Problem Set 1

Opener

Every positive integer has divisors, numbers that divide evenly into it. The divisors of 4 are 1, 2, and 4. The divisors of 18 are 1, 2, 3, 6, 9, and 18. In this Problem Set, you will investigate a function called σ, which takes in a positive integer, and returns the *sum* of all its divisors. For example, $\sigma(4) = 7$ and $\sigma(18) = 39$.

The Opener problems are important!

Here's a large table for the σ function. Complete the table without help from a calculator or computer.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\sigma(n)$				7								

n	13	14	15	16	17	18	19	20	21	22	23	24
$\sigma(n)$												

n	25	26	27	28	29	30	31	32	33	34	35	36
$\sigma(n)$												

n	37	38	39	40	41	42	43	44	45	46	47	48
$\sigma(n)$												

n	49	50	51	52	53	54	55	56	57	58	59	60
$\sigma(n)$					54							

n	61	62	63	64	65	66	67	68	69	70	71	72
$\sigma(n)$												

n	73	74	75	76	77	78	79	80	81	82	83	84
$\sigma(n)$												

n	85	86	87	88	89	90	91	92	93	94	95	96
$\sigma(n)$												

Important Stuff

1. Describe some patterns in the table for the σ function, especially patterns that helped you complete the table quickly, or patterns you could use to find other outputs.

Each Problem Set is divided into Important Stuff, Neat Stuff, and Tough Stuff—and the Opener, which is more important than any of the rest.

2. Determine each of the following without technology.

Why might part (c) be written as $5 \cdot 49$ instead of 245?

a. $\sigma(128)$ **b.** $\sigma(243)$ **c.** $\sigma(5 \cdot 49)$ **d.** $\sigma(257)$ **e.** $\sigma(1001)$

3. Define $A(n) = \frac{\sigma(n)}{n}$. Use a calculator if you find it helpful here.

a. Find all numbers n with $A(n) \leqslant 1$.
b. Find three numbers n with $A(n) = 2$.
c. Are there any numbers n with $A(n) = 3$?

Neat Stuff

Here are some more good questions to think about.

4. If p is prime, what can you say about $\sigma(p)$? About $A(p)$?

5. If p and q are primes, what can you say about $\sigma(pq)$? About $A(pq)$?

6. If p and q are primes, find the maximum possible value of $A(pq)$.

7. Without technology, find a number for which $\sigma(n) = 1000$ or show that no such number exists.

8. Find the maximum possible value of $A(n)$.

9. Go back to the problems on the previous page, except now use $\sigma_2(n)$, the sum of the *squares* of the divisors, and $B(n) = \frac{\sigma_2(n)}{n^2}$.

Tough Stuff

Here are two much more difficult problems to try.

10. Without using technology, find a number n for which $A(n) \geqslant 5$ or a proof that no such number exists.

11. Find an odd number for which $A(n) = 2$, or prove that no such number exists.

Problem Set 2

Opener

Problem Set 1 focused on the σ function, which outputs the sum of the divisors of its input. In this Problem Set, you will explore a function called a, which takes in a positive integer, and returns the sum of its divisors' *reciprocals*. For example, $a(12) = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{6} + \frac{1}{12} = \frac{7}{3}$.

Here's a table for the a function. Complete the table without using a calculator. Write answers in "lowest terms."

n	1	2	3	4	5	6	7	8	9	10	11	12
$a(n)$												$\frac{7}{3}$

n	13	14	15	16	17	18	19	20	21	22	23	24
$a(n)$												

n	25	26	27	28	29	30	31	32	33	34	35	36
$a(n)$												

n	37	38	39	40	41	42	43	44	45	46	47	48
$a(n)$												

Important Stuff

1. Determine each of the following.
   - **a.** $a(3) \cdot a(4)$
   - **b.** $a(2) \cdot a(5)$
   - **c.** $a(8) \cdot a(15)$
   - **d.** $a(120)$
   - **e.** $a(10) \cdot a(12)$

2. Determine each of the following without using a calculator.
   - **a.** $\left(1 + \frac{1}{3}\right)\left(1 + \frac{1}{2} + \frac{1}{4}\right)$
   - **b.** $\left(1 + \frac{1}{2}\right)\left(1 + \frac{1}{5}\right)$

c. $\left(1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}\right)\left(1+\frac{1}{3}+\frac{1}{5}+\frac{1}{15}\right)$
d. $\left(1+\frac{1}{2}+\frac{1}{5}+\frac{1}{10}\right)\left(1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{6}+\frac{1}{12}\right)$

3. Calculate each of the following any way you like.

a. $1+\frac{1}{2}$
b. $1+\frac{1}{2}+\frac{1}{4}$
c. $\frac{1}{2^0}+\frac{1}{2^1}+\frac{1}{2^2}+\frac{1}{2^3}$
d. $\frac{1}{2^0}+\frac{1}{2^1}+\frac{1}{2^2}+\cdots\frac{1}{2^6}$
e. The sum of all numbers in the form $\frac{1}{2^n}$ as n goes from 0 to 10
f. $\displaystyle\sum_{n=0}^{11}\frac{1}{2^n}$
g. $\displaystyle\sum_{n=0}^{\infty}\frac{1}{2^n}$

The notation in part (f) 3f says to sum $\frac{1}{2^n}$ for all n from 0 to 11. A good shorthand to learn.

4. Find the *smallest* possible number k for which you are completely sure that $k > a(n)$ for *all* powers of 3. In other words, k is the smallest number larger than all the numbers in the sequence

$$a(1), a(3), a(9), a(27), \ldots$$

Neat Stuff

5. For certain values of n, it turns out that $\sigma(n) = 3+\frac{n}{2}+n$. Classify these numbers and find a generalization.

Remember, the σ function is the sum of the divisors.

6. If p and q are primes, write a rule for $\sigma(pq)$ in terms of p and q.

7. If p and q are primes, write a rule for $a(pq)$ in terms of p and q and give the simplest answer you can.

8. Let n be any of the large set of numbers whose only prime factors are 2 and 3. ($n = 12$ and $n = 324$ are two examples.)

a. Find the smallest possible number k for which you are completely sure that $k > a(n)$, no matter what n was picked.
b. Find a suitable number n such that $k - a(n) < 0.1$.

