A Group Activites Approach to Number Theory

Stefan Erickson
Dept. of Mathematics & Computer Science
Colorado College
Stefan.Erickson@ColoradoCollege.edu

July 27, 2017

Number Theory at Colorado College

- Block Plan - Every class is three and a half weeks long.

Number Theory at Colorado College

- Block Plan - Every class is three and a half weeks long.
- Students only take one class at a time, professors only teach one class at a time.

Number Theory at Colorado College

- Block Plan - Every class is three and a half weeks long.
- Students only take one class at a time, professors only teach one class at a time.
- Classes meet every day for 2.5–3 hours in morning, office hours / problem sessions in the afternoon.

Number Theory at Colorado College

- Block Plan - Every class is three and a half weeks long.
- Students only take one class at a time, professors only teach one class at a time.
- Classes meet every day for 2.5–3 hours in morning, office hours / problem sessions in the afternoon.
- Provides opportunity for in-depth group activites during class.

Teaching Philosophy

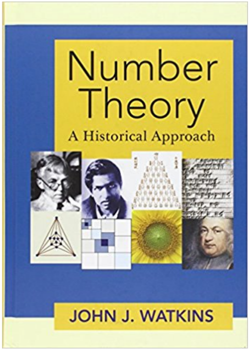
- Number Theory serves as our "introduction to proofs" course.

Teaching Philosophy

- Number Theory serves as our “introduction to proofs” course.
- Structured worksheets guide students to finding patterns.

Teaching Philosophy

- Number Theory serves as our "introduction to proofs" course.
- Structured worksheets guide students to finding patterns.
- "Number Theory: A Historical Approach" by John Watkins.



Worksheets

- Primitive Pythagorean Triples
- Linear Diophantine Equations
- Pell's Equation
- Euler's Theorem
- Primitive Roots
- Quadratic Residues
- Quadratic Reciprocity

Worksheets

- Primitive Pythagorean Triples
- Linear Diophantine Equations
- Pell's Equation
- Euler's Theorem
- Primitive Roots
- Quadratic Residues
- Quadratic Reciprocity

Powers Modulo n, Prime n

Modulo 7

$$
\begin{array}{cccccc}
1^1 \equiv 1 & 2^1 \equiv 2 & 3^1 \equiv 3 & 4^1 \equiv 4 & 5^1 \equiv 5 & 6^1 \equiv 6 \\
1^2 \equiv 1 & 2^2 \equiv 4 & 3^2 \equiv 2 & 4^2 \equiv 2 & 5^2 \equiv 4 & 6^2 \equiv 1 \\
1^3 \equiv 1 & 2^3 \equiv 1 & 3^3 \equiv 6 & 4^3 \equiv 1 & 5^3 \equiv 6 & 6^3 \equiv 6 \\
1^4 \equiv 1 & 2^4 \equiv 2 & 3^4 \equiv 4 & 4^4 \equiv 4 & 5^4 \equiv 2 & 6^4 \equiv 1 \\
1^5 \equiv 1 & 2^5 \equiv 4 & 3^5 \equiv 5 & 4^5 \equiv 2 & 5^5 \equiv 3 & 6^5 \equiv 6 \\
1^6 \equiv 1 & 2^6 \equiv 1 & 3^6 \equiv 1 & 4^6 \equiv 1 & 5^6 \equiv 1 & 6^6 \equiv 1 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots
\end{array}
$$

