sesh #3: April 30, 2024

2 The Well Ordering Principle

Non-negative Integers!
not rational, not real

> Every *nonempty* set of *nonnegative integers* has a *smallest* element.

nonempty!

This statement is known as The *Well Ordering Principle*. Do you believe it? Seems sort of obvious, right? But notice how tight it is: it requires a *nonempty* set—it's false for the empty set which has *no* smallest element because it has no elements at all. And it requires a set of *nonnegative* integers—it's false for the set of *negative* integers and also false for some sets of nonnegative *rationals*—for example, the set of positive rationals. So, the Well Ordering Principle captures something special about the nonnegative integers.

While the Well Ordering Principle may seem obvious, it's hard to see offhand why it is useful. But in fact, it provides one of the most important proof rules in discrete mathematics. In this chapter, we'll illustrate the power of this proof method with a few simple examples.

2.1 Well Ordering Proofs

We actually have already taken the Well Ordering Principle for granted in proving that $\sqrt{2}$ is irrational. That proof assumed that for any positive integers m and n, the fraction m/n can be written *in lowest terms*, that is, in the form m'/n' where m' and n' are positive integers with no common prime factors. How do we know this is always possible?

Suppose to the contrary that there are positive integers m and n such that the fraction m/n cannot be written in lowest terms. Now let C be the set of positive integers that are numerators of such fractions. Then $m \in C$, so C is nonempty. Therefore, by Well Ordering, there must be a smallest integer, $m_0 \in C$. So by definition of C, there is an integer $n_0 > 0$ such that

set of positive numerators of fractions that can't be put in lowest terms.

$$\text{the fraction } \frac{m_0}{n_0} \text{ cannot be written in lowest terms.}$$

such that it can be factored out.

This means that m_0 and n_0 must have a common prime factor, $p > 1$. But

$$\frac{m_0/p}{n_0/p} = \frac{m_0}{n_0},$$

so any way of expressing the left hand fraction in lowest terms would also work for m_0/n_0, which implies

$$\text{the fraction } \frac{m_0/p}{n_0/p} \text{ cannot be in written in lowest terms either.}$$

↳ since the equality is ensured as long as you do operation on both sides. ↓ meaning if i factor out p on one side, so should i on the other side hence $\frac{m_0/p}{n_0/p}$ not in lowest term.

So by definition of C, the numerator, m_0/p, is in C. But $m_0/p < m_0$, which contradicts the fact that m_0 is the smallest element of C.

Since the assumption that C is nonempty leads to a contradiction, it follows that C must be empty. That is, that there are no numerators of fractions that can't be written in lowest terms, and hence there are no such fractions at all.

We've been using the Well Ordering Principle on the sly from early on!

2.2 Template for Well Ordering Proofs

More generally, there is a standard way to use Well Ordering to prove that some property, $P(n)$ holds for every nonnegative integer, n. Here is a standard way to organize such a well ordering proof:

To prove that "$P(n)$ is true for all $n \in \mathbb{N}$" using the Well Ordering Principle:

- Define the set, C, of *counterexamples* to P being true. Specifically, define

  $$C ::= \{n \in \mathbb{N} \mid \text{NOT}(P(n)) \text{ is true}\}.$$

  (The notation $\{n \mid Q(n)\}$ means "the set of all elements n for which $Q(n)$ is true." See Section 4.1.4.)

- Assume for proof by contradiction that C is nonempty.

- By the Well Ordering Principle, there will be a smallest element, n, in C.

- Reach a contradiction somehow—often by showing that $P(n)$ is actually true or by showing that there is another member of C that is smaller than n. This is the open-ended part of the proof task.

- Conclude that C must be empty, that is, no counterexamples exist. ■

2.2.1 Summing the Integers

Let's use this template to prove

Theorem 2.2.1.
$$1 + 2 + 3 + \cdots + n = n(n+1)/2 \tag{2.1}$$
for all nonnegative integers, n.