9. Find the first ten numerators in the following bizarre-looking expansion. Do *not* try to simplify or combine terms, just expand!

$$\left(\frac{1}{1^x}+\frac{2}{2^x}+\frac{3}{3^x}+\frac{4}{4^x}+\cdots\right)\left(\frac{1}{1^x}+\frac{1}{2^x}+\frac{1}{3^x}+\frac{1}{4^x}+\cdots\right)$$
$$=\frac{?}{1^x}+\frac{?}{2^x}+\frac{?}{3^x}+\frac{?}{4^x}+\cdots$$

10. Find the first ten numerators in the following bizarre-looking expansion. Do *not* try to simplify or combine terms, just expand!

$$\left(\frac{1}{1^x}+\frac{4}{2^x}+\frac{9}{3^x}+\frac{16}{4^x}+\cdots\right)\left(\frac{1}{1^x}+\frac{1}{2^x}+\frac{1}{3^x}+\frac{1}{4^x}+\cdots\right)$$
$$=\frac{?}{1^x}+\frac{?}{2^x}+\frac{?}{3^x}+\frac{?}{4^x}+\cdots$$

Tough Stuff

11. Without using technology, find a number n for which $a(n) \geqslant 10$, or prove that no such number exists.

12. Find an odd number for which $a(n) = 2$, or prove that no such number exists.

Problem Set 1

Goals of the Problem Set

This course is about multiplicative functions, a concept that will be developed throughout the first few problem sets. Problem Set 1 is a study of one specific function, the σ ("sigma") function, that counts the sum of the divisors of an integer. Pattern recognition is a priority here, with the goal of emphasizing patterns that recur in many different functions.

Specifically, the σ function follows the rule that $\sigma(xy) = \sigma(x) \cdot \sigma(y)$ whenever x and y are relatively prime (share no common factors larger than 1). This fact may or may not emerge in Problem Set 1. As more multiplicative functions are presented, commonalities will emerge. There is no need to formalize any of the patterns participants discover at this time.

Problem Set 1 is also intended as an introduction to the style of the course. Consider having participants read the Introduction to learn about the course expectations.

Note that some participants may not get past Problem 1, and that's fine.

Notes on the Problems

The opener asks participants to complete the table without help from a calculator or computer, and we mean it! The table is deliberately too big for participants to blindly fill it in without using some sort of pattern or recognition of related answers. Here are some conjectures participants may use:

- $\sigma(p) = p + 1$ for primes
- If n is a perfect square, $\sigma(n) = n^2 + n + 1$
- $\sigma(2^n) = 2^{n+1} - 1$
- $\sigma(p^n)$ for primes can be found using the formula for geometric series
- $\sigma(xy) = \sigma(x) \cdot \sigma(y)$
- If n is a multiple of 7, then $\sigma(n)$ is a multiple of 8

Not all these conjectures are true. Challenge all conjectures with numeric examples. Participants may recognize in this set that the behavior for primes and nonprimes are different, or that the behavior for a number is based on its prime factorization. Both of these are important concepts

that will be developed further in later problem sets with new functions.

When discussing the opener, and the followup problem (Problem 1), try to keep the focus on numeric examples—especially if you feel that *any* participant is having trouble algebraically. Some examples:

- $\sigma(13) = 1 + 13 = 14$
- $\sigma(7) = 1 + 7 = 8$
- $\sigma(91) = 112 = 14 \cdot 8$
- $\sigma(2) = 1 + 2 = 3$
- $\sigma(9) = 1 + 3 + 9 = 13$
- $\sigma(18) = 39 = 3 \cdot 13$

In Problem 2, compare two different methods participants may use here. The first is enumerating the factors of the given number, and the second is using patterns discovered in the opener or during work on Problem 1. For example, work on part (c) could go like this:

$$\sigma(5 \cdot 49) = 1 + 5 + 7 + 35 + 49 + 245 = 342$$

or like this:

$$\sigma(5 \cdot 49) = \sigma(5) \cdot \sigma(49) = 6 \cdot 57 = 342$$

Look for any participant able to synthesize these methods by expanding $\sigma(5)$ and $\sigma(49)$:

$$\sigma(5) \cdot \sigma(49) = (1+5)(1+7+49) = 1+5+7+35+49+245$$

This gets to the heart of why multiplicative functions may behave as they do. If this comes up in this problem set or in a future problem set, try to bring it to everyone's attention. Some problems in later problem sets are intended to key on this concept.

Problem 3 will be revisited, but some participants may be interested especially in part (b), since it asks to identify "perfect" numbers without saying so.

Problems beyond Problem 3 will generally be revisited in "Important Stuff" later in the course. Only discuss a problem with the whole group if you are sure the entire group has had a chance to work on it. For Problem Set 1, almost all discussion should be about Problems 1 and 2.

Problem Set 2

Goals of the Problem Set

As with Problem Set 1, this problem set introduces a new multiplicative function, here called the a function. Names of functions are consistent throughout the course, but only the four functions with Greek letter names ϕ, σ, τ, and μ, have mathematical relevance outside this course. The goal here is to recognize consistent behavior: that the a function behaves "like" the σ function in significant ways.

A lesser goal of this problem set is to familiarize participants with sigma notation for summations (not related to the "sigma" function). This notation will be used more and more frequently as the course progresses, and this is a good opportunity to check or develop the notation before it becomes more relevant.

An optional goal is to present the number-line model for summing a series. See the details about Problem 3 below. The "comparison test" for series will be useful in later problem sets.

Notes on the Problems

Some participants may recognize that the a function given here is the same as the A function given in Problem Set 1, even though it is not described the same way: $A(n)$ was defined as $\frac{\sigma(n)}{n}$. Ask participants who recognize this to prove that the two functions must always behave the same—a proof involves writing the reciprocals using the least common denominator, which is always n. Also, don't bring this up to the whole group unless you are certain everyone has had exposure to the A function in Problem 3 of Problem Set 1.

