The Fundamental Theorem of Arithmetic

MTH 350 -- Module 4A

A composite number is any integer that is not prime.

True

False

What would the NEGATION of the definition of "prime number" say? Fill in the blank: An integer $n > 1$ is "not prime" if...

Join by Web

1. Go to **PollEv.com**
2. Enter **TALBERT**
3. Respond to activity

The Fundamental Theorem of Arithmetic says that every integer greater than or equal to 1 can be factored into a product of two or more prime numbers, and this factorization is unique up to the ordering of the factors.

- True
- False

Tc 0

Consider the number 120. This number can be factored in two different ways: $120 = 2 \times 60$ and $120 = 10 \times 12$. Does this contradict the "uniqueness" part of the Fundamental Theorem of Arithmetic?

Join by Web

1 Go to **PollEv.com**

Mathematical induction review

Background

- Mathematical induction: Good tool for proving results where **recursion** is involved (something is defined or computed by using smaller versions of itself)
- Example: n!, the factorial function. Define **0! = 1**, and then define n! as **n * (n-1)!** for all n > 0.
- Recursive definitions always have a “base case” and then an “inductive step”
- So do proofs by induction.

Suppose we are proving: For all integers $n \geq 7, n! > 3^n$.

We would begin the proof by

- Demonstrating that $0! > 3^0$
- Demonstrating that $1! > 3^1$
- Demonstrating that $7! > 3^7$
- Assuming that $k! > 3^k$ for all integers $k \geq 7$
- Assuming that for some integer n, $k! > 3^k$ for all integers in the range $7 \leq k \leq n$
- None of these

Suppose we are proving: For all integers $n \geq 7, n! > 3^n$. Once we've established the base case, we would then

- Demonstrate that $8! > 3^8$
- Prove that $k! > 3^k$ for all integers $k \geq 7$
- Assume that $k! > 3^k$ for all integers $k \geq 7$
- Assume that for some integer n, $k! > 3^k$ for all integers in the range $7 \leq k \leq n$
- None of these

To 0

Suppose we are proving: For all integers $n \geq 7, n! > 3^n$. Once we've assumed the inductive hypothesis ($k! > 3^k$ for all integers in the range $7 \leq k \leq n$ for some n), we then

- None of these
- Prove that $n! > 3^n$
- Prove that $(n+1)! > 3^{n+1}$
- Assume that $(n+1)! > 3^{n+1}$

To 0

What this looks like in practice

Base case: We can compute that $7! = 5040$ and $3^7 = 2187$. So $7! > 3^7$.

Inductive hypothesis: Now fix a value of n and assume that $k! > 3^k$ for all $0 \leq k \leq n$.

We want to show that $(n+1)! > 3^{n+1}$.

$$
\begin{aligned}
(n+1)! &= (n+1)\cdot(n!) \\
&> (n+1)\cdot 3^n \\
&\geq (7+1)\cdot 3^n \\
&= 8\cdot 3^n \\
&> 3\cdot 3^n \\
&= 3^{n+1}
\end{aligned}
$$

Predicates

Predicate: Like a logical statement, but has a variable.

Predicates are functions from the natural numbers to {`True, False`}

Example: P(n) = "The integer n is prime". P(3) = `True`, P(6) = `False`.

Example: P(n) = "$n! > 3^n$". This returns `False` for n = 1, 2, 3, 4, 5, 6 and `True` otherwise.

The Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic. *Every integer greater than 1 is either prime or a product of primes. Furthermore, this factorization is unique up to the order of the factors.*

Has both existence and uniqueness parts.
Strategy of the existence proof: Prove it with induction because **factoring is recursive**.

```
factor(p) = p if p is prime

Otherwise if n = ab, factor(n) =
factor(a)*factor(b)
```

In groups: Work out the framework for the existence proof

The Fundamental Theorem of Arithmetic. *Every integer greater than 1 is either prime or a product of primes. Furthermore, this factorization is unique up to the order of the factors.*

Let P(n) = “n is either a prime or a product of primes”.

- What is the base case here, and what do you need to do to prove it?
- What is the inductive hypothesis?
- What would you need to prove, once you assume the inductive hypothesis?

Euclid's Lemma. *Let a and b be integers, and let p be prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Theorem 4.5. *Let a, b, and c be integers. If $c \mid ab$ and $\gcd(c, a) = 1$, then $c \mid b$.*

Euclid's Lemma (Strong Form)**.** *Let $a_1, a_2, \ldots, a_n$ be integers, and let p be prime. If $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_i$ for some i with $1 \leq i \leq n$.*

For uniqueness, first note that 2 is prime and therefore cannot be factored in any non-trivial way. Thus, 2 (like any prime) has a unique—and trivial—prime factorization.? Now assume that, for some $n \geq 2$, every integer between 2 and n, inclusive, has a factorization into primes that is unique up to the order of the factors. Suppose also that for some primes $p_1, p_2, \ldots p_j$, and $q_1, q_2, \ldots, q_k$,

$$\underline{\hspace{5cm}} = n + 1 = \underline{\hspace{5cm}}.$$

By Euclid's Lemma, $p_1 \mid q_i$ for some i with $1 \leq i \leq k$.? Without loss of generality, assume that $p_1 \mid q_1$.? Then $p_1 = q_1$,? and so

$$p_2 p_3 \cdots p_j = q_2 q_3 \cdots q_k \leq n.^{?} \tag{4.3}$$

The induction hypothesis then implies that $j = k$,? and the factors on each side of equation (4.3) can be re-ordered and/or re-numbered so that $p_i = q_i$ for all i with $2 \leq i \leq j = k$.? Thus, the factorization of $n + 1$ into primes is unique up to the order of the factors, as desired. ■

Feedback:

http://gvsu.edu/s/1zN