Chapter 7 Notes

Greg Knapp

April 19, 2022

1 The Euler Phi Function

1.1 Intro

- From Euler's Theorem in last chapter, we know it will be to our benefit to be able to compute φ of some numbers
- The goal of this section is to be able to easily compute something like $\varphi(1001)$.
- As of now, our only way of computing $\varphi(1001)$ is to write down $(\mathbb{Z}\,/\,1001\mathbb{Z})^\times$
- So for each number less than 1001, we run the Euclidean algorithm to determine if that number is relatively prime to 1001 and at the end, we count up all the numbers that were
- That's a pretty bad algorithm for computing φ.
- It would be really nice if we had a good way of computing φ
- For some numbers, we do.
- For example, if p is prime, we know that $\varphi(p) = p - 1$ because every integer $1 \leqslant n < p$ satisfies $(n, p) = 1$
- We can use similar reasoning to compute $\varphi(p^a)$ where p is prime and $a \geqslant 1$.
- **Ex:** Compute $\varphi(9)$ and $\varphi(27)$. Conjecture a formula for $\varphi(3^a)$.
- If I look at the set $\mathbb{Z}\,/\,p^a\mathbb{Z} = \{0, 1, 2, \ldots, p^a - 1\}$, we can ask which of its elements are NOT relatively prime to p^a
- The elements which are not relatively prime to p^a are exactly $0, p, 2p, 3p, \ldots, kp$ where k is the greatest integer so that $kp \leqslant p^a - 1$, i.e. k is the greatest integer $\leqslant \frac{p^a-1}{p} = p^{a-1} - \frac{1}{p}$.
- Hence, $k = p^{a-1} - 1$, so there are p^{a-1} integers which are NOT relatively prime to p^a in $\mathbb{Z}\,/\,p^a\mathbb{Z}$.
- This means there are $p^a - p^{a-1}$ integers which ARE relatively prime to p^a in $\mathbb{Z}\,/\,p^a\mathbb{Z}$
- I.e. $\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1) = p^a(1 - \frac{1}{p})$
- A result that we get is that if we randomly choose an element of $\mathbb{Z}\,/\,p^a\mathbb{Z}$, the probability that we get a number relatively prime to p is $1 - \frac{1}{p}$ (this is independent of a!)

1.2 Multiplicativity

- Knowing how φ behaves on powers of primes is great, but there are a bunch of integers that aren't powers of primes.
- If you've seen abstract algebra before, I can motivate the following. If you haven't, this will seem unmotivated, but it will be just as true
- Sun-Tsu's Theorem states that if $n = p_1^{e_1} \cdots p_g^{e_g}$, then

$$\mathbb{Z}\Big/_{n\mathbb{Z}} \cong \mathbb{Z}\Big/_{p_1^{e_1}\mathbb{Z}} \times \cdots \times \mathbb{Z}\Big/_{p_g^{e_g}\mathbb{Z}}$$

- Apply unit groups everywhere and count, giving $\varphi(n) = \varphi(p_1^{e_1}) \cdots \varphi(p_g^{e_g})$
- This is the quick proof that φ is multiplicative.
- Here's another proof:
- **Thm:** If $m, n \in \mathbb{Z}_{>0}$ and $(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$
- Pf:
  - **Ex:** Here's a fact we're going to use a bunch: a number is relatively prime to mn if and only if it is relatively prime to m and relatively prime to n.
  - We already know that 0 isn't relatively prime to any number, so we'll exclude it from our argument
  - Consider the numbers from 1 through mn written as follows:

$$\begin{array}{ccccc} 1 & 1+m & 1+2m & \cdots & 1+(n-1)m \\ 2 & 2+m & 2+2m & \cdots & 2+(n-1)m \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ r & r+m & r+2m & \cdots & r+(n-1)m \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ m & 2m & 3m & \cdots & mn \end{array}$$

  - We want to count the number of entries in this table which are relatively prime to n
  - We do this argument in pieces:
  - Look at row 1. Its entries are all 1 mod m and hence, relatively prime to m.
  - Additionally, there are n entries in row 1 and since $(m, n) = 1$, those entries form a complete set of residues mod n (This is theorem 4.7, not 4.6 like your book says)
  - So in row 1, there must be $\varphi(n)$ entries relatively prime to n.
  - Since every entry in row 1 is relatively prime to m, there are $\varphi(n)$ entries in row 1 that are relatively prime to mn
  - Now lets look at row 2. If $(2, m) = 1$, then every element of row 2 is relatively prime to m.
  - We apply the same argument as above and find that there are $\varphi(n)$ elements of row 2 which are relatively prime to mn
  - IF $(2, m) > 1$, then every element of row 2 shares a factor with m and hence, is not relatively prime to mn, so there are 0 elements of row 2 which are relatively prime to mn.
  - Continue this argument in general: if $(r, m) = 1$, there are $\varphi(n)$ entries in row r relatively prime to mn. Otherwise there are 0
  - In total, there are $\varphi(m)$ rows which are prime to m, each containing $\varphi(n)$ entries relatively prime to mn
  - Hence, there are $\varphi(m)\varphi(n)$ numbers in this grid which are relatively prime to mn, i.e. $\varphi(mn) = \varphi(m)\varphi(n)$

- Stop and ask for questions
- Comprehension check: at which point(s) in the proof did we use the hypothesis that $(m, n) = 1$?
- Comprehension check: is it true for every m, n that $\varphi(mn) = \varphi(m)\varphi(n)$?
- Exploration: Are there any m, n with $(m, n) > 1$ and $\varphi(mn) = \varphi(m)\varphi(n)$?