The opener here should proceed similarly to the opener of Problem Set 1. Here are some conjectures like the ones from Problem Set 1:

- $a(p) = 1 + \frac{1}{p}$ for primes
- If n is a perfect square, $a(n) = 1 + \frac{1}{n} + \frac{1}{n^2}$
- $a(2^n) = 2 - \frac{1}{2^n}$
- $a(p^n)$ for primes can be found using the formula for geometric series
- $a(xy) = a(x) \cdot a(y)$
- If n is a multiple of 7, then $\sigma(n)$ is a multiple of $\frac{8}{7}$

As before, ask participants to verify conjectures by focusing on numeric examples, or by determining values for $a(n)$ when n isn't listed.

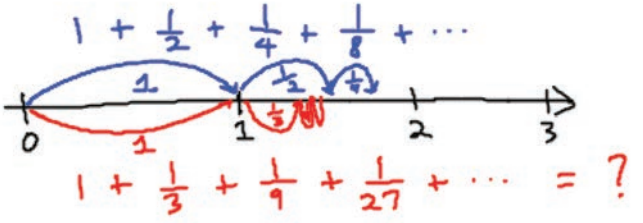
Problem 1 gives some cases to check against $a(xy) = a(x) \cdot a(y)$. The product for part (a), $\frac{7}{3}$, is given in the table. Parts (c) through (e) are designed to help participants recognize that $a(xy) = a(x) \cdot a(y)$ isn't always true. Some may write their suspected answer for part (e) without computing it.

Problem 2 is closely tied to Problem 1, as these are the expanded expressions for each $a(n)$ in all but part (d) of Problem 1. Some participants may use this problem as a basis for proving why $a(xy) = a(x) \cdot a(y)$ works when it does, and why it fails when it does. Specifically, the product in part (d) includes additional cross terms such as $\frac{1}{6}$ twice, and this never happens when x and y are relatively prime.

Problem 3 gives an opportunity for illustrating number line addition for working with summations like

$$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots$$

Here is an illustration for both the summation of $\frac{1}{2^n}$ and $\frac{1}{3^n}$:



This gives participants an understanding about infinite sums, but there is a more important piece at work here, the *comparison test*:

> If in two series, $a(n) \geqslant b(n)$ for each term,
> then $\sum a(n) \geqslant \sum b(n)$.

This concept will be useful in proving that the harmonic series $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots$ diverges, since another smaller series can be found that also diverges.

CHAPTER

4 Mathematical Overview

This overview contains a sample of the mathematical themes that the development team hammered out in the process of designing the 2009 PCMI course, *Famous Functions in Number Theory* (*FFNT* from now on). It contains some of the mathematical background used when creating the problem sets as well as some mathematical extensions that never made it into the "soup" of problems that was created by PfT alumni and then went out to PCMI. It also makes explicit some of the mathematical results used in the creation of the problem sets. This part is written by people who were in on the design but were not involved in the day-to-day classes at PCMI. The areas treated in this overview include

In addition to the teachers participating in the course, PCMI hosts research programs in mathematics and education, programs for graduate students and undergraduate faculty, and institutes for staff development professionals. See `pcmi.ias.edu` for more details.

1. The use of formal algebra in number theory.
2. Summing over divisors and its connection to Dirichlet series.
3. The number of representations of an integer as the sum of two squares.

There are many more ideas that are introduced in the problem sets—concrete examples or applications of the highlighted machinery, different ways to understand some of the results, and connections to other related areas. These are described in more detail in the day-by-day facilitator notes.

One of the things that's unique about *FFNT* is how it motivates rather technical results through numerical experiments. For example, one of the main results is a beautiful theorem of Fermat:

> *Suitably counted, the number of ways a positive integer* n *can be written as a sum of two squares can be calculated by looking at all the positive divisors of* n*, ignoring the even ones, and taking the excess of the number of divisors of form* $4k+1$ *over those of form* $4k+3$*.*

The result is striking and surprising. What's more, the only proof we know uses some fairly advanced techniques from number theory (we sketch an outline of such a proof below). But, stepping back, how could the theorem even be conjectured? Certainly, one could look at data, but what would prompt someone to count divisors of form $4k+1$ and $4k+3$?

Why should the number of divisors that are 1 mod 4 be at least as large as the number that are 3 mod 4? That's a corollary to the theorem.

The instructors of *FFNT*, Bowen Kerins and Darryl Yong, devised an ingenious way to make the conjecture jump out of a numerical experiment. The approach uses several devices, developed slowly and experientially throughout the problem sets:

- Throughout the course, formal calculations with polynomials and power series are used to generate numerical data. In this case, calculations with polynomials and power series yields the values of the values of $s_2(n)$ where

  $$s_2(n) = \text{the number of ways } n \text{ can be written as a sum of two squares}$$

  The definition of s_2 is given precisely later in this overview.

- In a different thread of the *FFNT*, a notion is developed over several problem sets: a function f, defined on non-negative integers, is compiled in a certain way to produce another function g , called its "child". More precisely, $g(n)$ is the sum of the values of f over the divisors of n.

  The compilation is a special case of what's known as *Dirichlet convolution*.

- This compilation process can be reversed, so that a child produces a "parent." This produces, starting with a function f, a stream of functions—ancestors and descendants of f:

  $$\ldots \quad f_{-3} \leftarrow f_{-2} \leftarrow f_{-1} \leftarrow f_0 = f \leftarrow f_1 \leftarrow f_2 \leftarrow f_3 \leftarrow f_4 \quad \ldots$$

  Here, each f_i points to its parent. This parent-child relationship is discussed in great detail in [4].

The conjecture develops, through a series of assumptions and calculations:

1. Use a generating polynomial calculation to generate data for s_2. The values of $s_2(n)$ for $n > 0$ are all divisible by 4.
2. Calculate, one value at a time, the values of the parent for $S_2(n) = \frac{s_2(n)}{4}$. These values turn out to be, conjecturally, 0 if n is even, 1 if n is 1 mod 4, and -1 if n is 3 mod 4.
3. If this is true, then $S_2(n)$ is the sum over the divisors of n of this parent function, and this is exactly the excess of the number of $4k+1$ divisors over the

number of $4k + 3$ divisors. This is precisely the statement of Fermat's theorem on the sum of two squares.