First, we'd better address a couple of ambiguous special cases before they trip us up:

- If $n = 1$, then there is only one term in the summation, and so $1 + 2 + 3 + \cdots + n$ is just the term 1. Don't be misled by the appearance of 2 and 3 or by the suggestion that 1 and n are distinct terms!
- If $n = 0$, then there are no terms at all in the summation. By convention, the sum in this case is 0.

So, while the three dots notation, which is called an *ellipsis*, is convenient, you have to watch out for these special cases where the notation is misleading. In fact, whenever you see an ellipsis, you should be on the lookout to be sure you understand the pattern, watching out for the beginning and the end.

We could have eliminated the need for guessing by rewriting the left side of (2.1) with *summation notation*:
$$\sum_{i=1}^{n} i \qquad \text{or} \qquad \sum_{1 \le i \le n} i.$$
Both of these expressions denote the sum of all values taken by the expression to the right of the sigma as the variable, i, ranges from 1 to n. Both expressions make it clear what (2.1) means when $n = 1$. The second expression makes it clear that when $n = 0$, there are no terms in the sum, though you still have to know the convention that a sum of no numbers equals 0 (the *product* of no numbers is 1, by the way).

OK, back to the proof:

Proof. By contradiction. Assume that Theorem 2.2.1 is *false*. Then, some nonnegative integers serve as *counterexamples* to it. Let's collect them in a set:
$$C ::= \{n \in \mathbb{N} \mid 1 + 2 + 3 + \cdots + n \neq \frac{n(n+1)}{2}\}.$$
Assuming there are counterexamples, C is a nonempty set of nonnegative integers. So, by the Well Ordering Principle, C has a minimum element, which we'll call c. That is, among the nonnegative integers, c is the *smallest counterexample* to equation (2.1).

Since c is the smallest counterexample, we know that (2.1) is false for $n = c$ but true for all nonnegative integers $n < c$. But (2.1) is true for $n = 0$, so $c > 0$. This means $c - 1$ is a nonnegative integer, and since it is less than c, equation (2.1) is true for $c - 1$. That is,

$$1 + 2 + 3 + \cdots + (c - 1) = \frac{(c-1)c}{2}.$$

But then, adding c to both sides, we get

$$1 + 2 + 3 + \cdots + (c - 1) + c = \frac{(c-1)c}{2} + c = \frac{c^2 - c + 2c}{2} = \frac{c(c+1)}{2},$$

which means that (2.1) does hold for c, after all! This is a contradiction, and we are done. ■

2.3 Factoring into Primes (Fundamental Theorem of Arithmetic)

We've previously taken for granted the *Prime Factorization Theorem*, also known as the *Unique Factorization Theorem* and the *Fundamental Theorem of Arithmetic*, which states that every integer greater than one has a unique[1] expression as a product of prime numbers. This is another of those familiar mathematical facts which are taken for granted but are not really obvious on closer inspection. We'll prove the uniqueness of prime factorization in a later chapter, but well ordering gives an easy proof that every integer greater than one can be expressed as *some* product of primes.

weaker Funda Theorem (not unique product)

Theorem 2.3.1. *Every positive integer greater than one can be factored as a product of primes.*

Proof. The proof is by well ordering.

Let C be the set of all integers greater than one that cannot be factored as a product of primes. We assume C is not empty and derive a contradiction.

If C is not empty, there is a least element, $n \in C$, by well ordering. The n can't be prime, because a prime by itself is considered a (length one) product of primes and no such products are in C.

So n must be a product of two integers a and b where $1 < a, b < n$. Since a and b are smaller than the smallest element in C, we know that $a, b \notin C$. In other words, a can be written as a product of primes $p_1 p_2 \cdots p_k$ and b as a product of

[1]...unique up to the order in which the prime factors appear

primes $q_1 \cdots q_l$. Therefore, $n = p_1 \cdots p_k q_1 \cdots q_l$ can be written as a product of primes, contradicting the claim that $n \in C$. Our assumption that C is not empty must therefore be false. ■

Sesh 3: In-Class Problems

May 1, 2024 → delayed b.c. I had to fix the syllabus acc'dg to PS, Qz, Exams etc. sol'n availability.

