Discrete Structures

Day 16

Q. Use a proof by contradiction to show that there is no rational number r for which $r^3 + r + 1 = 0$.

Assume that $r = a/b$ is a root, where a and b are integers and a/b is in lowest terms.

$$(a/b)^3 + (a/b) + 1 = 0$$

$$a^3/b^3 + a/b + 1 = 0$$

$$(a^3+ab^2+b^3)/b^3=0$$

$$a^3+ab^2+b^3=0$$

a	b	$a^3+ab^2+b^3$
Odd	Odd	Odd + Odd + Odd = Odd
Odd	Even	Odd + Even + Even = Odd
Even	Odd	Even + Even + Odd = Odd
Even	Even	Even + Even + Even = Even

Only when a and b are even, 0 can be obtained, which means a/b is not in lowest terms. Our assumption is wrong.

Hence, there is no rational number r for which $r^3 + r + 1 = 0$.

Q. Prove that at least one of the real numbers $a_1, a_2, \ldots, a_n$ is greater than or equal to the average of these numbers. What kind of proof did you use?

Q. Prove that at least one of the real numbers $a1, a2, \ldots, an$ is greater than or equal to the average of these numbers. What kind of proof did you use?

p: At least one of the real numbers $a1, a2, \ldots, an$ is greater than or equal to the average of these numbers.

Assume ¬p is T.

¬p: None of the real numbers $a1, a2, \ldots, an$ is greater than or equal to the average of these numbers.

$a1<(a1+a2+\ldots+an)/n \quad (1)$

$a2<(a1+a2+\ldots+an)/n \quad (2)$

.

.

$an<(a1+a2+\ldots+an)/n \quad (n)$

Adding, $a1+a2+\ldots+an<1/n\{n(a1+a2+\ldots+an)\}$

$a1+a2+\ldots+an<(a1+a2+\ldots+an)$ which is a contradiction.

Our assumption is wrong.

Hence, At least one of the real numbers $a1, a2, \ldots, an$ is greater than or equal to the average of these numbers.

Proof by Cases

Sometimes we cannot prove a theorem using a single argument that holds for all possible cases.

To prove a conditional statement of the form

$(p1 \lor p2 \lor \cdots \lor pn) \rightarrow q$

the tautology

$[(p1 \lor p2 \lor \cdots \lor pn) \rightarrow q] \leftrightarrow [(p1 \rightarrow q) \land (p2 \rightarrow q) \land \cdots \land (pn \rightarrow q)]$

can be used as a rule of inference.

This shows that the original conditional statement with a hypothesis made up of a disjunction of the propositions $p1, p2, \ldots, pn$ can be proved by proving each of the n conditional statements $pi \rightarrow q$, $i = 1, 2, \ldots, n$, individually. Such an argument is called a **proof by cases**.

EXHAUSTIVE PROOF

Some theorems can be proved by examining a relatively small number of examples. Such proofs are called **exhaustive proofs**, or **proofs by exhaustion** because these proofs proceed by exhausting all possibilities.

Q. Prove that $(n + 1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.

We use a proof by exhaustion. We only need verify the inequality $(n + 1)^3 \geq 3^n$

when $n = 1, 2, 3$, and 4.

For $n = 1$, we have $(n + 1)^3 = 2^3 = 8$ and $3^n = 3^1 = 3$;

for $n = 2$, we have $(n + 1)^3 = 3^3 = 27$ and $3^n = 3^2 = 9$;

for $n = 3$, we have $(n + 1)^3 = 4^3 = 64$ and $3^n = 3^3 = 27$;

and for $n = 4$, we have $(n + 1)^3 = 5^3 = 125$ and $3^n = 3^4 = 81$.

In each of these four cases, we see that $(n + 1)^3 \geq 3n$. We have used the method of exhaustion to prove that $(n + 1)^3 \geq 3n$ if n is a positive integer with $n \leq 4$.

Q. Prove that if n is an integer, then $n^2 \geq n$.

We can prove that $n^2 \geq n$ for every integer by considering three cases, when $n = 0$, when $n \geq 1$, and when $n \leq -1$. We split the proof into three cases zero, positive integers, and negative integers separately.