The Kerins-Yong approach to making the statement of the theorem seem natural has all the features of a genuine mathematical investigation: experimental data is generated and analyzed, assumptions (lemmas, in fact) are stated and temporarily assumed (in order to see if they lead to interesting ideas), and precise language is used to help one frame a conjecture. The only missing piece is a proof that this all works. *FFNT* doesn't quite nail down a proof, but it provides participants with all of the necessary ingredients. After a discussion of the method leading up to the conjecture, we'll sketch out a proof here, pointing to the references for the complete details.

Children, Parents, and Dirichlet Series

This approach to conjecturing the result about sums of squares might seem natural, once one thinks of using the parent-child relationship, but this raises the question of why one would think about compiling over divisors in the first place.

One answer lies in the theory of Dirichlet series. Dirichlet introduced these series to answer combinatorial questions in number theory, and they have since found applications all over mathematics. A formal ***Dirichlet series*** is an expression of the form

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} = a(1) + \frac{a(2)}{2^s} + \frac{a(3)}{3^s} + \cdots,$$

where a is a function defined on positive integers taking values in the complex numbers.

A function $a : \mathbb{N} \to \mathbb{C}$ is sometimes called an ***arithmetic*** function.

The word "formal" is important here—just as in other parts of *FFNT*, we think of these series as bookkeeping devices keeping track of combinatorial or numerical data. So, we don't worry about questions of convergence. This misses many of the wonderful analytic applications of such series, but it turns out that the formal algebraic properties are all we need for this discussion.

. . . [to] omit those parts of the subject, however, is like listening to a stereo broadcast of, say, Beethoven's Ninth Symphony, using only the left audio channel. [9], p. vii.

Dirichlet series are added and multiplied formally. Addition is done term by term:

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} + \sum_{n=1}^{\infty} \frac{b(n)}{n^s} = \sum_{n=1}^{\infty} \frac{a(n) + b(n)}{n^s}.$$

Multiplication is also done term by term, but then one gathers up all terms with the same denominator. So, for example, if we're looking for $c(12)/12^s$ in

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} \sum_{n=1}^{\infty} \frac{b(n)}{n^s} = \sum_{n=1}^{\infty} \frac{c(n)}{n^s}, \tag{1}$$

then a denominator of 12^s could come only from the products

$$\frac{a(1)}{1^s}\cdot\frac{b(12)}{12^s}, \frac{a(2)}{2^s}\cdot\frac{b(6)}{6^s}, \frac{a(3)}{3^s}\cdot\frac{b(4)}{4^s}, \frac{a(4)}{4^s}\cdot\frac{b(3)}{3^s}, \frac{a(6)}{6^s}\cdot\frac{b(2)}{2^s}, \frac{a(12)}{12^s}\cdot\frac{b(1)}{1^s}.$$

In general, the coefficient $c(n)$ in equation (1) is given by

$$c(n) = \sum_{d|n} a(d) \cdot b\left(\frac{n}{d}\right), \tag{2}$$

where $\sum_{d|n}$ means that the sum is over the divisors of n.

The simplest Dirichlet series is the ***Riemann zeta function***:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Eq. (2) implies a result that we'll need later:

Theorem 4.1

$$\zeta(s) \sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \sum_{n=1}^{\infty} \frac{b(n)}{n^s},$$

then

$$b(n) = \sum_{d|n} a(d). \tag{3}$$

And so we see the appearance of a sum over the divisors.

If two functions a and b, defined on non-negative integers, are related as in Equation (3), we say that b is the ***child*** of a (and a is the ***parent*** of b).

Ways to Think About It

Many functions that arise in number theory are related by this parent-child connection. For example, if e is the identity function, $e(n) = n$, then e is the parent of σ, the *sum of the divisors* function:

$$\sigma(n) = \sum_{d|n} d$$

And e is the child of the *Euler totient function* ϕ defined by

$$\phi(n) = \text{the number positive of integers} \leqslant n \text{ that are relatively prime to } n$$

because it tuns out (See [6]) that:

So, $\phi \leftarrow e \leftarrow \sigma$.

$$n = e(n) = \sum_{d|n} \phi(d)$$

Sums of Two Squares

A question that runs through the problem sets is:

> *Which integers can be written as the sum of two (integer) squares*?

Participants develop some conjectures (some with proofs). For example, they conjecture that an odd prime can be written as a sum of two squares if and only if it is congruent to 1 mod 4. What about composite integers? For example, 15 can't be written as $a^2 + b^2$, but 65 can: $65 = 8^2 + 1^2$. In fact, 65 can be written as the sum of two squares in another way: $65 = 4^2 + 7^2$. This leads to a more refined question (open to experiment by high school students):

> *In how many ways can a positive integer be written as the sum of two squares*?

For example, 5 is a sum of two squares: $5 = 2^2 + 1^2$. But we could also write 5 in other related ways:

$$\begin{aligned} 5 &= 2^2 + 1^2 \\ &= 2^2 + (-1)^2 \\ &= (-2)^2 + (-1)^2 \\ &= (-2)^2 + 1^2 \\ &= 1^2 + 2^2 \\ &= 1^2 + (-2)^2 \\ &= (-1)^2 + (-2)^2 \\ &= (-1)^2 + 2^2. \end{aligned}$$

The course starts out with this counting method and calls the function that returns this count s_2. So, for example,

$$s_2(5) = 8, s_2(8) = 4, s_2(14) = 0, s(9) = 4, \text{ and } s_2(25) = 12$$

Ways to Think About It

If you tabulate s_2, you see that all the values all positive integers are divisible by 4. Essentially, $s_2(n)$ is the number of lattice points (points with integer coordinates) (a, b) in the plane so that $a^2 + b^2 = n$. If there is such a point in any quadrant, there will another such in each of the other three quadrants.

In later problem sets, attention turns to the function S_2 defined at positive integers by $S_2(n) = \frac{s_2(2)}{4}$. There are several reasons for this, besides the convenience of dividing out by the common factor of 4 in the tabulation. One is that, unlike s_2, S_2 is ***multiplicative***: $S_2(mn) = S_2(m)S_2(n)$ whenever m and n are relatively prime. Another has to do with arithmetic in the Gaussian integers $\mathbb{Z}[i]$, something we'll touch on briefly below (and see [5] for a detailed development).