→ fee for postal service ↓ can be paid by putting stamps

Whaaat?!

Problem 1.

The proof below uses the Well Ordering Principle to prove that every amount of postage that can be paid exactly using only 6 cent and 15 cent stamps, is divisible by 3. Let the notation "$j \mid k$" indicate that integer j is a divisor of integer k, and let $S(n)$ mean that exactly n cents postage can be paid using only 6 and 15 cent stamps. Then the proof shows that

if S(n) then →

$$S(n) \text{ IMPLIES } 3 \mid n, \quad \text{for all nonnegative integers } n. \qquad (*)$$

Fill in the missing portions (indicated by "...") of the following proof of (*).

i.e. S(n) holds but n not div by 3 ...

Let C be the set of *counterexamples* to (*), namely[1]

(x)
$$C ::= \{n \mid \dots\}$$

→ a counterexample exists...

(a) Assume for the purpose of obtaining a contradiction that C is nonempty. Then by the WOP, there is a smallest number, $m \in C$. This m must be positive because....

(b) But if $S(m)$ holds and m is positive, then $S(m-6)$ or $S(m-15)$ must hold, because....

(c) So suppose $S(m-6)$ holds. Then $3 \mid (m-6)$, because...

But if $3 \mid (m-6)$, then obviously $3 \mid m$, contradicting the fact that m is a counterexample.

↳ since $3|m$ is required by $3|m-6$

(d) Next suppose $S(m-15)$ holds. Then the proof for $m-6$ carries over directly for $m-15$ to yield a contradiction in this case as well. Since we get a contradiction in both cases, we conclude that...

which proves that (*) holds.

(x) $C ::= \{n \mid S(n) = \text{true and } (3|n) = \text{false}\}$ ✓

(a) Since we're proving $S(m) = \text{true}$ but $3|m = \text{false}$ as counterexample. Hence $S(m)$ means m is a postage amt, which positive by definition.

→ nope... m is positive b.c. it's not zero since $3|0$.

(b) ... $S(m)$ means that m is paid in combination of 6 and 15 stamps.

↳ so removing 6 or 15 maintains it to be a combi of 6 &/or 15.

(c) ... since $S(m-6)$: $m-6 = a \cdot 6 + b \cdot 15$ for any integer $a, b \geq 0$, and RHS is div by 3.

↳ not sure why we can't do this but solution's answer shows:

$3|(m-6)$ must hold b.c. we've assumed m is the least counterexample & we don't want to contradict that.

(d) C must be empty... ✓

Problem 2.
Use the Well Ordering Principle to prove that

$$\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}. \tag{1}$$

for all nonnegative integers, n.

To prove that "$P(n)$ is true for all $n \in \mathbb{N}$" using the Well Ordering Principle:

- Define the set, C, of *counterexamples* to P being true. Specifically, define

  $C ::= \{n \in \mathbb{N} \mid \text{NOT}(P(n)) \text{ is true}\}$.

  (The notation $\{n \mid Q(n)\}$ means "the set of all elements n for which $Q(n)$ is true." See Section 4.1.4.)
- Assume for proof by contradiction that C is nonempty.
- By the Well Ordering Principle, there will be a smallest element, n, in C.
- Reach a contradiction somehow—often by showing that $P(n)$ is actually true or by showing that there is another member of C that is smaller than n. This is the open-ended part of the proof task.
- Conclude that C must be empty, that is, no counterexamples exist. ■

→ Proof. Let the above formula be $P(n)$. To prove $P(n)$ is true for all $n \in \mathbb{N}$, assume $\exists$ a set C of counterexamples n to $P(n)$:

$$C ::= \left\{ n \in \mathbb{N} \,\middle|\, \sum_{k=0}^{n} k^2 \neq \frac{n(n+1)(2n+1)}{6} \right\}$$

→ assume that $C \neq \emptyset$.

→ Since C is a set of nonnegative integers, WOP tells us that theres a smallest element $m \in C$.

→ Since if $n=0$ the eq holds, then $m \geq 1$.

→ From that we know that $m-1$ must hold since $m-1 < m$ the smallest element of C.