Case (i): When $n = 0$, because $0^2 = 0$, we see that $0^2 \geq 0$. It follows that $n^2 \geq n$ is true in this case.

Case (ii): When $n \geq 1$, when we multiply both sides of the inequality $n \geq 1$ by the positive integer n, we obtain $n \cdot n \geq n \cdot 1$. This implies that $n^2 \geq n$ for $n \geq 1$.

Case (iii): In this case $n \leq -1$. However, $n^2 \geq 0$. It follows that $n^2 \geq n$.

Because the inequality $n^2 \geq n$ holds in all three cases, we can conclude that if n is an integer, then $n^2 \geq n$.

Proof Strategies

Forward reasoning

direct proof and indirect proof

Backward reasoning

Unfortunately, forward reasoning is often difficult to use to prove more complicated results, because the reasoning needed to reach the desired conclusion may be far from obvious. In such cases it may be helpful to use *backward reasoning*. To reason backward to prove a statement q, we find a statement p that we can prove with the property that $p \rightarrow q$.

Q. Given two positive real numbers x and y, their **arithmetic mean** is $(x + y)/2$ and their **geometric mean** is $\sqrt{xy}$. When we compare the arithmetic and geometric means of pairs of distinct positive real numbers, we find that the arithmetic mean is always greater than the geometric mean. Prove that this inequality is always true?

To prove that $(x + y)/2 > \sqrt{xy}$ when x and y are distinct positive real numbers,

we can work backward. We construct a sequence of equivalent inequalities. The equivalent inequalities are:

$(x + y)/2 > \sqrt{xy}$

$(x + y)^2/4 > xy$, *(Squaring)*

$(x + y)^2 > 4xy$

$x^2 + 2xy + y^2 > 4xy$

$x^2 - 2xy + y^2 > 0$

$(x - y)^2 > 0$

Because $(x - y)^2 > 0$ when $x \neq y$, it follows that the final inequality is true.

Once we have carried out this backward reasoning, we can easily reverse the steps to construct a proof using forward reasoning. We now give this proof.

Suppose that x and y are distinct positive real numbers.

Then $(x - y)^2 > 0$

….

Q. Suppose that two people play a game taking turns removing one, two, or three stones at a time from a pile that begins with 15 stones. The person who removes the last stone wins the game. Show that the first player can win the game no matter what the second player does.

To prove that the first player can always win the game, we work backward.

	First player	Second player
Last step	Pick 1/2/3 (win)	
Last step -1		Force to pick 1/2/3 out of 4
Last step -2	Pick 1/2/3 and leave 4	
Last step -3		Force to pick 1/2/3 out of 8 and leave (7/6/5)
Last step -4	Pick 1/2/3 and leave 8	
Last step –5		Force to pick 1/2/3 out of 12 and leave (11/10/9)
First step	Pick 3 and leave 12	

Mathematical Induction

PRINCIPLE OF MATHEMATICAL INDUCTION

To prove that $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function, we complete two steps:

BASIS STEP: We verify that $P(1)$ is true.

INDUCTIVE STEP: We show that the conditional statement $P(k) \rightarrow P(k + 1)$ is true for all positive integers k.

To complete the inductive step of a proof using the principle of mathematical induction, we assume that $P(k)$ is true for an arbitrary positive integer k and show that under this assumption, $P(k + 1)$ must also be true. The assumption that $P(k)$ is true is called the **inductive hypothesis**.

Q. Show that if n is a positive integer, then $1 + 2 + \cdots + n = n(n + 1)/2$.

Let $P(n)$ be the proposition that the sum of the first n positive integers, $1 + 2 + \cdots n = n(n+1)/2$.

We must show that $P(1)$ is true and that the conditional statement $P(k)$ implies $P(k + 1)$ is true for $k = 1, 2, 3, \ldots$.

BASIS STEP: $P(1)$ is true, because $1 = 1(1 + 1)/2$

INDUCTIVE STEP: For the inductive hypothesis we assume that $P(k)$ holds for an arbitrary positive integer k. That is, we assume that

$$1 + 2 + \cdots + k = k(k + 1)/2 \qquad \text{--- (1)}$$

Under this assumption, it must be shown that $P(k + 1)$ is true, i.e.

