

Contents

1	Induction	1
1.1	Template and Weak Induction	1
1.2	Strong Induction	2
2	Number Theory	3
2.1	Definitions	3
2.2	Properties of Congruence Relations:	3
2.3	GCD	3
2.4	Multiplicative Inverse	3
2.5	Fermat's <small>little</small> Theorem	4
2.6	Euler's Totient Function	4
3	Counting	5
3.1	Product Rule and Permutations	5
3.2	Binomial Coefficients and Theorem	5
3.3	Counting Arguments	5
3.4	Inclusion/Exclusion Formula	6
3.5	Counting Donuts	6
3.6	Pigeonhole Principle	7

1 Induction

1.1 Template and Weak Induction

Induction is a proof method for which we can assume some n case, and prove that every $n + 1$ case holds. If we can prove that the $n + 1$ case holds, we can confirm that our original claim holds for all values of n in the desired domain..

Idea: If you are stuck on an induction problem on the exam, start by writing out the inductive hypothesis and the structure of the proof. You will receive partial credit for this and it will also help you think of how to proceed.

*Idea: Often the inductive step is a direct proof using the inductive hypothesis. This is not always the case; sometimes you might have to use **proof by cases** or even **contradiction**.*

We will first provide a review of the template for an inductive proof and provide an example.

Example

For example, say we are trying to prove that $\sum_{i=0}^n i = \frac{n(n+1)}{2}$ is true for all $n \in \mathbb{N}$.

1. Define the predicate $P(n)$.

Let $P(n)$ be the predicate that $\sum_{i=0}^n i = \frac{n(n+1)}{2}$.

2. Show that the base case is true.

We will first show $P(0)$ is true. $\sum_{i=0}^0 i = 0$ and $\frac{0(0+1)}{2} = 0$ so they are equal as needed.

3. Assume the inductive hypothesis is true. If you are using standard induction then you will assume $P(k)$ is true for some integer k . If you are using strong induction then you will assume $P(i)$ is true for all $i \leq k$. Either way, you should specify that k is some integer greater than or equal to your greatest base case.

Assume $P(k)$ is true for some arbitrary integer $k \geq 0$.

4. Show that $P(k + 1)$ is true given the inductive hypothesis.

We will now show that $\sum_{i=0}^{k+1} i = \frac{(k+1)(k+2)}{2}$.

We know that $\sum_{i=0}^{k+1} i = \left(\sum_{i=0}^k i\right) + (k + 1)$.

By our inductive hypothesis $\sum_{i=0}^k i = \frac{k(k+1)}{2}$.

Therefore

$$\begin{aligned}\sum_{i=0}^{k+1} i &= \left(\sum_{i=0}^k i \right) + (k+1) \\ &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k(k+1) + 2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2}\end{aligned}$$

as needed. □

5. Conclude the proof.

Therefore, as $P(0)$ is true and $P(k)$ implies $P(k+1)$ for all $k \in \mathbb{Z}$, $k \geq 0$, $P(n)$ is true for all nonnegative integers n .

More generally, our induction doesn't have to start from 0 but can start from any $n_0 \geq 0$. In particular, induction still works if our goal is to show $\forall n \geq n_0$ $p(n)$ where here this quantification is over all natural numbers at least n_0 .

1.2 Strong Induction

The difference in approach between weak and strong induction comes in the induction hypothesis! In weak induction, we only assume that the predicate holds for some arbitrary step k , while in strong induction, we assume that the predicate holds at all steps from the base case to some arbitrary step k . Your inductive step may differ depending on whether you approach a problem using weak or strong induction, but they are equivalent!

Why would we need to do that? Sometimes, you can't just rely on the fact that $P(k)$ is true. Maybe you also need $P(k-1)$ to be true, or perhaps also $P(k-2)$, or even $P(k/2)$. While writing out your inductive step, if you realize that $P(k)$ isn't enough to prove $P(k+1)$, odds are, you need strong induction.

2 Number Theory

Number theory is the study of the integers. For this section, all numbers are integers.

2.1 Definitions

Definition 1: We say that a divides b , denoted $a \mid b$, when $b = ka$ for some $k \in \mathbb{Z}$.