Generating Functions

One of the themes in *FFNT* is the use of calculations with formal expressions to keep track of numerical data. A good example of this is perhaps the simplest one in the course: The coefficient of x^n in

$$(x + x^2 + x^3 + x^4 + x^5 + x^6)^k$$

is the number of ways you can roll a value of n if k dice are thrown.

Equivalently, it's the number of k-tuples of integers, each between 1 and 6, that sum to n.

On the surface, this seems a little amazing. The polynomial

$$x + x^2 + x^3 + x^4 + x^5 + x^6$$

is the generating function for the roll of one die: each of the integers between 1 and 6 can show up once, and no other integer can show up. When you square it, the coefficient of x^n is the number of ways n can be written as the sum of *two* integers between 1 and 6. And when you cube it, the coefficient of x^n is the number of ways n can be written as the sum of *three* integers between 1 and 6.

The reason that this works is because polynomial multiplication is tailor made for this kind of bookkeeping—it's the generalized distributive law. And counting, say, pairs of numbers between 1 and 6 that add to n involves exactly this kind of "each with each" calculation. So, there's a general principle here: if the coefficient of each x^n in a polynomial is the number of ways that n can be

represented by some function, the coefficient if x^n in the kth power of that polynomial is number of ways that the n can be written as a sum of k values of that function.

This can be made precise, but in *FFNT* the principle is developed informally through examples. One of the most striking is used, together with a CAS, to generate values of s_2. If you want to count the number of ways an integer n is the sum of two squares, take a polynomial in which the coefficient of x^n is the number of ways n can be written as *one* square and multiply it by itself.

For example, $9 = 3^2 = (-3)^2$.

But the number of ways a non-negative integer n can be written as a perfect square is

$$\begin{cases} 1 & \text{if } n = 0, \\ 0 & \text{if } n \text{ is not a perfect square, and} \\ 2 & \text{if } n \text{ is a perfect square} \end{cases}$$

So, if you want to look at s_2 for values between 0 and 49, build the polynomial

$$f(x) = 1 + 2x + 2x^4 + 2x^9 + 2x^{16} + 2x^{25} + 2x^{36} + 2x^{49}$$

The coefficient of x^n in $(f(x))^2$ for $0 \leqslant n \leqslant 49$ will be $s_2(n)$. And a CAS makes it easy to do the expansion; it reports the first fifty terms of $f(x)^2$:

Yes, a CAS helps reduce the computational overhead, but Jacobi calculated powers of this polynomial completely unplugged, around 1830. People had algebraic stamina back then.

$$\begin{aligned} &\cdots + 4x^{49} + 8x^{45} + 8x^{41} + 8x^{40} + 8x^{37} + 4x^{36} + 8x^{34} \\ &+ 4x^{32} + 8x^{29} + 8x^{26} + 12x^{25} + 8x^{20} + 4x^{18} + 8x^{17} + 4x^{16} \\ &+ 8x^{13} + 8x^{10} + 4x^9 + 4x^8 + 8x^5 + 4x^4 + 4x^2 + 4x + 1 \end{aligned}$$

Ways to Think About It

The degree of $(f(x))^2$ is 98, and, in fact, the coefficient of x^n will be $s_2(n)$ up to $n = 63$ (why?), but then for $n \geqslant 64$ the coefficients will no longer be the appropriate values of s_2. We'd need to include more terms in f—what we really want is a power series.

This method leads to a tabulation of s_2 at integers n between 1 and 50:

n	$s_2(n)$	n	$s_2(n)$	n	$s_2(n)$	n	$s_2(n)$	n	$s_2(n)$
1	4	11	0	21	0	31	0	41	8
2	4	12	0	22	0	32	4	42	0
3	0	13	8	23	0	33	0	43	0
4	4	14	0	24	0	34	8	44	0
5	8	15	0	25	12	35	0	45	8
6	0	16	4	26	8	36	4	46	0
7	0	17	8	27	0	37	8	47	0
8	4	18	4	28	0	38	0	48	0
9	4	19	0	29	8	39	0	49	4
10	8	20	8	30	0	40	8	50	12

The Conjecture

The main use of the generating polynomial for s_2 in *FFNT* is to create tables like the one above. Let $S_2 = \frac{s_2}{4}$, and denote the parent of S_2 by χ, so that for $n \geqslant 1$,

$$S_2(n) = \sum_{d|n} \chi(d)$$

This condition is essentially a recurrence, so that $S_2(n)$ can be calculated if one knows the $S_2(m)$ for $m \leqslant n$ (in fact for $m \mid n$). So, for example, one can calculate like this:

$$\begin{aligned}
1 &= S_2(1) &&= \chi(1) \\
&&&\text{so } \chi(1) = 1 \\
1 &= S_2(2) &&= \chi(1) + \chi(2) \\
&&&= 1 + \chi(2), \qquad \text{so } \chi(2) = 0 \\
0 &= S_2(3) &&= \chi(1) + \chi(3) \\
&&&= 1 + \chi(3), \qquad \text{so } \chi(3) = -1 \\
1 &= S_2(4) &&= \chi(1) + \chi(2) + \chi(4) \\
&&&= 1 + (-1) + \chi(4), \qquad \text{so } \chi(4) = 0 \\
2 &= S_2(5) &&= \chi(1) + \chi(5) \\
&&&= 1 + \chi(5), \qquad \text{so } \chi(5) = 1 \\
0 &= S_2(6) &&= \chi(1) + \chi(2) + \chi(3) + \chi(6) \\
&&&= 1 + 0 + (-1) + \chi(6), \qquad \text{so } \chi(6) = 0 \\
0 &= S_2(7) &&= \chi(1) + \chi(7) \\
&&&= 1 + \chi(7), \qquad \text{so } \chi(7) = -1
\end{aligned}$$

$$\begin{aligned} 1 &= S_2(8) &&= \chi(1) + \chi(2) + \chi(4) + \chi(8) \\ &&&= 1 + 0 + 0 + \chi(8), && \text{so } \chi(8) = 0 \end{aligned}$$