Powers Modulo n, Prime n

Modulo 7

$1^1 \equiv 1$	$2^1 \equiv 2$	$3^1 \equiv 3$	$4^1 \equiv 4$	$5^1 \equiv 5$	$6^1 \equiv 6$
$1^2 \equiv 1$	$2^2 \equiv 4$	$3^2 \equiv 2$	$4^2 \equiv 2$	$5^2 \equiv 4$	$6^2 \equiv 1$
$1^3 \equiv 1$	$2^3 \equiv 1$	$3^3 \equiv 6$	$4^3 \equiv 1$	$5^3 \equiv 6$	$6^3 \equiv 6$
$1^4 \equiv 1$	$2^4 \equiv 2$	$3^4 \equiv 4$	$4^4 \equiv 4$	$5^4 \equiv 2$	$6^4 \equiv 1$
$1^5 \equiv 1$	$2^5 \equiv 4$	$3^5 \equiv 5$	$4^5 \equiv 2$	$5^5 \equiv 3$	$6^5 \equiv 6$
$1^6 \equiv 1$	$2^6 \equiv 1$	$3^6 \equiv 1$	$4^6 \equiv 1$	$5^6 \equiv 1$	$6^6 \equiv 1$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Powers will eventually reach 1.

Fermat's Little Theorem

- Have students find powers modulo 11, 13, 17, and 19.

Fermat's Little Theorem

- Have students find powers modulo 11, 13, 17, and 19.
- Make a conjecture as to what is the smallest power for which *all* nonzero congruence classes are congruent 1.

Fermat's Little Theorem

- Have students find powers modulo 11, 13, 17, and 19.
- Make a conjecture as to what is the smallest power for which *all* nonzero congruence classes are congruent 1.

Theorem (Fermat, 1640)

For any prime p and integer a not divisible by p,

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

Euler's Theorem Handout

Introduction

We have already seen Fermat's Little Theorem, which states that $a^{p-1} \equiv 1 \pmod{p}$ *for any* $p \nmid a$. *Unfortunately, this only applies for prime numbers* p. *Our goal today is to generalize to composite numbers* n.

Euler's Theorem Handout, Question 1

Question 1

Start by taking powers of a modulo n for all numbers a between 1 and $n-1$*, when* $n =$ *4, 6, 8, 9, 10, 12, and 15 (you should divide and conquer in your groups). Which numbers between 1 and* $n-1$ *will eventually have a power equal to 1 modulo n? Do you notice any patterns in the smallest powers for which are equal to 1 modulo n?*

Euler's Theorem Handout, Question 1

For composite n, not all powers will eventually equal 1.

$$\begin{aligned}
2^1 &\equiv 2 \pmod{10}\\
2^2 &\equiv 4 \pmod{10}\\
2^3 &\equiv 8 \pmod{10}\\
2^4 &\equiv 6 \pmod{10}\\
2^5 &\equiv 2 \pmod{10}\\
&\vdots
\end{aligned}$$

Euler's Theorem Handout, Question 1

Modulo 10

$$\begin{array}{llll} 1^1 \equiv 1 & 3^1 \equiv 3 & 7^1 \equiv 7 & 9^1 \equiv 9 \\ 1^2 \equiv 1 & 3^2 \equiv 9 & 7^2 \equiv 9 & 9^2 \equiv 1 \\ 1^3 \equiv 1 & 3^3 \equiv 7 & 7^3 \equiv 3 & 9^3 \equiv 9 \\ 1^4 \equiv 1 & 3^4 \equiv 1 & 7^4 \equiv 1 & 9^4 \equiv 1 \\ \vdots & \vdots & \vdots & \vdots \end{array}$$

Euler's Theorem Handout, Question 1

Modulo 10

$$\begin{array}{cccc}
1^1 \equiv 1 & 3^1 \equiv 3 & 7^1 \equiv 7 & 9^1 \equiv 9 \\
1^2 \equiv 1 & 3^2 \equiv 9 & 7^2 \equiv 9 & 9^2 \equiv 1 \\
1^3 \equiv 1 & 3^3 \equiv 7 & 7^3 \equiv 3 & 9^3 \equiv 9 \\
1^4 \equiv 1 & 3^4 \equiv 1 & 7^4 \equiv 1 & 9^4 \equiv 1 \\
\vdots & \vdots & \vdots & \vdots
\end{array}$$

If the integer a is relatively prime to n, the powers of a will eventually reach 1.