Definition 2: We say that a is congruent to $b \pmod{m}$, denoted $a \equiv b \pmod{m}$, if $m \mid (b - a)$. Another way to say this is that $a = b + km$ for some $k \in \mathbb{Z}$. Yet another way to say this: a and b have the same remainder upon division by m . Take a moment to convince yourself that these statements are equivalent.

2.2 Properties of Congruence Relations:

For $a, b \in \mathbb{Z}$, if $a \equiv b \pmod{m}$,

1. $a + c \equiv b + c \pmod{m}$ for any $c \in \mathbb{Z}$
2. $ac \equiv bc \pmod{m}$ for any $c \in \mathbb{Z}$
3. $a^n \equiv b^n \pmod{m}$ for $n \in \mathbb{Z}^+$

If we also have $c \equiv d \pmod{m}$,

1. $a + c \equiv b + d \pmod{m}$
2. $ac \equiv bd \pmod{m}$

2.3 GCD

The greatest common denominator of a and b is the largest positive integer which divides both a and b . To find the gcd of two numbers, we can run the Euclidean algorithm.

Theorem 1: For any $a, b \in \mathbb{Z}$ there exists $u, v \in \mathbb{Z}$ such that $au + bv = \gcd(a, b)$. In words, we say that a and b can be written as a linear combination of their gcd.

Theorem 2: An integer is a linear combination of a and b if and only if it is a multiple of their gcd.

2.4 Multiplicative Inverse

Consider the particular congruence

$$ax \equiv 1 \pmod{m}.$$

If this equation has a solution, then we know we can find some integer x which, when multiplied by a , yields $1 \pmod{m}$. We define this integer to be the *multiplicative inverse* of $a \pmod{m}$, and we denote it a^{-1} . If a multiplicative inverse exists \pmod{m} , then when working \pmod{m} ,

we can “divide” by a —that is, we can multiply two sides of a congruence by a^{-1} , cancelling a from both sides.

When does a multiplicative inverse exist? According to the above Theorem 2: a^{-1} exists if and only if $\gcd(a, m)$ divides 1 (which is c in this particular congruence.) Thus, a^{-1} exists $(\text{mod } m)$ if and only if $\gcd(a, m) = 1$, that is, if and only if a and m are relatively prime. How do we find the multiplicative inverse? We can run the Euclidean algorithm and then backtrack to obtain the multiplicative inverse (gcdcombo).

2.5 Fermat's little Theorem

If p is prime and does not divide $a \in \mathbb{Z}$ then

$$a^{p-1} \equiv 1 \pmod{p}.$$

This means a^{p-2} is a multiplicative inverse for $a \text{ mod } p$.

2.6 Euler's Totient Function

The totient function of n is a count of how many positive integers less than or equal to n are relatively prime to it. For any prime p , $\phi(p) = p - 1$. If m and a are relatively prime, then

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

This means $a^{\phi(m)-1}$ is a multiplicative inverse for $a \text{ mod } m$. Fermat's little theorem is just a special case of this rule.

3 Counting

3.1 Product Rule and Permutations

The **product rule** states that for finite sets S_1, \dots, S_n , $|S_1 \times \dots \times S_n| = |S_1| * \dots * |S_n|$. This can be useful in representing how many ways we could make a series of n independent choices. If we know how many options we have for each choice, we can find the number of ways we could make all of the choices by multiplying all the numbers of options together.

If the choices are instead dependent on each other, so what we choose from S_1 affects what we can choose from S_2 but not the *number* of things we could choose from S_2 , we can use the **generalized product rule**. The generalized product rule tells us that if we are making a sequence of length k and we have n_1, \dots, n_k options for each position, then there are $n_1 * \dots * n_k$ total sequences we can form.

A **permutation** of a set A is an ordered list of the elements of A . The number of permutations of n elements is $n!$, which we can prove with the generalized product rule.

Example

The number of permutations of n elements is $n!$. This follows by the generalized product rule because we can break down constructing a sequence into choosing the first element for which there are n choices, then choosing the second element for which there are $n - 1$ choices and so on for $n \cdot (n - 1) \cdot (n - 2) \cdot \dots = n!$.