Continuing in this way, one can build up a table for χ from that of S_2. Along the way, conjectures arise about values of χ at, say, primes or even integers. The complete picture shows some clear regularity:

n	$S_2(n)$	$\chi(n)$
1	1	1
2	1	0
3	0	-1
4	1	0
5	2	1
6	0	0
7	0	-1
8	1	0
9	1	1
10	2	0

n	$S_2(n)$	$\chi(n)$
11	0	-1
12	0	0
13	2	1
14	0	0
15	0	-1
16	1	0
17	2	1
18	1	0
19	0	-1
20	2	0

n	$S_2(n)$	$\chi(n)$
21	0	1
22	0	0
23	0	-1
24	0	0
25	3	1
26	2	0
27	0	-1
28	0	0
29	2	1
30	0	0

n	$S_2(n)$	$\chi(n)$
31	0	-1
32	1	0
33	0	1
34	2	0
35	0	-1
36	1	0
37	2	1
38	0	0
39	0	-1
40	2	0

n	$S_2(n)$	$\chi(n)$
41	2	1
42	0	0
43	0	-1
44	0	0
45	2	1
46	0	0
47	0	-1
48	0	0
49	1	1
50	3	0

In the table, χ takes on values -1, 0, and 1. $\chi(n)$ is 0 if n is even, $\chi(n)$ is 1 if n is of form $4k+1$, and $\chi(n)$ is -1 if n is of the form $4k+3$. The evidence leads one to a conjecture:

Conjecture 4.1

If $\chi : \mathbb{N} \to \mathbb{C}$ *is defined by*

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

then

$$S_2(n) = \sum_{d|n} \chi(d) \qquad \blacksquare \qquad (4)$$

Note that the sum on the right-hand side of this equation is the excess of the number of divisors of n of the form $4k+1$ over those of form $4k+3$. Hence, if the conjecture is true, we have a theorem, due to Fermat:

Theorem 4.2 (tentative)
Notation as above, for n a positive integer, $S_2(n)$ is the excess of the number of divisors of n of the form $4k+1$ over those of form $4k+3$.

Note also that the left-hand side of Equation (4) is non-negative. Hence, if the theorem is true, there are, for any positive integer n, at least as many divisors that are 1 mod 4 as there are that are 3 mod 4.

The Proof

Theorem 4.2 is a corollary of Conjecture 4.3. And one proof of Conjecture 4.3 uses many of the ideas developed in *FFNT*. For example, one way to show that

$$S_2(n) = \sum_{d|n} \chi(d)$$

is to use Theorem 4.1 and to show that

$$\zeta(s) \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \sum_{n=1}^{\infty} \frac{S_2(n)}{n^s} \tag{5}$$

This looks like a good lead, but, in fact, Equation (5) just uses Theorem 4.1 to restate what we want to prove. It *is* useful, but only after we get some alternate formulas for S_2 and χ. A detailed development with complete proofs is in Chapter 8 of [5], but we give the main points here:

1. Multiplicative functions and the product expansion.

Some functions $a : \mathbb{C} \to \mathbb{C}$ have the property that they respect multiplication, in the sense that for positive integers m, n,

$$a(mn) = a(m)a(n)$$

Such functions are called ***multiplicative*** (or "strongly multiplicative"). Examples include $n \mapsto n^k$ and the function χ defined above (a fact that you can check). If a is multiplicative, there is a sum-to-product representation of the Dirichlet series $\sum_{n=1}^{\infty} \frac{a(n)}{n^s}$, a consequence of the fundamental theorem of arithmetic:

There are ***weakly multiplicitive*** functions, too. They satisfy $a(mn) = a(m)a(n)$ whenever m and n are relatively prime. We'll see that S_2 is weakly multiplicative.

Theorem 4.3

If a is multiplicative, the Dirichlet series

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s}$$

can be expressed as

$$\prod_p \left(\frac{1}{1 - \frac{a(p)}{p^s}} \right) \tag{6}$$

where the product is over all prime numbers p.

Proof.

Each factor in expression (6) is a geometric series:

To be rigorous, we should put some restrictions on the values of $a(k)$ to ensure that the series converges.

$$\begin{aligned} \frac{1}{1 - \frac{a(p)}{p^s}} &= 1 + \left(\frac{a(p)}{p^s} \right) + \left(\frac{a(p)}{p^s} \right)^2 + \left(\frac{a(p)}{p^s} \right)^3 + \dots \\ &= 1 + \left(\frac{a(p)}{p^s} \right) + \left(\frac{a(p^2)}{p^{2s}} \right) + \left(\frac{a(p^3)}{p^{3s}} \right) + \dots \end{aligned}$$

Multiply all these together (one for every prime) and you get the sum of every possible expression of the form:

$$\frac{a(p_1^{e_1}) a(p_2^{e_2}) \dots a(p_r^{e_r})}{p_1^{e_1 s} p_2^{e_2 s} \dots p_r^{e_r s}} = \frac{a(p_1^{e_1} p_2^{e_2} \dots p_r^{e_r})}{\left(p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}\right)^s}$$

Since every $n \in \mathbb{Z}$ can be written in one and only one way as a product of powers of primes, this is the same as the sum

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s}$$

■

As examples, we have

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(\frac{1}{1 - \frac{1}{p^s}} \right), \quad \text{and}$$

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \left(\frac{1}{1 - \frac{\chi(p)}{p^s}} \right)$$

So, we can express Conjecture 4.1 (via equation 5) as

Conjecture 4.2 (Conjecture 4.1, restated)

$$\prod_p \left(\frac{1}{1 - \frac{1}{p^s}} \right) \prod_p \left(\frac{1}{1 - \frac{\chi(p)}{p^s}} \right) = \sum_{n=1}^{\infty} \frac{S_2(n)}{n^s} \tag{7}$$

2. S_2 and Gaussian integers.

We're looking at the number of ways an integer can be expressed integrally as $a^2 + b^2$. If we move up to the complex numbers,

$$a^2 + b^2 = (a + bi)(a - bi).$$

So, for $n \geqslant 1$, $s_2(n)$ is the number of complex numbers z with integer real and imaginary parts such that $z\overline{z} = n$, and $S_2(n)$ is one fourth of this number.

If $z = a + bi$, $\overline{z} = a - bi$, the complex conjugate of z.