1.3 Examples

- How does this help?
- **Ex:** Compute $\varphi(1001)$
  - $1001 = 7 \cdot 11 \cdot 13$ and since $(7, 11 \cdot 13) = 1$ and $(11, 13) = 1$, we can conclude that...

$$\varphi(1001) = \varphi(7 \cdot 11 \cdot 13) = \varphi(7) \cdot \varphi(11 \cdot 13) = 6 \cdot \varphi(11) \cdot \varphi(13) = 6 \cdot 10 \cdot 12 = 720$$

  - That's super nice that we're able to compute $\varphi(n)$ where the only complicating factor is factoring n We don't need to run the Euclidean algorithm around n times.
- More generally, suppose that n has $p_1^{e_1} \cdots p_g^{e_g}$ as its prime factorization
- Then

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \cdots \varphi(p_g^{e_g}) \\
&= p_1^{e_1-1}(p_1 - 1) \cdot p_2^{e_2-1}(p_2 - 1) \cdots p_g^{e_g-1}(p_g - 1) \\
&= p_1^{e_1}\left(1 - \frac{1}{p_1}\right) p_2^{e_2}\left(1 - \frac{1}{p_2}\right) \cdots p_g^{e_g}\left(1 - \frac{1}{p_g}\right) \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_g}\right)
\end{aligned}$$

- **Ex:** Compute $\varphi(36)$
  - $36 = 2^2 \cdot 3^2$, so $\varphi(36) = 36 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 12$
- Note: you may use the following results on the homework.
- **Ex:** For which positive integers n does $\varphi(n) = 1$?
  - First note that $n = 1$ works (by definition)
  - For $n > 1$, factor n into distinct primes: $n = p_1^{e_1} \cdots p_g^{e_g}$ for distinct primes p_i and $e_i > 0$
  - Then $1 = p_1^{e_1-1} \cdots p_g^{e_g-1}(p_1 - 1) \cdots (p_g - 1)$
  - Hence, all $e_i = 1$.
  - Moreover, each $p_i - 1 = 1$, i.e. there can only be one prime and it must be 2
- **Ex:** For which positive integers n does $\varphi(n) = 2$?
  - Again, $2 = p_1^{e_1-1} \cdots p_g^{e_g-1}(p_1 - 1) \cdots (p_g - 1)$
  - If $e_i > 1$ for some i, then $e_1 - 1 = 1$, so $e_i = 2$, $p_i = 2$ and there are no more primes
  - If all $e_i = 1$, then some $p_i - 1 = 2$, so $p_i = 3$
  - We could also have some $p_i = 2$.
  - This yields possible $n = 3$ or $n = 6$.
- **Ex:** For which positive integers n does $\varphi(n) = 3$?

- Note that $\varphi(n)$ is always either 1 or even.
- If n has an odd prime factor p, then $p-1 \mid \varphi(n)$, so $2 \mid \varphi(n)$
- Otherwise, $n = 2^k$ for some $k \geqslant 0$
- For $k = 0, 1$, $\varphi(n) = 1$
- For $k \geqslant 2$, $\varphi(n) = 2^{k-1}$ which is even.
- So no integer n has $\varphi(n) = 3$

1.4 A Weird Property

- If you're Euler and you have a lot of time on your hands, you might notice the following property of the φ function you just created
- **Thm:** Let n be a positive integer. Then

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

- **Ex:** Show that $\sum_{d|18} \varphi(d) = 18$
  - The divisors of 18 are: $1, 2, 3, 6, 9, 18$
  - $\varphi(1) = 1$
  - $\varphi(2) = 1$
  - $\varphi(3) = 2$
  - $\varphi(6) = 2$
  - $\varphi(9) = 6$
  - $\varphi(18) = 6$
  - Adding them up yields 18
- But why does that work?
- Note that every integer has $(x, 18)$ equal to one of $1, 2, 3, 6, 9, 18$ (i.e. the divisors of 18)
- Let's group the elements of $\mathbb{Z}/18\mathbb{Z}$ according to their gcd with 18
- Which elements of $\mathbb{Z}/18\mathbb{Z}$ have $(x, 18) = 1$? $x = 1, 5, 7, 11, 13, 17$
  - There are $\varphi(18)$ of them
- Which elements of $\mathbb{Z}/18\mathbb{Z}$ have $(x, 18) = 2$? $x = 2, 4, 8, 10, 14, 16$
  - Note that $(x, 18) = 2$ if and only if $\left(\frac{x}{2}, 9\right) = 1$
  - There are $\varphi(9)$ of them
  - Moreover, each $x/2$ gives the congruence classes mod 9 which are relatively prime to 9
- Which elements of $\mathbb{Z}/18\mathbb{Z}$ have $(x, 18) = 3$? $x = 3, 15$
  - Note that $(x, 18) = 3$ if and only if $\left(\frac{x}{3}, 6\right) = 1$
  - Moreover, each $x/3$ gives the congruence classes mod 6 which are relatively prime to 6
  - There are $\varphi(6)$ of them
- Which elements of $\mathbb{Z}/18\mathbb{Z}$ have $(x, 18) = 6$? $x = 6, 12$
  - Note that $(x, 18) = 6$ if and only if $\left(\frac{x}{6}, 18\right) = 1$
  - Moreover, each $x/6$ gives the congruence classes mod 3 which are relatively prime to 3

