central Round Second Stage 2016). Find all integers a and b such that $a^3 - b^2 = 2$.

Problem 7.332 (Syria TST 2016). Find all positive integers m and n such that

$$\frac{1}{m} + \frac{1}{n} = \frac{3}{2014}$$

Problem 7.333 (Taiwan TST First Round 2016). Find all ordered pairs (a, b) of positive integers that satisfy $a > b$ and the equation $(a - b)^{ab} = a^b b^a$.

Problem 7.334 (Taiwan TST Second Round 2016). Let a and b be positive integers such that $a! + b!$ divides $a!b!$. Prove that $3a \geq 2b + 2$.

Problem 7.335 (Taiwan TST Second Round 2016). Let $\langle F_n \rangle$ be the Fibonacci sequence, that is, $F_0 = 0$, $F_1 = 1$, and $F_{n+2} = F_{n+1} + F_n$ holds for all non-negative integers n. Find all pairs (a, b) of positive integers with $a < b$ such that $F_n - 2na^n$ is divisible by b for all positive integers n.

Problem 7.336 (Taiwan TST Third Round 2016). Let n be a positive integer. Find the number of odd coefficients of the polynomial $(x^2 - x + 1)^n$.

Problem 7.337 (Taiwan TST Third Round 2016). Let k be a positive integer. A sequence $a_0, a_1, \dots, a_n$ $(n > 0)$ of positive integers satisfies the following conditions:

(i) $a_0 = a_n = 1$;

(ii) $2 \leq a_i \leq k$ for each $k = 1, 2, \ldots, n-1$

(iii) For each $j = 2, 3, \ldots, k$, the number j appears $\varphi(j)$ times in the sequence $a_0, a_1, \ldots, a_n$ ($\varphi(j)$ is the number of positive integers that do not exceed j and are relatively prime to j);

(iv) For any $i = 1, 2, \ldots, n-1$, $\gcd(a_{i-1}, a_i) = 1 = \gcd(a_i, a_{i+1})$, and a_i divides $a_{i-1} + a_{i+1}$

There is another sequence $b_0, b_1, \ldots, b_n$ of integers such that

$$\frac{b_{i+1}}{a_{i+1}} > \frac{b_i}{a_i}$$

for all $i = 0, 1, \ldots, n-1$. Find the minimum value for $b_n - b_0$.

Problem 7.338 (Taiwan TST Third Round 2016). Let $f(x)$ be the polynomial with integer coefficients ($f(x)$ is not constant) such that

$$(x^3 + 4x^2 + 4x + 3)f(x) = (x^3 - 2x^2 + 2x - 1)f(x+1)$$

Prove that for each positive integer $n \geq 8$, $f(n)$ has at least five distinct prime divisors.

Problem 7.339 (Turkey TST for European Girls' Mathematical Olympiad 2016). Prove that for every square-free integer $n > 1$, there exists a prime number p and an integer m satisfying $p \mid n$ and $n \mid p^2 + p \cdot m^p$.

Problem 7.340 (Turkey TST for Junior Balkan Mathematical Olympiad 2016). Let n be a positive integer, p and q be prime numbers such that

$$pq \mid n^p + 2$$
$$n + 2 \mid n^p + q^p$$

Prove that there exists a positive integer m satisfying $q \mid 4^m \cdot n + 2$.

Problem 7.341 (Turkey TST for Junior Balkan Mathematical Olympiad 2016). Find all pairs (p, q) of prime numbers satisfying

$$p^3 + 7q = q^9 + 5p^2 + 18p$$

Problem 7.342 (Turkey TST 2016). p is a prime. Let K_p be the set of all polynomials with coefficients from the set $\{0, 1, \ldots, p-1\}$ and degree less than p. Assume that for all pairs of polynomials $P, Q \in K_p$ such that $P(Q(n)) \equiv n \pmod{p}$ for all integers n, the degrees of P and Q are equal. Determine all primes p with this condition.

Problem 7.343 (Turkmenistan Regional Olympiad 2016). Find all distinct prime numbers p, q, r, s such that

$$1 - \frac{1}{p} - \frac{1}{q} - \frac{1}{r} - \frac{1}{s} = \frac{1}{pqrs}$$

Problem 7.344 (Tuymaada Senior League 2016). For each positive integer k determine the number of solutions of the equation

$$8^k = x^3 + y^3 + z^3 - 3xyz$$

in non-negative integers x, y, and z such that $0 \leq x \leq y \leq z$.

Problem 7.345 (Tuymaada Senior League 2016). The ratio of prime numbers p and q does not exceed 2 ($p \neq q$). Prove that there are two consecutive positive integers such that the largest prime divisor of one of them is p and that of the other is q.