The function N defined on $\mathbb{C}$ by $N(z) = z\overline{z}$ is called the ***norm***, and it has some important properties:

1. If $z = a + bi$, $N(z) = N(\overline{z}) = a^2 + b^2$.
2. $N(z)$ is a non-negative real number, and $N(z) = 0$ if and only if $z = 0$.
3. N is multiplicative: $N(zw) = N(z)N(w)$ for all complex numbers z and w.

The proofs of these facts amount to generic calculations, and the details are in [5].

The complex numbers with integer real and imaginary parts form a ring $\mathbb{Z}[i]$ called the ring of ***Gaussian integers***. $\mathbb{Z}[i]$ shares many structural properties with the ordinary integers $\mathbb{Z}$: There's a division algorithm, a Euclidean algorithm, and unique factorization into primes.

$\mathbb{Z}[i]$ is the set of all lattice points in the complex plane.

Ways to Think About It

Unique factorization means that every element can be written as a product of prime elements in "essentially one way." In $\mathbb{Z}$, this means there's only one prime factorization of an integer if you ignore the order in which the factors are listed and the insertion of unit factors of 1 and -1. It's the same with $\mathbb{Z}[i]$, except there are more unit factors to consider: The only elements of $\mathbb{Z}[i]$ whose reciprocals are also in $\mathbb{Z}[i]$ a are 1, -1, i, and $-i$. So, a prime factorization of 2 in $\mathbb{Z}[i]$ is $(1 - i)^2$ because $1 - i$ is a prime in $\mathbb{Z}[i]$ and

$$2 = (-i)(1 - i)^2$$

Two Gaussian integers that are unit multiples of each other are called ***associates***.

Put another way, two Gaussian integers that are unit multiples of each other generate the same ideal in $\mathbb{Z}[i]$.

So, another way to think about $s_2(n)$ is *the number of Gaussian integers of norm* n. And, if we define the first quadrant Q_1 like this:

$$Q_1 = \{z = a + bi \in \mathbb{C} \mid a > 0, b \geqslant 0\},$$

we have another way to state the definition of S_2: $S_2(n)$ is the number of Gaussian integers in Q_1 with norm n. In

Note that we are excluding 0 from Q_1.

symbols,

$$S_2(n) = |\{z \in \mathbb{Z}[i] \mid N(z) = n \text{ and } z \in Q_1\}|$$

So, the right-hand side of Equation (5)

$$\sum_{n=1}^{\infty} \frac{S_2(n)}{n^s}$$

can be written in another way: Each term in the sum is a sum of unit fractions, and the number of such fractions is the number of Gaussian integers with given norm. For example, the $\frac{3}{25^s}$ comes from

$$\frac{1}{N(3+4i)} + \frac{1}{N(4+3i)} + \frac{1}{N(5+0i)}$$

Using this idea and the mutiplicitivity of N, we get a product formula for the right-hand side to Equation (5):

$$\sum_{n=1}^{\infty} \frac{S_2(n)}{n^s} = \sum_{\alpha \in Q_1} \frac{1}{(N(\alpha))^s}$$

The right side is called the ***Dedekind zeta function*** for $\mathbb{Z}[i]$.

$$= \prod_{\mathfrak{p} \in Q_1} \sum_{k=0}^{\infty} \frac{1}{\left((N(\mathfrak{p}))^k\right)^s} \quad \text{(use the fundamental theorem in } \mathbb{Z}[i]\text{)}$$

$$= \prod_{\mathfrak{p} \in Q_1} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}} \quad \text{(sum a geometric series)}$$

Here, the product is over all Gaussian primes in the first quadrant. This is another example of a calculation that is best understood by working it out.

Putting together the pieces, we get a form of Conjecture 4.1 that can be used to prove it:

Conjecture 4.3 (Conjecture 4.2, restated)

$$\prod_{p} \left(\frac{1}{1 - \frac{1}{p^s}}\right) \prod_{p} \left(\frac{1}{1 - \frac{\chi(p)}{p^s}}\right) = \prod_{\mathfrak{p} \in Q_1} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}} \qquad (8)$$

We've converted a conjecture about sums to a conjecture about products. The last step is to dig into the right-hand side in order to transform it into the left-hand side.

3. Law of decomposition.

One of the most beautiful aspects of the structure of $\mathbb{Z}[i]$ is the classification of its primes. Some ordinary primes like 5 are no longer primes in the Gaussian integers; they ***split*** into two distinct prime factors $(5 = (2+i)(2-i))$. Other primes like 7 stay prime (they are ***inert***) even when you look at them in this larger setting. And the prime 2 exhibits a special behavior called ***ramification***—it is essentially the square of $1-i$, because $2 = -i(1-i)^2$. And these are the only three kinds of decomposition when you move from $\mathbb{Z}$ to $\mathbb{Z}[i]$.

How can you tell how an ordinary prime will behave when you move up to $\mathbb{Z}[i]$. Remarkably, there's a simple test that can be carried out inside $\mathbb{Z}$ that will tell you exactly what happens. Here are the details, without proof (again, see [5] for details):

Theorem 4.4

Every prime p *in* $\mathbb{Z}$ *does one of three things when you move up to* $\mathbb{Z}[i]$*:*

- *It can* split *into two (conjugate) factors:*

$$p = \mathfrak{p}\overline{\mathfrak{p}}$$

The primes in $\mathbb{Z}[i]$ that enter into the decomposition of the prime p in $\mathbb{Z}$ are said to ***lie above*** p.

- *It can remain* inert*, staying prime in* $\mathbb{Z}[i]$*.*
- *It can* ramify *into the square of a prime in* $\mathbb{Z}[i]$*:*

$$p = \mathfrak{p}^2$$

Furthermore, we have the following decomposition law *to tell which is which:*

This theorem was generalized independently in the 1920s by Artin and Takagi.

- p *splits* $\Leftrightarrow p \equiv 1 \pmod 4$
- p *is inert* $\Leftrightarrow p \equiv 3 \pmod 4$
- p *ramifies* $\Leftrightarrow p = 2$

The decomposition law looks upstairs from $\mathbb{Z}$ to $\mathbb{Z}[i]$. We can also look downstairs from $\mathbb{Z}[i]$ to $\mathbb{Z}$, in a form that is especially useful for the next calculation:

Theorem 4.5

Every prime in Q_1 *lies above one of these:*

- *the prime 2. There's just one:* $1+i$*, and* $N(1+i) = 2$

- *a prime* $\mathfrak{p}$ *that is congruent to 1 mod 4. There are two for each such* $\mathfrak{p}$*—if*

$$\mathfrak{p} = \mathfrak{p}\,\overline{\mathfrak{p}},$$

then both $\mathfrak{p}$ *and* $\overline{\mathfrak{p}}$ *have an associate in* $\mathbb{Q}_1$ *(and they are different), and each has norm* $\mathfrak{p}$.