  - There are $\varphi(3)$ of them
- Which elements of $\mathbb{Z}/18\mathbb{Z}$ have $(x, 18) = 9$? $x = 9$
  - Note that $(x, 18) = 9$ if and only if $\left(\frac{x}{9}, 2\right) = 1$
  - Each $x/9$ gives the congruence classes mod 2 which are relatively prime to 2
  - There are $\varphi(2)$ of them
- Which elements of $\mathbb{Z}/18\mathbb{Z}$ have $(x, 18) = 18$? $x = 18$
  - Note that $(x, 18) = 18$ if and only if $\left(\frac{x}{18}, 1\right) =$, i.e. x is a multiple of 18
  - Each $x/18$ gives the congruence classes "mod 1" which are relatively prime to 1
  - There are $\varphi(1)$ of them
- How do we generalize this? Exactly the way you expect
- Proof of Weird Property
  - For each $d \mid n$, define $C_d := \{0 \leqslant x < n : (x, n) = d\}$
  - Since $(x, n) = d$ if and only if $\left(\frac{x}{d}, \frac{n}{d}\right) = 1$, we can write $C_d := \{0 \leqslant x < n : \left(\frac{x}{d}, \frac{n}{d}\right) = 1\}$
  - So $x \in C_d$ if and only if $0 \leqslant \frac{x}{d} < \frac{n}{d}$ and $\left(\frac{x}{d}, \frac{n}{d}\right) = 1$
  - There are $\varphi(\frac{n}{d})$ such elements, so $|C_d| = \varphi(n/d)$
  - The sets C_d are disjoint and together they have every element of $\mathbb{Z}/n\mathbb{Z}$
  - Hence,
$$n = \#\left(\mathbb{Z}\Big/_{n\mathbb{Z}}\right) = \#\bigcup_{d|n} C_d = \sum_{d|n} \#C_d = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi(n)$$

2 The Sum and Number of Divisors

2.1 Some Definitions

- Here were some notable properties of the Euler φ function
  1. $\varphi(mn) = \varphi(m)\varphi(n)$ when $(m, n) = 1$
  2. $\varphi(p^e)$ was easy to compute
- **Def:** An arithmetic function is a function defined for all positive integers
- **Def:** An arithmetic function, f, is called multiplicative if $f(mn) = f(m)f(n)$ whenever $(m, n) = 1$. The function f is called completely multiplicative if $f(mn) = f(m)f(n)$ for all positive integers m and n.
- In the last chapter we saw that φ is an arithmetic function. It is multiplicative, but not completely multiplicative.
- We're going to look at a few more multiplicative functions in this section.

2.2 σ and τ

- **Def:** Define the sum of divisors function, $\sigma : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ by $\sigma(n) = \sum_{d|n} d$
- **Def:** Define the number of divisors function, $\tau : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ by $\tau(n) = \sum_{d|n} 1 = \#\{d > 0 : d \mid n\}$
- **Ex:** We have

n	1	2	3	4	5	6
$\tau(n)$	1	2	2	3	2	4
$\sigma(n)$	1	3	4	7	6	12

- If you play with enough examples, you'll notice some patterns like this: $\sigma(6) = \sigma(2)\sigma(3)$ and $\tau(6) = \tau(2)\tau(3)$.
- Note however that $\sigma(4) \neq \sigma(2)\sigma(2)$ and $\tau(4) \neq \tau(2)\tau(2)$
- We could prove that σ and τ are multiplicative directly, but the proof of each fact is the same, just with different functions.
- Here's the more general theorem we're going to prove:
- **Thm:** Suppose that f is a multiplicative, arithmetic function. Then $F(n) = \sum_{d|n} f(d)$ is also multiplicative.
- Note that we use a little f and a big F here, just like in calculus.
- There's a reason for this—there's a meaningful sense in which F is kind of like an antiderivative for f.
- **Ex:** Here's a proof for $n = 36 = 4 \cdot 9$:

$$\begin{aligned}
F(36) &= f(1) + f(2) + f(3) + f(4) + f(6) + f(9) + f(12) + f(18) + f(36) \\
&= f(1)f(1) + f(2)f(1) + f(1)f(3) + f(4)f(1) + f(2)f(3) + f(1)f(9) + f(4)f(3) + f(2)f(9) + f(4)f(9) \\
&= f(1)f(1) + f(1)f(3)f(1)f(9) + f(2)f(1) + f(2)f(3) + f(2)f(9) + f(4)f(1) + f(4)f(3) + f(4)f(9) \\
&= f(1)(f(1) + f(3) + f(9)) + f(2)(f(1) + f(3) + f(9)) + f(4)(f(1) + f(3) + f(9)) \\
&= (f(1) + f(2) + f(4)) \cdot (f(1) + f(3) + f(9)) \\
&= F(4)F(9)
\end{aligned}$$

- Pf of theorem:
  - Suppose that $(m, n) = 1$.
  - We first note that if $d \mid mn$, then there exist $d_1 \mid m$ and $d_2 \mid n$ so that $d = d_1 d_2$ (namely, $d_1 = (d, m)$ and $d_2 = (d, n)$). FTA is the fastest way to see this
  - Then

$$F(mn) = \sum_{d|mn} f(d) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1)f(d_2) = \left(\sum_{d_1|m} f(d_1)\right)\left(\sum_{d_2|n} f(d_2)\right) = F(m)F(n)$$

- Now consider the functions $f(x) = x$ and $g(x) = 1$.
- f and g are both multiplicative.
- Note that $\sigma(n) = \sum_{d|n} d = \sum_{d|n} f(d)$ and $\tau(n) = \sum_{d|n} 1 = \sum_{d|n} g(d)$ and so both σ and τ are multiplicative
- Here's a silly way of seeing that $f(x) = x$ is multiplicative.

- Recall that we showed that $\varphi(n)$ is multiplicative and $n = \sum_{d|n} \varphi(d)$.
- Since φ is multiplicative, our theorem indicates that $F(n) = n$ is mulitplicative
- To actually compute σ and τ then, it suffices to compute them on prime powers
- Let p be prime and $e \geqslant 1$
- Then the divisors of p^e are $1, p, p^2, \ldots, p^e$.
- There are $e + 1$ such divisors, so $\tau(p^e) = e + 1$
- Moreover, $\sigma(p^e) = 1 + p + p^2 + \cdots + p^e = \frac{p^{e+1}-1}{p-1}$
- Finally, this allows us to conclude that:

$$\tau(p_1^{e_1} \cdots p_g^{e_g}) = (e_1 + 1) \cdots (e_g + 1)$$
$$\sigma(p_1^{e_1} \cdots p_g^{e_g}) = \frac{p_1^{e_1+1} - 1}{p_1 - 1} \cdots \frac{p_g^{e_g+1} - 1}{p_g - 1}$$