Problem 7.346 (Tuymaada Junior League 2016). Is there a positive integer $N > 10^{20}$ such that all its decimal digits are odd, the numbers of digits $1, 3, 5, 7, 9$ in its decimal representation are equal, and it is divisible by each 20—digit number obtained from it by deleting digits? (Neither deleted nor remaining digits must be consecutive.)

Problem 7.347 (Ukraine TST for UMO 2016). Find all numbers n such, that in $[1; 1000]$ there exists exactly 10 numbers with digit sum equal to n.

Problem 7.348 (Ukraine TST for UMO 2016). Number 125 is written as the sum of several pairwise distinct and relatively prime numbers, greater than 1. What is the maximal possible number of terms in this sum?

Problem 7.349 (Ukraine TST for UMO 2016). Given prime number p and different natural numbers m, n such that $p^2 = \frac{m^2+n^2}{2}$. Prove that $2p - m - n$ is either square or doubled square of an integer number.

Problem 7.350 (Ukraine TST for UMO 2016). Solve the equation $n(n^2+19) = m(m^2-10)$ in positive integers.

Problem 7.351 (USA AIME 2016). For $-1 < r < 1$, let $S(r)$ denote the sum of the geometric series

$$12 + 12r + 12r^2 + 12r^3 + \cdots$$

Let a between -1 and 1 satisfy $S(a)S(-a) = 2016$. Find $S(a) + S(-a)$.

Problem 7.352 (USA AIME 2016). For a permutation $p = (a_1, a_2, \ldots, a_9)$ of the digits $1, 2, \ldots, 9$, let $s(p)$ denote the sum of the three 3-digit numbers $a_1a_2a_3$, $a_4a_5a_6$, and $a_7a_8a_9$. Let m be the minimum value of $s(p)$ subject to the condition that the units digit of $s(p)$ is 0. Let n denote the number of permutations p with $s(p) = m$. Find $|m - n|$.

Problem 7.353 (USA AIME 2016). A strictly increasing sequence of positive integers $a_1, a_2, a_3, \ldots$ has the property that for every positive integer k, the subsequence $a_{2k-1}, a_{2k}, a_{2k+1}$ is geometric and the subsequence $a_{2k}, a_{2k+1}, a_{2k+2}$ is arithmetic. Suppose that $a_{13} = 2016$. Find a_1.

Problem 7.354 (USA AIME 2016). Find the least positive integer m such that $m^2 - m + 11$ is a product of at least four not necessarily distinct primes.

Problem 7.355 (USA AIME 2016). Let x, y and z be real numbers satisfying the system

$$\log_2(xyz - 3 + \log_5 x) = 5$$
$$\log_3(xyz - 3 + \log_5 y) = 4$$
$$\log_4(xyz - 3 + \log_5 z) = 4$$

Find the value of $|\log_5 x| + |\log_5 y| + |\log_5 z|$.

Problem 7.356 (USA AIME 2016). For polynomial $P(x) = 1 - \frac{1}{3}x + \frac{1}{6}x^2$, define

$$\begin{aligned} Q(x) &= P(x)P(x^3)P(x^5)P(x^7)P(x^9) \\ &= \sum_{i=0}^{50} a_i x^i \end{aligned}$$

Then,

$$\sum_{i=0}^{50} |a_i| = \frac{m}{n}$$

where m and n are relatively prime positive integers. Find $m + n$.

Problem 7.357 (USA AIME 2016). Find the number of sets $\{a, b, c\}$ of three distinct positive integers with the property that the product of a, b, and c is equal to the product of $11, 21, 31, 41, 51$, and 61.

Problem 7.358 (USA AIME 2016). The sequences of positive integers $1, a_2, a_3, \ldots$ and $1, b_2, b_3, \ldots$ are an increasing arithmetic sequence and an increasing geometric sequence, respectively. Let $c_n = a_n + b_n$. There is an integer k such that $c_{k-1} = 100$ and $c_{k+1} = 1000$. Find c_k.

Problem 7.359 (USA AIME 2016). For positive integers N and k, define N to be k-nice if there exists a positive integer a such that a^k has exactly N positive divisors. Find the number of positive integers less than 1000 that are neither 7-nice nor 8-nice.

Problem 7.360 (USAJMO 2016). Prove that there exists a positive integer $n < 10^6$ such that 5^n has six consecutive zeros in its decimal representation.

Problem 7.361 (USAMO 2016). Prove that for any positive integer k,

$$(k^2)! \cdot \prod_{j=0}^{k-1} \frac{j!}{(j+k)!}$$

is an integer.