Euler's Theorem Handout, Question 2

The numbers a for which $a^k \equiv 1 \pmod{n}$ *appear to be those which are relatively prime to n. Perhaps the set of numbers between* 1 *and n which are relatively prime to n is relevant. Make a table for each n between 2 and 12 of the set of relatively prime a between* 1 *and n and record how many elements are in each set.*

Euler's Theorem Handout, Question 2

The numbers a for which $a^k \equiv 1 \pmod{n}$ *appear to be those which are relatively prime to n. Perhaps the set of numbers between* 1 *and n which are relatively prime to n is relevant. Make a table for each n between 2 and 12 of the set of relatively prime a between* 1 *and n and record how many elements are in each set.*

n	2	3	4	5	6	7	8	9	10	11	12
#	1	2	2	4	2	6	4	6	4	10	4

Euler's Theorem Handout, Question 3

Question 3

The size of each set is seemingly random for the first 12 values of n, but maybe there's a deeper pattern. Let $\phi(n)$ *be the number of elements between* 1 *and* n *which relatively prime to* n*. What do know about* $\phi(p)$ *for any prime number* p*? Find the values of* $\phi(4)$, $\phi(9)$, $\phi(25)$, *and* $\phi(49)$*. What do you think* $\phi(p^2)$ *is? Explain why your formula for* $\phi(p^2)$ *is true for all primes* p*.*

Euler's Theorem Handout, Question 3

p	2	3	5	7	11	13	17	19
$\phi(p)$	1	2	4	6	10	12	16	18

Conjecture

For all primes p, $\phi(p) = p - 1$.

Euler's Theorem Handout, Question 3

p	2	3	5	7	11	13	17	19
$\phi(p)$	1	2	4	6	10	12	16	18

Conjecture

For all primes p, $\phi(p) = p - 1$.

p^2	4	9	25	49
$\phi(p^2)$	2	6	20	42

Conjecture

For all prime p, $\phi(p^2) = p^2 - p = p \cdot (p - 1)$.

Euler's Theorem Handout, Question 3

Question 3 (Cont.)

Now try $\phi(8)$, $\phi(16)$, *and* $\phi(32)$. *From the values of* $\phi(2^n)$, *what do you think a formula for* $\phi(p^n)$ *would be? Check this formula with* $\phi(27)$ *and (if you're brave)* $\phi(81)$. *Explain why your formula for* $\phi(p^n)$ *is true for all primes* p.

Euler's Theorem Handout, Question 3

2^n	2	4	8	16	32
$\phi(2^n)$	1	2	4	8	16

Conjecture

$\phi(2^n) = 2^{n-1} = 2^n - 2^{n-1}$.

Euler's Theorem Handout, Question 3

2^n	2	4	8	16	32
$\phi(2^n)$	1	2	4	8	16

Conjecture

$\phi(2^n) = 2^{n-1} = 2^n - 2^{n-1}$.

3^n	3	9	27	81
$\phi(2^n)$	2	6	18	54

Conjecture

$\phi(3^n) = 2 \cdot 3^{n-1} = 3^n - 3^{n-1}$.

Euler's Theorem Handout, Question 3

2^n	2	4	8	16	32
$\phi(2^n)$	1	2	4	8	16

Conjecture

$\phi(2^n) = 2^{n-1} = 2^n - 2^{n-1}$.

3^n	3	9	27	81
$\phi(2^n)$	2	6	18	54

Conjecture

$\phi(3^n) = 2 \cdot 3^{n-1} = 3^n - 3^{n-1}$.

$$\boxed{\phi(p^n) = p^n - p^{n-1} = p^{n-1} \cdot (p-1)}$$

Euler's Theorem Handout, Question 4

Question 4

Now try the product of two odd prime numbers, such as $\phi(15)$*,* $\phi(21)$*,* $\phi(33)$*, and* $\phi(35)$*. What is a formula for* $\phi(pq)$ *for distinct primes* p *and* q*? Explain why your formula for* $\phi(pq)$ *is true for all distinct primes* p *and* q*.*

Euler's Theorem Handout, Question 4

Question 4

Now try the product of two odd prime numbers, such as $\phi(15)$, $\phi(21)$, $\phi(33)$, and $\phi(35)$. What is a formula for $\phi(pq)$ for distinct primes p and q? Explain why your formula for $\phi(pq)$ is true for all distinct primes p and q.