- **Ex:**

$$\tau(200) = \tau(2^3 \cdot 5^2) = (3 + 1)(2 + 1) = 12$$
$$\sigma(200) = \sigma(2^3)\sigma(5^2) = \frac{2^4 - 1}{2 - 1} \cdot \frac{5^3 - 1}{5 - 1} = 15 \cdot 31 = 465$$

3 Partitions

3.1 Introduction

- We want to talk about the number of ways to add up positive integers to get 10.
- For example, $10 = 4 + 6 = 5 + 5 = 2 + 2 + 6 = 1 + 1 + 1 + \cdots + 1$, etc.
- Okay, we want to do something slightly more general, but this is the basic idea.
- Why aren't we counting other things?
- Well, if we allowed ourselves any nonpositive integers, we'd get infinitely many ways to do it: $10 = 10 + 0 = 10 + 0 + 0 = 10 + 0 + 0 + 0 = \ldots$
- When are two different ways "the same?"
- When they're the same up to reordering
- E.g. $10 = 1 + 2 + 6 + 1 = 1 + 6 + 2 + 1$ are "the same"
- Note that we can write each partition uniquely if we put the summands in nonincreasing order: $10 = 6 + 2 + 1 + 1$
- These are the things that we want to count:
- **Def:** Given a positive integer n, a partition of n is a tuple $(\lambda_1, \ldots, \lambda_r)$ so that $\lambda_1, \ldots, \lambda_r \in \mathbb{Z}_{>0}$, $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_r$, and $n = \sum_{i=1}^{r} \lambda_i$. Each λ_i is called a part of the partition
- **Ex:** $(3, 1, 1)$ is a partition of 5 because all three conditions are met
- **Ex:** The partitions of 4 are: (4), $(3, 1)$, $(2, 2)$, $(2, 1, 1)$, $(1, 1, 1, 1)$
- **Def:** Define the function $p : \mathbb{N} \to \mathbb{Z}_{>0}$ by $p(0) = 1$ and for any $n > 0$, $p(n)$ is the number of partitions of n
- As with many things, the naive way of computing p is not the best way. However, it's kind of where you have to start.

3.2 Restricted Partitions and Notation

- Unfortunately, counting partitions is quite hard.
- It's easier to make progress when you only count partitions with certain properties
- E.g. How many partitions of 5 have only odd parts?
  - The partitions of 5 are $4+1$, $3+2$, $3+1+1$, $2+2+1$, $2+1+1+1$, $1+1+1+1+1$
  - The partitions with only odd parts are $3+1+1$ and $1+1+1+1+1$
  - So there are only two partitions of 5 with only odd parts
- This leads to a lot of notation.
- **Def:** Let $S \subseteq \mathbb{Z}_{>0}$ and $m \in \mathbb{Z}_{>0}$. Define

$$\begin{aligned} p_S(n) &= \text{ number of partitions of } n \text{ into parts from } S \\ p^D(n) &= \text{ number of partitions of } n \text{ into distinct parts} \\ p_m(n) &= \text{ number of partitions of } n \text{ into parts each } \geqslant m \end{aligned}$$

- We can even combine these pieces of notation in ways that I'll remind you of when we get there.
- We may even come up with more notation like $p(n \mid \text{conditions})$ to count the number of partitions of n subject to conditions, like $p(n \mid \text{no part appears more than once})$
- **Ex:** Let O denote the set of odd numbers and E the set of even numbers. Then

$$\begin{aligned} p_O(5) &= 2 \\ p_E(5) &= 0 \\ p^D(5) &= 2 \\ p_2(5) &= 1 \end{aligned}$$

- What comes after this is going to be a smorgasboard of techniques for how people count partitions and prove things about partitions.

3.3 Ferrers Diagrams

- **Def:** To a partition $\lambda_1 \geqslant \ldots \geqslant \lambda_k$, we define the Ferrers Diagram to have k rows of dots with row j having λ_j dots
- **Ex:** Do the Ferrers diagrams for the partitions $(4,4,2,1)$ and $(3,2,2,2,2)$ and whatever else might be helpful
- Note that the number being partitioned corresponds to the number of dots in the diagram
- The number of parts of the partition corresponds to the number of rows
- Because we require $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_k$, we see that the number of dots per row must be weakly decreasing
- **Q.** What corresponds to the number of columns?
- The largest part determines the number of columns.
- A useful concept for a Ferrers diagram is that of its conjugate
- Looking at the diagram for $(4,4,2,1)$, we might ask how many parts have size at least one?

- Well, 4, because there are 4 parts
- This corresponds to looking at the number of rows which have an entry in the left-most column
- How many parts have size at least 2?
- This corresponds to counting how many rows have dots in the second column, so 3
- How many parts have size at least 3?
- How many rows have a dot in the third column?
- 2
- How many parts have size at least 4?
- How many rows have a dot in the fourth column?
- 2
- How many parts have size at least 5?
- How many rows have a dot in the fifth column?
- 0
- Etc.
- Note that the numbers we collect this way (4,3,2,2) form a different partition of 11
- In fact, you might note that the Ferrers diagram for this new partition is the reflection of the old Ferrers diagram across the diagonal
- **Def:** Given a partition of n, $(\lambda_1, \ldots, \lambda_k)$, define the conjugate partition as follows: for each $1 \leqslant i \leqslant \lambda_1$, set $\lambda'_i = \#\{\lambda_j : \lambda_j \geqslant i\}$. The conjugate partition of n is the partition $(\lambda'_1, \ldots, \lambda'_{\lambda_1})$
- There's a theorem hidden in here. Namely, that the conjugate partition of $(\lambda_1, \ldots, \lambda_k)$ is another partition of n.
- Let's prove that, just to make sure that our definition is legal
- Pf:
  - We need to show two things: that $\sum_{i=1}^{\lambda_1} \lambda'_i = \sum_{j=1}^{k} \lambda_j$ and that $\lambda'_1 \geqslant \lambda'_2 \geqslant \cdots \geqslant \lambda'_{\lambda_1}$
  - For the first claim, we note that λ'_j counts the size of the jth column of the Ferrers diagram for $(\lambda_1, \ldots, \lambda_k)$
  - So the Ferrers diagram for $(\lambda_1, \ldots, \lambda_k)$ and $(\lambda'_1, \ldots, \lambda'_{\lambda_1})$ have interchanged rows and columns, hence the same number of dots
  - For the proof of the second claim, note that