3.2 Binomial Coefficients and Theorem

The **binomial coefficient**, also called n choose k , is defined to be

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

for $n \geq k$ and $n, k \in \mathbb{Z}^+$.

The binomial coefficient $\binom{n}{k}$ counts the number of ways to choose k objects from n objects. Equivalently, it counts the number of subsets of size k of a set of size n .

Binomial Theorem: The coefficients of the terms in the polynomial $(x + y)^n$ are binomial coefficients, i.e.

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

3.3 Counting Arguments

A **counting argument** shows that the LHS (lefthand side) and the RHS (righthand side) of some equation count the same thing. Instead of using algebraic manipulation, we explain why both sides ultimately count the elements of some set, just in different ways.

Importantly, if a question asks you to use a counting argument, you cannot use the definition of $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ or other algebraic arguments.

For instance, consider the following identity.

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

Let S be a set with n elements. The LHS counts the number of ways to form a subset of S size k . Let x be some element of S . Each subset of S of size k either includes x or does not include x . If the subset includes x , then we need to pick $k-1$ other elements for the subset from the remaining $n-1$ elements, which we can do in $\binom{n-1}{k-1}$ ways. If the subset does not include x , then we still need to pick all k elements, and can do so from the remaining $n-1$ elements since we can't pick x , which we can do in $\binom{n-1}{k}$ ways. So, adding these together to get the RHS, this also counts the number of subsets of S of size k .

3.4 Inclusion/Exclusion Formula

The inclusion/exclusion formula provides a way of counting the size of a union of sets, and it is especially helpful if the sets overlap (and thus merely summing the sizes would result in over-counting.)

For two sets A and B , the inclusion/exclusion formula says that

$$|A \cup B| = |A| + |B| - |A \cap B|$$

While the formula for three sets A , B , and C is

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$$

Going further, we can repeat this process for any number of sets, alternating between adding and subtracting the sizes of sets.

3.5 Counting Donuts

The number of ways to distribute m identical objects among n distinct groups is

$$\binom{m+n-1}{n-1}.$$

Why is this? We can uniquely represent such a distribution with a 0/1 string of length $m+n-1$ that has exactly m 0's:

Let the m 0's represent the objects. The remaining $n-1$ bits in the string are 1's. Let all of the 0's to the left of the first 1 belong to group 1. Then, let all the 0's between the first 1 and the second 1 belong to the second group. Continue determining group membership in this fashion.

Below is a diagram illustrating this. Note that, since 1's two and three are adjacent, nothing is in group 3.

$$\underbrace{0\dots 01}_{\text{group 1}} \underbrace{0\dots 011}_{\text{group 2}} \underbrace{0\dots 010\dots 01}_{\text{group 4}} \underbrace{000}_{\text{group } n}$$

What's important to note is that (1) any distribution we choose can be represented with some length $m + n - 1$ binary string, and (2) any such binary string represents a valid distribution of m identical objects into n distinct groups under this interpretation. In other words, the distributions and binary strings are in bijection with each other, meaning we can count one by counting the other.

We know how to count such binary strings: it is simply the number of ways you can choose $n - 1$ of the bits to be 1's, leaving the other m bits to be 0's: $\binom{m+n-1}{n-1}$.

3.6 Pigeonhole Principle

Pigeonhole Principle: If we put $k + 1$ objects into k boxes, then some box has at least 2 objects. More generally, if we place n objects into k boxes, then some box must have at least $\lceil \frac{n}{k} \rceil$ objects.

Another way we can think about the Pigeonhole Principle is this. It tells us that if we have a function, $f : |X| \rightarrow |Y|$, such that the cardinality of X is n and the cardinality of Y is k , then there is some $y \in Y$ such that the number of $x \in X$ that map to y is greater than or equal to $\lceil \frac{n}{k} \rceil$.

Pigeonhole principle basically says that *some* box must have the average number of items per box (assume for the sake of contradiction that this were not the case—what would have to be true?) We get the ceiling function because we can't have fractional objects—objects must remain whole as they are placed into boxes.