- *a prime* $\mathfrak{p}$ *that is congruent to 3 mod 4. There's only one such prime in* $\mathbb{Q}_1$*, because such a* $\mathfrak{p}$ *is inert, and* $N(\mathfrak{p}) = \mathfrak{p}^2$.

The decomposition law allows us to derive Equation (8)

4. The calculation.

Remember, we want to show that

$$\prod_{\mathfrak{p}} \left(\frac{1}{1-\frac{1}{\mathfrak{p}^s}}\right) \prod_{\mathfrak{p}} \left(\frac{1}{1-\frac{\chi(\mathfrak{p})}{\mathfrak{p}^s}}\right) = \prod_{\mathfrak{p}\in\mathbb{Q}_1} \frac{1}{1-\frac{1}{N(\mathfrak{p})^s}}$$

Using the results so far—especially the result of Theorem 4.5 and the facts that χ is 0 on even integers, the calculation goes like this:

$$\begin{aligned}
\prod_{z\in\mathbb{Q}_1} \frac{1}{1-\frac{1}{N(z)^s}} &= \frac{1}{1-\frac{1}{2^s}} \left(\prod_{p\equiv 1 \bmod 4} \frac{1}{1-\frac{1}{p^s}}\right)^2 \left(\prod_{p\equiv 3 \bmod 4} \frac{1}{1-\frac{1}{p^{2s}}}\right) \\
&= \frac{1}{1-\frac{1}{2^s}} \left(\prod_{p\equiv 1 \bmod 4} \frac{1}{1-\frac{1}{p^s}}\right)^2 \left(\prod_{p\equiv 3 \bmod 4} \frac{1}{1-\frac{1}{p^s}}\right) \left(\prod_{p\equiv 3 \bmod 4} \frac{1}{1+\frac{1}{p^s}}\right) \\
&= \frac{1}{1-\frac{1}{2^s}} \left(\prod_{p \text{ odd}} \frac{1}{1-\frac{1}{p^s}}\right) \left(\prod_{p\equiv 1 \bmod 4} \frac{1}{1-\frac{1}{p^s}}\right) \left(\prod_{p\equiv 3 \bmod 4} \frac{1}{1+\frac{1}{p^s}}\right) \\
&= \left(\prod_{p} \frac{1}{1-\frac{1}{p^s}}\right) \left(\prod_{p\equiv 1 \bmod 4} \frac{1}{1-\frac{\chi(p)}{p^s}}\right) \left(\prod_{p\equiv 3 \bmod 4} \frac{1}{1-\frac{\chi(p)}{p^s}}\right) \\
&= \left(\prod_{p} \frac{1}{1-\frac{1}{p^s}}\right) \left(\prod_{p} \frac{1}{1-\frac{\chi(p)}{p^s}}\right)
\end{aligned}$$

This establishes (granting all that we've assumed) Conjecture 4.3 and hence Fermat's Theorem 4.2.

Bonus Results and Further Results

Several results follow from Theorem 4.2. We've already mention one: Since

$$S_2(n) = \sum_{d|n} \chi(d)$$

and since the left-hand side is non-negative, so is the right-had side, and hence *every integer has at least as many divisors of form* $4k+1$ *as it has of form* $4k+3$.

Another result, one that is experimentally conjectured and proved in *FFNT* (and in many workshops we've been in with teachers) comes from a general result about multiplicative functions: The child of a multiplicative function is weakly multiplicative (see Chapter 1 of [2] for a proof). In particular, if m and n are relatively prime,

$$S_2(mn) = S_2(m)S_2(n)$$

This implies that we only need to look at values of S_2 at prime powers, and a beautiful formula for this (and a generalization to S_2's family tree) evolves in the problem sets.

If you tabulate S_2, the results seem to be erratic. When this happens, it's useful to look at its average value. Using s_2 rather than S_2, there's a beautiful result, due to Gauss and developed over the problem sets, that shows that

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} s_2(k) = \pi$$

Essentially, $\sum_{k=1}^{n} s_2(k)$ counts the lattice points (a,b) such that $a^2 + b^2 \leqslant n$. These are the lattice points on or interior to a circle of radius $\sqrt{n}$. For large n, this approximates the area of this circle, which is πn. The complete proof is in [1].

Finally, the same program is used in *FFNT* to conjecture a formula for $s_4(n)$, the number or ways an integer cane written as a sum of four squares. One uses the coefficients of

$$(1 + 2x + 2x^4 + 2x^9 + \dots)^4$$

to generate data and then, one by one, calculates the values of the parent function. The result again jumps out of

What about carrying out this program for the cube of the polynomial (and hence the representations as a sum of three squares)? Try it.

the calculations: $s_4(n)$ seems to be eight times the sum of the positive divisors of n that are not divisible by 4. See [3] for a proof.

Bibliography

[1] Andrews, G. *Number Theory*. Dover, New York, 1994.

[2] Apostol, T. *Analytic Number Theory*, Springer Verlag, New York, 1976.

[3] Berndt, B.C. *Number Theory in the Spirit of Ramanujan*, AMS, Providence, 2006.

[4] Cuoco, A. *Investigations in Algebra*, MIT Press, Cambridge MA, 1990.

[5] Cuoco, A., and Joseph J. Rotman. *Learning Modern Algebra*, MAA, Washington DC, 2013.

[6] Cuoco, A. "Searching for Möbius", College Mathematics Journal, 37:2, 148–153.

[7] EDC. *CME Project*. Pearson, Boston MA, 2013.

[8] Ireland, K. and Rosen, M. *A Classical Introduction to Modern Number Theory* Springer-Verlag, 1991.

[9] Wilf, H., *Generatingfunctionology*, Academic Press, New York, 1994.