    $$\{\lambda_j : \lambda_j \geqslant 1\} \supseteq \{\lambda_j : \lambda_j \geqslant 2\} \supseteq \cdots \supseteq \{\lambda_j : \lambda_j \geqslant \lambda_1\}$$

    implying that

    $$\lambda'_1 \geqslant \lambda'_2 \geqslant \cdots \geqslant \lambda'_{\lambda_1}$$
- Why does anyone care? It helps us prove things like:
- **Thm:** If n is a positive integer,

  $$p(n \mid \text{largest part } = r) = p(n \mid \text{exactly } r \text{ parts})$$
- Pf:

- Let S be the set of all partitions of n with exactly r parts
- Let T be the set of all partitions of n with largest part equal to r
- Note that for any $(\lambda_1, \ldots, \lambda_r) \in S$, the conjugate has largest part equal to r
- So we can define a map $c : S \to T$ by $(\lambda_1, \ldots, \lambda_r) \mapsto (\lambda'_1, \ldots, \lambda'_{\lambda_1})$
- Moreover, c maps T to S by $(r, \lambda_2, \ldots, \lambda_k) \mapsto (\lambda'_1, \ldots, \lambda'_r)$
- c is self-inverse because it is reflection on the Ferrers diagram and so it must be a bijection and hence $\#S = \#T$

- Which of these is easier to count? For humans, it depends on the context.
- **Ex:** Find the number of partitions of 10 with largest part equal to 2.
  - By the theorem, this is equal to the number of partitions of 10 with exactly 2 parts.
  - But these are

$$\begin{aligned} 10 &= 9 + 1 \\ &= 8 + 2 \\ &= 7 + 3 \\ &= 6 + 4 \\ &= 5 + 5 \end{aligned}$$

  - So there must be 5 partitions of 10 with largest part equal to 2.
  - If we wanted to write them out, they would be...

$$\begin{aligned} 10 &= 2 + 2 + 2 + 2 + 2 \\ &= 2 + 2 + 2 + 2 + 1 + 1 \\ &= 2 + 2 + 2 + 1 + 1 + 1 + 1 \\ &= 2 + 2 + 1 + 1 + 1 + 1 + 1 + 1 \\ &= 2 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 \\ &= 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 \end{aligned}$$

- **Ex:** Find the number of partitions of 100 with largest part equal to 5.
  - We know that our partition has to look like $100 = 5 + \text{stuff}$
  - So $95 = \text{stuff}$.
  - I.e. "stuff" has to be a partition of 95 with largest part less than or equal to 5.
  - Let's say 5 is the largest part.
  - Then we need a partition of 90 with largest part less than or equal to 5.
- In any case, we have a pretty clear algorithm for how to construct these

3.4 Generating Functions

3.4.1 Motivation

- Lets recall the binomial formula: $(x+1)^n = \sum_{i=0}^{n} \binom{n}{i} x^n$
- Where does this formula come from?
- We write out $(x+1)^n = (x+1)(x+1)\cdots(x+1)$.
- How many ways are there of getting x^n? Just one

- This is why we have 1 as the coefficient on x^n in the expansion
- How many ways are there of getting x^{n-1}?
- n ways because we have to pick $n-1$ copies of x and 1 copy of 1
- More generally, to get x^i, we have to count the number of ways to pick i copies of x from a set of n
- I.e. the coefficient will be $\binom{x}{i}$
- This is how coefficients of polynomials can contain "counting" information
- However, the factored form is much easier to deal with when working with plugging things in, or proving identities.
- For example, note that

$$\sum_{i=0}^{n} \binom{n}{i} x^n y^{n-i} = (x+y)^n = (y+x)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^n = \sum_{i=0}^{n} \binom{n}{n-i} x^n y^{n-i}$$

  and we immediately have a proof that $\binom{n}{i} = \binom{n}{n-i}$
- There are other proofs of course, but polynomials and their coefficients can provide us with proofs of facts, even if those proofs don't tell you much about what's going on
- Now if we want to learn something about an infinite sequence, a polynomial won't be exactly the right tool.

3.4.2 Philosophy

- Generating functions are a hugely useful concept in number theory and combinatorics
- The idea is that we can represent combinatorial objects (like sequences) as algebraic/analytic objects, then do algebra/analysis to prove things about them
- For generating functions, we're taking a sequence, and representing it via a power series.
- For example, start with the sequence $1, 2, 4, 8, \ldots$
- The generating function for that sequence is $1 + 2x + 4x^2 + 8x^2 + \cdots$
- First, recognize that

$$1 + 2x + 4x^2 + 8x^3 + \cdots = \sum_{n=0}^{\infty} 2^n x^n = \sum_{n=0}^{\infty} (2x)^n = \frac{1}{1-2x}$$

  when $|x| < 1/2$
- And now, since we know things about taylor series, we can do analysis to determine things like the growth rate of 2^n
- Of course, this is silly, because we already know all that there is to know about the sequence 2^n
- But there are a lot of sequences that we know a lot less about.
- **Def:** For a sequence $\{a_n\}_{n=0}^{\infty}$, the <u>generating function</u> for $\{a_n\}_{n\in\mathbb{N}}$ is

$$\sum_{n\in\mathbb{N}} a_n x^n$$

- **Ex:** The generating function for $p(n)$ is

$$\sum_{n\in\mathbb{N}} p(n)x^n = p(0) + p(1)x + p(2)x^2 + p(3)x^3 + \cdots = 1 + x + 2x^2 + 3x^3 + 5x^4 + \cdots$$

- **Thm:** The generating function for $p(n)$ equals

$$\prod_{j=1}^{\infty} \frac{1}{1-x^j} = \frac{1}{1-x} \cdot \frac{1}{1-x^2} \cdot \frac{1}{1-x^3} \cdots$$

- We're not going to worry about convergence very much and we're going to treat this as a purely algebraic problem
- If you know things about convergence though, you'll know that the usual algebraic rules don't always apply when convergence gets icky.