$1 + 2 + \cdots + k + (k + 1) = (k + 1)[(k + 1) + 1]/2 = (k + 1)(k + 2)/2$

When we add $k + 1$ to both sides of the equation in (1), we obtain

$$\begin{aligned} 1 + 2 + \cdots + k + k+1 &= k(k+1)/2 + k+1 \\ &= \{k(k+1)+2(k+1)\}/2 \\ &= (k+1)(k+2)/2 \end{aligned}$$

This shows that $P(k + 1)$ is true under the assumption that $P(k)$ is true.

We have completed the basis step and the inductive step, so by mathematical induction we know that $P(n)$ is true for all positive integers n. That is, we have proven that $1 + 2 + \cdots + n = n(n + 1)/2$ for all positive integers n.

Q. Use mathematical induction to show that $1 + 2 + 2^2 + \cdot\cdot\cdot + 2^n = 2^{n+1} - 1$ for all nonnegative integers n.

Q. Sums of Geometric Progressions Use mathematical induction to prove this formula for the sum of a finite number of terms of a geometric progression with initial term *a* and common ratio *r*:

$$\sum_{j=0}^{n} ar^j = a + ar + ar^2 + \cdots + ar^n = \frac{ar^{n+1} - a}{r - 1} \; where\ r \neq 1$$

where *n* is a nonnegative integer.

*BASIS STEP: P(*0*)* is true, because $\frac{ar^{0+1}-a}{r-1} = a$

INDUCTIVE STEP: The inductive hypothesis is the statement that *P(k)* is true, where *k* is an arbitrary nonnegative integer. That is, *P(k)* is the statement that

$$a + ar + ar^2 + \cdots + ar^k = \frac{ar^{k+1}-a}{r-1}$$

To prove: $a + ar + ar^2 + \cdots + ar^k + ar^{k+1} = \frac{ar^{k+2}-a}{r-1}$

L.H.S.

$$\begin{aligned} a + ar + ar^2 + \cdots + ark + ar^{k+1} &= \frac{ar^{k+1}-a}{r-1} + ar^{k+1} \\ &= \frac{(ar^{k+1}-a)+ar^{k+1}(r-1)}{r-1} \\ &= \frac{(ar^{k+1}-a)+ar^{k+2}-ar^{k+1}}{r-1} \\ &= \frac{(ar^{k+2}-a)}{r-1} = R.H.S. \end{aligned}$$

This shows that if the inductive hypothesis *P(k)* is true, then *P(k* + 1*)* must also be true. This completes the inductive argument.

PROVING INEQUALITIES

Q. Use mathematical induction to prove the inequality $n < 2^n$ for all positive integers n.

Let $P(n)$ be the proposition that $n < 2^n$.

BASIS STEP: $P(1)$ is true, because $1 < 2^1 = 2$. This completes the basis step.

INDUCTIVE STEP: We first assume the inductive hypothesis that $P(k)$ is true for an arbitrary positive integer k. We need to show that if $k < 2^k$, then $k + 1 < 2^{k+1}$.

Adding 1 on both side of P(k)

$$k+1 < 2^k + 1$$

$$k+1 < 2^k + 1 \leq 2^k + 2^k = 2 \cdot 2^k = 2^{k+1}. \quad \textit{Since } 1 \leq 2^k$$

This shows that $P(k + 1)$ is true, namely, that $k + 1 < 2^{k+1}$, based on the assumption that $P(k)$ is true. The induction step is complete. Therefore, because we have completed both the basis step and the inductive step, by the principle of mathematical induction we have shown that $n < 2^n$ is true for all positive integers n.

Q. Use mathematical induction to prove that $2^n < n!$ for every integer n with $n \geq 4$. (Note that this inequality is false for $n = 1, 2$, and 3.)

Q. Use mathematical induction to prove that $2^n < n!$ for every integer n with $n \geq 4$. (Note that this inequality is false for $n = 1, 2,$ and 3.)

Let $P(n)$ be the proposition that $2^n < n!$.