Problem 7.362 (USAMO 2016).

(a) Prove that if n is an odd perfect number then n has the following form $n = p^s m^2$ where p is prime has form $4k + 1$, s is positive integers has form $4h + 1$, and $m \in \mathbb{Z}^+$, m is not divisible by p.

(b) Find all $n \in \mathbb{Z}^+, n > 1$ such that $n-1$ and $\frac{n(n+1)}{2}$ is perfect number.

Problem 7.363 (USA TSTST 2016). Decide whether or not there exists a nonconstant polynomial $Q(x)$ with integer coefficients with the following property: for every positive integer $n > 2$, the numbers

$$Q(0),\ Q(1), Q(2),\ \ldots,\ Q(n-1)$$

produce at most $0.499n$ distinct residues when taken modulo n.

Problem 7.364 (USA TSTST 2016). Suppose that n and k are positive integers such that

$$1 = \underbrace{\varphi(\varphi(\ldots \varphi(}_{k \text{ times}} n) \ldots))$$

Prove that $n \leq 3^k$.

Problem 7.365 (USA TST 2016). Let $\sqrt{3} = 1.b_1b_2b_3\ldots_{(2)}$ be the binary representation of $\sqrt{3}$. Prove that for any positive integer n, at least one of the digits $b_n, b_{n+1}, \ldots, b_{2n}$ equals 1.

Problem 7.366 (Venezuela Final Round Fourth Year 2106). Find all pairs of prime numbers (p, q), with $p < q$, such that the numbers $p + 2q, 2p + q$ and $p + q - 22$ are also primes.

Problem 7.367 (Zhautykov Olympiad 2016). $a_1, a_2, \ldots, a_{100}$ are permutation of $1, 2, \ldots, 100$. $S_1 = a_1, S_2 = a_1 + a_2, \ldots, S_{100} = a_1 + a_2 + \ldots + a_{100}$ Find the maximum number of perfect squares from S_i.

Problem 7.368 (Zhautykov Olympiad 2016). We call a positive integer q a *convenient denominator* for a real number α if

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{10q}$$

for some integer p. Prove that if two irrational numbers α and β have the same set of convenient denominators then either $\alpha + \beta$ or $\alpha - \beta$ is an integer.

§§7 Glossary

Binomial Identities 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. $\binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n-1}^2 + \binom{n}{n}^2 = \binom{2n}{n}$
7. If n and k are relatively prime, then n divides $\binom{n}{k}$ and k divides $\binom{n-1}{k-1}$.

PBinomial Theorem For any positive integer n,

$$\begin{aligned}(a+b)^n &= a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{1}ab^{n-1} + b^n \\ &= \sum_{i=0}^{n}\binom{n}{i}a^{n-i}b^i \\ &= \sum_{i=0}^{n}\binom{n}{i}a^{i}b^{n-i}\end{aligned}$$

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 $n = 1$,

$$\begin{aligned}(a^2 + b^2)(c^2 + d^2) &= (ac + bd)^2 + (ad - bc)^2 \\ &= (ad + bc)^2 + (ac - bd)^2\end{aligned}$$

Sum of Differences Let $a_1, a_2, a_3, \cdots$ be an infinite sequence of numbers. Then, for any positive integer n,

$$a_n = a_1 + \sum_{k=1}^{n-1} (a_{k+1} - a_k)$$

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.

§§7 Bibliography

[9] Arthur Engel. *Problem-solving strategies*. Springer, 1997.

[10] Titu Andreescu, D. Andrica, and Zuming Feng. *104 number theory problems: from the training of the USA IMO team*. Birkhäuser, 2007.

[11] Wacław Sierpiński. *Elementary theory of numbers*. eng. 1964. URL: http://eudml.org/doc/219306.

[14] L. Carlitz. "A Note on Wolstenholme's Theorem". In: *The American Mathematical Monthly* 61.3 (1954), pp. 174–176. DOI: 10.2307/2307217.

[15] Peter Vandendriessche and Hojoo Lee. "Problems in Elementary Number Theory (PEN)". In: (2007).

[16] Edouard Lucas. "Théorie des Fonctions Numériques Simplement Périodiques. [Continued]". In: *American Journal of Mathematics* 1.3 (1878), pp. 197–240. ISSN: 00029327, 10806377. URL: http://www.jstor.org/stable/2369311.

[17] Robert Daniel Carmichael. "Note on a new number theory function". In: *Bulletin of the American Mathematical Society* 16.5 (1910), pp. 232–239. DOI: 10.1090/s0002-9904-1910-01892-9.

[18] Wacław Sierpiński and Andrzej Schinzel. *Elementary theory of numbers*. Polish Scientific Publishers, 1988.