3.4.3 Generating Functions for Partition Functions

- For example: for any real number x, there exists a way to rearrange the terms of the sequence $\{a_n\}_{n\geqslant 1} = \{(-1)^n/n\}_{n\geqslant 1}$ so that $\sum_{n=1}^{\infty} a_n$ converges to x...
- So the fact that we're ignoring convergence here is something that needs justified, we're just not going to do it
- Pf of thm:
  - Recall that $\frac{1}{1-x} = 1 + x + x^2 + \cdots$
  - So $\frac{1}{1-x^j} = 1 + x^j + x^{2j} + x^{3j} + \cdots$
  - Hence

$$\prod_{j=1}^{\infty} \frac{1}{1-x^j} = \prod_{j=1}^{\infty} (1+x^j+x^{2j}+x^{3j}+\cdots) = (1+x+x^2+x^3+\cdots)(1+x^2+x^4+x^6+\cdots)(1+x^3+x^6+x^9+\cdots)\cdots$$

  - We want to convert this infinite product into a power series by expanding polynomials "like usual"
  - Starting with the constant term, it definitely has to be 1.
  - For the linear term, note again that there's only one way to get it: x^1 from the first term and x^0 from all the other terms
  - For the quadratic term, note that there are two ways to get it: x^2 from the first and x^0 from the rest OR x^0 from the first, x^2 from the second, and x^0 from the rest
  - For the cubic term, we have three ways: x^3 from the first and x^0 from the rest, x from the first and x^2 from the second and x^0 from the rest, and x^0 from the first two and x^3 from the third and x^0 from the rest
  - The idea here is to think about the exponent in the first term of the product as the "number of ones" in a partition of n
  - The exponent in the second term counts the "number of twos" in a partition
  - And so on
  - So the number of ways to get n as an exponent is the number of partitions of n.
- Here's another example/theorem
- **Thm:** The generating function for $p^D(n)$ (the number of partitions of n into distinct parts) equals

$$\sum_{n\in\mathbb{N}} p^D(n)x^n = \prod_{j=1}^{\infty} (1 + x^j)$$

- "Proof:"
  - Consider $(1+x)(1+x^2)(1+x^3)(1+x^4)\cdots$
  - The only way to get x^0 is by picking all 1s
  - The only way to get x^1 is by picking x, then all 1s
  - The only way to get x^2 is by picking 1, then x^2, then all 1s
  - Two ways of getting x^3: Take x, x^2, then all 1s OR take 1, 1, x^3, and all 1s
  - These correspond to $3 = 3 = 2 + 1$
  - Two ways of getting x^4: x^4 and all 1s OR x^3 and x and all 1s
  - More generally, how many ways of getting x^n?
  - Number of partitions into distinct parts: $p^D(n)$
- More generally, if we want to only worry about parts that live in some set $S \subseteq \mathbb{N}$, it turns out that the generating functions for $p_S(n)$ and $p_S^D(n)$ are

$$\sum_{n\in\mathbb{N}} p_S(n)x^n = \prod_{j\in S} \frac{1}{1-x^j}$$
$$\sum_{n\in\mathbb{N}} p_S^D(n)x^n = \prod_{j\in S} (1+x^j)$$

- Now, let's actually see how generating functions can be helpful
- **Thm:** (Euler Parity) For any positive integer n, $p_O(n) = p^D(n)$. I.e. the number of partitions of n into odd parts is equal to the number of partitions of n into distinct parts.
- Pf:
  - Let's look at the generating functions for these two partition functions:

$$\sum_{n\in\mathbb{N}} p^D(n)x^n = \prod_{i=1}^{\infty}(1+x^i)$$
$$\sum_{n\in\mathbb{N}} p_O(n)x^n = \prod_{j\in O} \frac{1}{1-x^j} = \prod_{i=1}^{\infty} \frac{1}{1-x^{2i-1}}$$

  - First observe that we can manipulate the generating function for distinct partitions so that

$$\prod_{i=1}^{\infty}(1+x^i) = \prod_{i=1}^{\infty} \frac{1-x^{2i}}{1-x^i}$$

  - But now take a look at what happens in the manipulated product:

$$\sum_{n\in\mathbb{N}} p^D(n)x^n = \prod_{i=1}^{\infty}(1+x^i) = \prod_{i=1}^{\infty} \frac{1-x^{2i}}{1-x^i} = \frac{1-x^2}{1-x}\cdot\frac{1-x^4}{1-x^2}\cdot\frac{1-x^6}{1-x^3}\cdot\frac{1-x^8}{1-x^4}\cdots = \prod_{i=1}^{\infty} \frac{1}{1-x^{2i-1}} = \sum_{n\in\mathbb{N}} p_O(n)x^n$$

  - Now since $p_O(n)$ and $p^D(n)$ have the same generating function, they must be the same function.
- Weird! Notice that this proof doesn't tell you anything about how partitions with odd parts and partitions with distinct parts relate.
- But it tells you that they are the same number
- These types of arguments can sometimes serve as proofs (when the analytic stuff works out), but even when they can't, they serve as motivation to find a bijection
- For instance, now that we know that $p_O(n) = p^D(n)$, we might be motivated to try to find a bijection between partitions with odd parts and partitions with distinct parts.