↳ and also since we know $m-1$ is non-negative.

$$\sum_{k=0}^{m-1} k^2 = \frac{(m-1)(m)(2m-2+1)}{6}$$

$$\sum_{k=0}^{m} k^2 - m^2 = \frac{(m^2-m)(2m-1)}{6}$$

$$\sum_{k=0}^{m} k^2 = \frac{6m^2 + 2m(m^2-m) - m^2 + m}{6} = \frac{m(5m + 2(m^2-m) + 1)}{6}$$

$$= \frac{m(2m^2+3m+1)}{6} = \frac{m(2m+1)(m+1)}{6}$$

this shows that $P(n)$ holds for $n=m$, which contradicts the assumption that m is the smallest elem of C. Hence the assumption that C is nonempty leads to a contradiction, meaning C is empty and $P(n)$ holds for all $n \in \mathbb{N}$.

■

// correct

Problem 3.
Euler's Conjecture in 1769 was that there are no positive integer solutions to the equation

$$a^4 + b^4 + c^4 = d^4.$$

Integer values for a, b, c, d that do satisfy this equation, were first discovered in 1986. So Euler guessed wrong, but it took more two hundred years to prove it.

Now let's consider Lehman's[2] equation, similar to Euler's but with some coefficients:

$$8a^4 + 4b^4 + 2c^4 = d^4 \tag{2}$$

Prove that Lehman's equation (2) really does not have any positive integer solutions.

Hint: Consider the minimum value of a among all possible solutions to (2).

↳ Let's consider the opposite of Lehman's equation and try to derive a contradiction. Let the opposite be $P(n)$, stating...

"Given some positive integers $b = b_0$, $c = c_0$, and $d = d_0$, then there exist a nonempty set A containing all solutions $a = n$ of Lehman's eq"

$$A ::= \{ n \mid 8n^4 + 4b_0^4 + 2c_0^4 = d_0^4 \}$$

By well ordering principle, we know that among all possible solutions in A, there is a smallest value n_0, s.t.

$$(\heartsuit) \quad 8n_0^4 + 4b_0^4 + 2c_0^4 = d_0^4$$

Let's ignore the trivial sol'n so that we know $n_0 \neq 0$, hence $n_0 - 1$ is nonnegative and $< n_0$. Then we know since it's $<$, that the eqn shouldn't hold for $n_0 - 1$.

$$8(n_0-1)^4 + 4b_0^4 + 2c_0^4 \neq d_0^4$$

→ wrong approach...
it uses very subtle WOP on a, b, c, d; and doesn't consider sets.

Sub'ng $(\heartsuit)$ we get:

$$8(n_0-1)^4 + k \neq 8n_0^4 + k$$

$$8(n_0-1)^4 \neq 8n_0^4$$

... don't know anymore...

Solution. Suppose that there exists a solution. Then there must be a solution in which a has the smallest possible value. We will show that, in this solution, a, b, c, and d must all be even. However, we can then obtain another solution over the positive integers with a smaller a by dividing a, b, c, and d in half. This is a contradiction, and so no solution exists.

All that remains is to show that a, b, c, and d must all be even. The left side of Lehman's equation is even, so d^4 is even, so d must be even. Substituting $d = 2d'$ into Lehman's equation gives:

$$8a^4 + 4b^4 + 2c^4 = 16d'^4 \tag{4}$$

Now $2c^4$ must be a multiple of 4, since every other term is a multiple of 4. This implies that c^4 is even and so c is also even. Substituting $c = 2c'$ into the previous equation gives:

$$8a^4 + 4b^4 + 32c'^4 = 16d'^4 \tag{5}$$

Arguing in the same way, $4b^4$ must be a mutliple of 8, since every other term is. Therefore, b^4 is even and so b is even. Substituting $b = 2b'$ gives:

$$8a^4 + 64b'^4 + 32c'^4 = 16d'^4 \tag{6}$$

Finally, $8a^4$ must be a multiple of 16, a^4 must be even, and so a must also be even. Therefore, a, b, c, and d must all be even, as claimed. ■