BASIS STEP: To prove the inequality for $n \geq 4$ requires that the basis step be $P(4)$. Note that $P(4)$ is true, because $2^4 = 16 < 24 = 4!$

INDUCTIVESTEP: For the inductive step, we assume that $P(k)$ is true for an arbitrary integer k with $k \geq 4$. We must show that if $2^k < k!$ for an arbitrary positive integer k where $k \geq 4$, then $2^{k+1} < (k + 1)!$.

$$
\begin{aligned}
2^{k+1} &= 2 \cdot 2^k \\
&< 2 \cdot k! \quad \text{(by the inductive hypothesis)} \\
&< (k+1)k! \quad \text{(since } 2 < k + 1\text{)} \\
&< (k+1)!
\end{aligned}
$$

This shows that $P(k + 1)$ is true when $P(k)$ is true. This completes the inductive step of the proof.

PROVING DIVISIBILITY RESULTS

Q. Use mathematical induction to prove that $n^3 - n$ is divisible by 3 whenever n is a positive integer.

To construct the proof, let $P(n)$ denote the proposition: "$n^3 - n$ is divisible by 3."

BASIS STEP: The statement $P(1)$ is true because $1^3 - 1 = 0$ is divisible by 3. This completes the basis step.

INDUCTIVE STEP: For the inductive hypothesis we assume that $P(k)$ is true; that is, we assume that $k^3 - k$ is divisible by 3 for an arbitrary positive integer k.

We must show that $(k + 1)^3 - (k + 1)$ is divisible by 3.

$$
\begin{aligned}
(k+1)^3 - (k+1) &= (k^3 + 3k^2 + 3k + 1) - (k + 1) \\
&= (k^3 - k) + 3(k^2 + k). \\
&= \textit{Divisible by 3 from } P(k) + \textit{Multiple of 3} \\
&= \textit{Divisible by 3.}
\end{aligned}
$$

Because we have completed both the basis step and the inductive step, by the principle of mathematical induction we know that $n3 - n$ is divisible by 3 whenever n is a positive integer.

Q. Use mathematical induction to prove that $7^{n+2} + 8^{2n+1}$ is divisible by 57 for every nonnegative integer n.

Strong Induction

STRONG INDUCTION

To prove that $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function, we complete two steps:

BASIS STEP: We verify that the proposition $P(1)$ is true.

INDUCTIVE STEP: We show that the conditional statement $[P(1) \wedge P(2) \wedge \cdots \wedge P(k)] \rightarrow P(k + 1)$ is true for all positive integers k.

When we use strong induction to prove that $P(n)$ is true for all positive integers n, our inductive hypothesis is the assumption that $P(j)$ is true for $j = 1, 2, \ldots, k$. That is, the inductive hypothesis includes all k statements $P(1), P(2), \ldots, P(k)$. Because we can use all k statements $P(1), P(2), \ldots, P(k)$ to prove $P(k + 1)$, rather than just the statement $P(k)$ as in a proof by mathematical induction, strong induction is a more flexible proof technique.

Q. Show that if n is an integer greater than 1, then n can be written as the product of primes.

Let $P(n)$ be the proposition that n can be written as the product of primes.

BASIS STEP: $P(2)$ is true, because 2 can be written as the product of one prime, itself.

INDUCTIVE STEP: The inductive hypothesis is the assumption that $P(j)$ is true for all integers j with $2 \leq j \leq k$, that is, the assumption that j can be written as the product of primes whenever j is a positive integer at least 2 and not exceeding k.

To complete the inductive step, it must be shown that $P(k + 1)$ is true under this assumption, that is, that $k + 1$ is the product of primes.

There are two cases to consider, namely, when $k + 1$ is prime and when $k + 1$ is composite.

If $k + 1$ is prime, we immediately see that $P(k + 1)$ is true.

Otherwise, $k + 1$ is composite and can be written as the product of two positive integers a and b with $2 \leq a \leq b < k + 1$. Because both a and b are integers at least 2 and not exceeding k, we can use the inductive hypothesis to write both a and b as the product of primes. Thus, if $k + 1$ is composite, it can be written as the product of primes, namely, those primes in the factorization of a and those in the factorization of b.