3.4.4 Euler's Pentagonal Number Theorem

- We have this result from the previous section that

$$f(x) = \sum_{n=0}^{\infty} p(n)x^n = \prod_{j=1}^{\infty} \frac{1}{1-x^j}$$

- A good question to ask is the following: what power series do we need to multiply $f(x)$ by to get 1?
- There's a question of why such a thing should exist in the first place and there's also a question of why we would care about finding such a thing.
- The answer to the first question is...
  - ...The constant term of $f(x)$ is 1, so it's invertible in $\mathbb{Z}[\![x]\!]$
  - $$\frac{1}{f(x)} = \prod_{j=1}^{\infty}(1-x^j)$$

    which is definitely a power series
- Also note that $\prod_{j=1}^{\infty}(1+x^j)$ was the generating function for "number of partitions of n into distinct parts" so maybe the inverse of f also carries some combinatorial information.
- **Thm:** We have

$$\prod_{j=1}^{\infty}(1-x^j) = \sum_{n\in\mathbb{N}} a_n x^n$$

  where $a_n = p(n \mid \text{even number of distinct parts}) - p(n \mid \text{odd number of distinct parts})$
- Proof:
  - Expand out the product

$$\prod_{j=1}^{\infty}(1-x^j) = (1-x)(1-x^2)(1-x^3)\cdots = 1 - x - x^2 + x^3 - x^3 + x^4 - x^4 - x^5 + x^5 + x^5 - \cdots$$

  - Instead of every partition with distinct parts counting towards the coefficients of the expansion, we get every partition with an even number of distinct parts counting towards the coefficient and every partition with an odd number of distinct parts counting against the coefficient
  - This is what we want
- If we look a little closer though, we might notice a pattern: sometimes the coefficients are 0, 1, or -1, but we don't see any other numbers showing up.
- **Q.** How are the number of partitions of n with an odd number of distinct parts related to the number of partitions of n with an even number of distinct parts?
- You can prove this with generating functions, but there's also a cute argument that gives a near-bijection
- **Thm:** The number of partitions of n into an odd number of distinct parts equals the number of partitions of n into an even number of distinct parts unless $n = \frac{k(3k\pm1)}{2}$ for some positive integer k. In the latter case,

$$p(n \mid \text{even number of distinct parts}) - p(n \mid \text{odd number of distinct parts}) = (-1)^k$$

- "Proof:" (bad proof to give in a lecture—give proof only if time)

- Here's a procedure that can be done with most Ferrers diagrams *with distinct parts*
- The goal is to produce a new partition with distinct parts, but reverse the parity of the number of parts (i.e. odd number of parts to even number of parts or vice versa)
- Let B be the last row of a Ferrers diagram and suppose it has b dots
- Let D be the "diagonal" of the Ferrers diagram starting in the upper right corner and proceeding for as long as each row has exactly one more dot than the row above it. Suppose that D has d dots.
- SUPPOSE THAT B AND D HAVE NO DOTS IN COMMON <u>OR</u> $b \neq d, d+1$
- Depending on the size of b relative to d, we're going to alter our Ferrers diagram to get a new one
- <u>Case 1:</u> $b \leqslant d$
  - In this case, we're going to take B and place it to the right of D so that one dot gets added to each of the top rows
  - If B and D have no common dots, this isn't a problem.
  - Also, if $b < d$, this isn't a problem (even if B and D have common dots)
  - We get distinct rows because each of the top k rows was already distinct
- <u>Case 2:</u> $b > d$
  - In this case, we're going to take D and place it below B.
  - If B and D have no dots in common this again isn't a problem and moreover, we get distinct rows
  - If $b > d+1$ this again isn't a problem and again we get distinct rows
- This procedure maps

$$\{\text{partitions with an even number of distinct parts where } B \cap D = \varnothing \text{ or } b \neq d, d+1\}$$
$$\to \{\text{partitions with an odd number of distinct parts where } B \cap D = \varnothing \text{ or } b \neq d, d+1\}$$

- The above claim requires a lot of detailed checking.
- Some more detailed checking shows that this procedure is its own inverse (show that if B', D', b', d' are the bottom row and diagonal of the output of this procedure, then $b \leqslant d \leftrightarrow b' > d'$)
- Hence,

$$\{\text{partitions with an even number of distinct parts where } B \cap D = \varnothing \text{ or } b \neq d, d+1\}$$
$$\to \{\text{partitions with an odd number of distinct parts where } B \cap D = \varnothing \text{ or } b \neq d, d+1\}$$

  is a bijection
- So to count the difference

$$p(n \mid \text{even number of distinct parts}) - p(n \mid \text{odd number of distinct parts})$$

  it suffices to count

$$p(n \mid \text{even number of distinct parts where } B \cap D \neq \varnothing \text{ and } b = d \text{ or } b = d+1)$$
$$- p(n \mid \text{odd number of distinct parts where } B \cap D \neq \varnothing \text{ and } b = d \text{ or } b = d+1)$$

- Note that n has a partition with Ferrers diagram with $B \cap D \neq \varnothing$ and $b = d$ if and only if there are d rows, the smallest of which has d dots, and each row has one more dot than the row above it

– In that case,

$$\begin{aligned} n &= d + (d+1) + \cdots + (2d-1) \\ &= \sum_{k=1}^{2d-1} k - \sum_{k=1}^{d-1} k \\ &= \frac{(2d-1)\cdot 2d}{2} - \frac{d(d-1)}{2} \\ &= \frac{4d^2 - 2d - d^2 + d}{2} \\ &= \frac{d(3d-1)}{2} \end{aligned}$$

– Note that n has a partition with Ferrers diagram with $B \cap D \neq \varnothing$ and $b = d+1$ if and only if there are d rows, the smallest of which has $d+1$ does and each row has one more dot than the row above it. In that case,

$$\begin{aligned} n &= (d+1) + (d+2) + \cdots + 2d \\ &= d + (d + (d+1) + \cdots + (2d-1)) \\ &= d + \frac{d(3d-1)}{2} \\ &= \frac{d(3d+1)}{2} \end{aligned}$$

– Each of these n values has only possibly one problematic Ferrers diagram which has d rows.