[20] Peter J. Cameron and D. A. Preece. "Primitive Lambda-Roots". In: (Jan. 2014). URL: https://cameroncounts.files.wordpress.com/2014/01/plr1.pdf.

[4] Leonard E. Dickson. *History of the theory of numbers*. Chelsea Pub. Co., 1952.

[1] D. Goldfeld. "The Elementary Proof of the Prime Number Theorem: An Historical Perspective". In: *Number Theory* (2004), pp. 179–192. DOI: 10.1007/978-1-4419-9060-0_10.

[1] Nils A. Baas and Christian F. Skau. "The lord of the numbers, Atle Selberg. On his life and mathematics". In: *Bulletin of the American Mathematical Society* 45.4 (2008), pp. 617–617. DOI: 10.1090/s0273-0979-08-01223-8.

[9] Srinivasa Ramanujan, Jaban Meher, and Ram M. Murty. "Ramanujan's Proof of Bertrand's Postulate". In: *The American Mathematical Monthly* 120.7 (2013), p. 650. DOI: 10.4169/amer.math.monthly.120.07.650.

[10] Paul Erdős. "Beweis eines Satzes von Tschebyschef". In: *Acta Litt. Sci. Szeged* 5 (1932), pp. 194–198.

[11] Jitsuro Nagura. "On the interval containing at least one prime number". In: *Proceedings of the Japan Academy* 28.4 (1952), pp. 177–181. DOI: 10.3792/pja/1195570997.

[12] M. El Bachraoui. "Primes in the interval [2n,3n]". In: *International Journal of Contemporary Mathematical Sciences* (2006), pp. 617–621. DOI: 10.12988/ijcms.2006.06065.

[13] Andy Loo. "On the Primes in the Interval [3n, 4n]". In: *International Journal of Contemporary Mathematical Sciences* 6.38 (2011). URL: http://www.m-hikari.com/ijcms-2011/37-40-2011/looIJCMS37-40-2011.pdf.

[14] Peter Moses J. C., Vladimir Shevelev, and Charles R. Greathouse. "On Intervals $(kn, (k+1)n)$ Containing a Prime for All $n \geq 1$". In: *Journal of Integer Sequences*. 13.7.3 16.7 (2013).

[16] Godfrey Harold Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford University Press, 1971.

[17] Peyman Nasehpour. "A computational criterion for the irrationality of some real numbers". In: (June 2018). URL: https://arxiv.org/abs/1806.07560v4.

[18] Dustin G. Mixon. "Another Simple Proof that the Sum of the Reciprocals of the Primes Diverges". In: *The American Mathematical Monthly* 120.9 (2013), pp. 831–831. DOI: 10.4169/amer.math.monthly.120.09.831. eprint: https://www.tandfonline.com/doi/pdf/10.4169/amer.math.monthly.120.09.831. URL: https://www.tandfonline.com/doi/abs/10.4169/amer.math.monthly.120.09.831.

[21] Neal Koblitz. *A course in number theory and cryptography*. Springer, 2012.

[24] Paulo Ribenboim. "The Little Book of Big Primes". In: (1991). DOI: 10.1007/978-1-4757-4330-2.

[25] J. W. Bruce. "A Really Trivial Proof of the Lucas-Lehmer Test". In: *The American Mathematical Monthly* 100.4 (1993), p. 370. DOI: 10.2307/2324959.

[26] J. M. Pollard. "A monte carlo method for factorization". In: *Bit* 15.3 (1975), pp. 331–334. DOI: 10.1007/bf01933667.

[27] Richard P. Brent. "An improved Monte Carlo factorization algorithm". In: *Bit* 20.2 (1980), pp. 176–184. DOI: 10.1007/bf01933190.

[1] Masum Billal and Samin Riasat. *Integer sequences: Divisibility, Lucas and Lehmer sequences*. 1st ed. Springer, 2021.

[3] Robert Daniel Carmichael. "On Euler's φ-function". In: *Bull. Amer. Math. Soc.* 13 (1907), pp. 241–243.

[4] Victor Klee Jr. "On a conjecture of Carmichael". In: *Bulletin of the American Mathematical Society* 53.12 (1947), pp. 1183–1187. DOI: 10.1090/s0002-9904-1947-08940-0.

[5] Carl Pomerance. "On Carmichael's Conjecture". In: *Proceedings of the American Mathematical Society*. 2nd ser. 43 (Apr. 1974), pp. 297–298.

[6] Hansraj Gupta. "Euler's Totient Function And Its Inverse". In: *Indian J. Pure Appl. Math* (1981), pp. 22–30.