– So if $n = \frac{d(3d\pm 1)}{2}$, then

$$\begin{aligned} &p(n \mid \text{even number of distinct parts}) - p(n \mid \text{odd number of distinct parts}) = \\ &\quad = p(n \mid \text{even number of distinct parts where } B \cap D \neq \varnothing \text{ and } b = d \text{ or } b = d+1) \\ &\qquad - p(n \mid \text{odd number of distinct parts where } B \cap D \neq \varnothing \text{ and } b = d \text{ or } b = d+1) \\ &\quad = \begin{cases} 1 & d \text{ even} \\ -1 & d \text{ odd} \end{cases} \\ &\quad = (-1)^d \end{aligned}$$

– Otherwise, we get 0

- That's a rough proof (and to think that it's much simpler than Euler's original proof!)
- We get a nice corollary though:

$$\prod_{j=1}^{\infty}(1-x^j) = 1 + \sum_{n=1}^{\infty}(-1)^n x^{n(3n-1)/2}(1+x^n)$$

- Proof:

– We already showed that

$$\prod_{j=1}^{\infty}(1-x^j) = \sum_{n=1}^{\infty} a_n x^n$$

where

$$a_n = p(n \mid \text{even number of distinct parts}) - p(n \mid \text{odd number of distinct parts})$$

– But now we know that

$$a_n = \begin{cases} (-1)^d & n = \frac{(3d\pm 1)d}{2} \\ 0 & \text{else} \end{cases}$$

and so we're going to skip all the terms that aren't indexed by an n of the form $\frac{(3d\pm 1)d}{2}$

– The way we do that is with

$$\sum_{n=1}^{\infty}(-1)^n x^{n(3n-1)/2} + (-1)^n x^{n(3n+1)/2} = \sum_{n=1}^{\infty}(-1)^n x^{n(3n-1)/2}(1+x^n)$$

- From this, we note that

$$\begin{aligned} 1 &= \prod_{j=1}^{\infty}\frac{1}{1-x^j}\prod_{j=1}^{\infty}(1-x^j) \\ &= \left(\sum_{n\in\mathbb{N}} p(n)x^n\right)\left(1+\sum_{n=1}^{\infty}(-1)^n x^{(3n-1)n/2}(1+x^n)\right) \end{aligned}$$

- Because these are the same generating function, they must have the same coefficients (this requires work to check!)
- We have

$$\begin{aligned} 1 &= (p(0)+p(1)x+p(2)x^2+\cdots)(1+(-x)(1+x)+(x^5)(1+x^2)+(-x^{12})(1+x^3)+\cdots) \\ &= (p(0)+p(1)x+p(2)x^2+p(3)x^3+p(4)x^4+\cdots)(1-x-x^2+x^5+x^7-x^{12}-x^{15}+\cdots) \end{aligned}$$

- So the constant term on the RHS must be 1, i.e. $p(0) = 1$. Check.
- The linear coefficent on the RHS must be 0, i.e.

$$0 = p(1)\cdot 1 - p(0)\cdot 1$$

so $p(1) = p(0)$.

- The quadratic coefficient on the RHS must be 0, i.e.

$$0 = p(2) - p(1) - p(0)$$

so $p(2) = p(0) + p(1)$. check.

- We also get

$$\begin{aligned} 0 &= p(3) - p(2) - p(1) \\ 0 &= p(4) - p(3) - p(2) \\ 0 &= p(5) - p(4) - p(3) + p(0) \\ 0 &= p(6) - p(5) - p(4) + p(1) \\ 0 &= p(7) - p(6) - p(5) + p(2) + p(0) \\ &\vdots \\ 0 &= p(n) - p(n-1) - p(n-2) + p(n-5) + p(n-7) - \cdots + (-1)^k p(n - \frac{k(3k-1)}{2}) + (-1)^k p(n - \frac{k(3k+1)}{2}) + \cdots \end{aligned}$$

- so we get a recursive relationship

$$p(n) = p(n-1)+p(n-2)-p(n-5)-p(n-7)+\cdots+(-1)^{k-1}p\left(n-\frac{k(3k-1)}{2}\right)+(-1)^{k-1}p\left(n-\frac{k(3k+1)}{2}\right)+\cdots$$

- This formula is known as Euler's Partition Formula and is still the most efficient known way to compute $p(n)$.

3.5 Ramanujan's Contributions

- The mathematician Ramanujan made huge progress in partition theory in the early-mid-20th-century
- Here's a summary of some cool facts that he discovered:
  - $p(5k+4) \equiv 0 \mod 5$
  - $p(7k+5) \equiv 0 \mod 7$
  - $p(11k+6) \equiv 0 \mod 11$
- As a consequence, congruences of the form $p(ak+b) \equiv 0 \mod m$ are called Ramanujan congruences
- In 2000, Ono showed that form every prime q, there is a congruence of the form $p(ak+b) \equiv 0 \mod q$ (uses modular forms!)
- A second major contribution is Ramanujan's discovery of a few other type of partition identities:
- **Thm:** (First Rogers-Ramanujan Identity): If n is a positive integer, then the number of partitions of n into parts differing by at least 2 equals the number of partitions of n into parts congruent to 1 or 4 mod 5.
- **Thm:** (Second Rogers-Ramanujan Idenity): IF n is a positive integer, then the number of partitions of n that have parts (all of which are at least 2) that differ by at least 2 equals the number of partitions of n into parts congruent to 2 or 3 mod 5.
- Similar types of results remain an active area of research in combinatorics/number theory.