n	15	21	33	35
$\phi(n)$	8	12	20	24

Euler's Theorem Handout, Question 4

Question 4

Now try the product of two odd prime numbers, such as $\phi(15)$, $\phi(21)$, $\phi(33)$, *and* $\phi(35)$. *What is a formula for* $\phi(pq)$ *for distinct primes* p *and* q? *Explain why your formula for* $\phi(pq)$ *is true for all distinct primes* p *and* q.

n	$3 \cdot 5$	$3 \cdot 7$	$3 \cdot 11$	$5 \cdot 7$
$\phi(n)$	$2 \cdot 4$	$2 \cdot 6$	$2 \cdot 10$	$4 \cdot 6$

Euler's Theorem Handout, Question 4

Question 4

Now try the product of two odd prime numbers, such as $\phi(15)$, $\phi(21)$, $\phi(33)$, and $\phi(35)$. What is a formula for $\phi(pq)$ for distinct primes p and q? Explain why your formula for $\phi(pq)$ is true for all distinct primes p and q.

n	$3 \cdot 5$	$3 \cdot 7$	$3 \cdot 11$	$5 \cdot 7$
$\phi(n)$	$2 \cdot 4$	$2 \cdot 6$	$2 \cdot 10$	$4 \cdot 6$

$$\boxed{\phi(p \cdot q) = (p-1) \cdot (q-1)}$$

Euler's Theorem Handout, Question 4

Question 4 (Cntd.)

Now try other products, such as $\phi(6)$, $\phi(12)$, $\phi(18)$, $\phi(20)$, $\phi(24)$, *and* $\phi(30)$. *On the basis of these investigations, find a general formula for* $\phi(n)$ *based on the prime factorization of* n.

n	6	12	18	20	24
$\phi(n)$	2	4	6	8	8

$$\boxed{\phi(p_1^{e_1}\cdots p_k^{e_k}) = p_1^{e_1-1}(p_1-1)\cdots p_k^{e_k-1}(p_k-1) = \phi(p_1^{e_1})\cdots\phi(p_k^{e_k})}$$

Euler's Theorem Handout, Question 5

Question 5

Let's return to the powers of a modulo n. Is there any relationship between the smallest powers of a for which $a^k \equiv 1 \pmod{n}$ *and the values of* $\phi(n)$*? Make a conjecture similar to Fermat's Little Theorem which holds for any modulus n. Test your conjecture for all the powers you found in #1.*

Euler's Theorem Handout, Question 5

Fact: $\phi(10) = 4$.

Euler's Theorem Handout, Question 5

Fact: $\phi(10) = 4$.

<u>Modulo 10</u>

$$\begin{array}{cccc}
1^1 \equiv 1 & 3^1 \equiv 3 & 7^1 \equiv 7 & 9^1 \equiv 9 \\
1^2 \equiv 1 & 3^2 \equiv 9 & 7^2 \equiv 9 & 9^2 \equiv 1 \\
1^3 \equiv 1 & 3^3 \equiv 7 & 7^3 \equiv 3 & 9^3 \equiv 9 \\
1^4 \equiv 1 & 3^4 \equiv 1 & 7^4 \equiv 1 & 9^4 \equiv 1 \\
\vdots & \vdots & \vdots & \vdots
\end{array}$$

Euler's Theorem Handout, Question 5

Fact: $\phi(10) = 4$.

<u>Modulo 10</u>

$1^1 \equiv 1$	$3^1 \equiv 3$	$7^1 \equiv 7$	$9^1 \equiv 9$
$1^2 \equiv 1$	$3^2 \equiv 9$	$7^2 \equiv 9$	$9^2 \equiv 1$
$1^3 \equiv 1$	$3^3 \equiv 7$	$7^3 \equiv 3$	$9^3 \equiv 9$
$1^4 \equiv 1$	$3^4 \equiv 1$	$7^4 \equiv 1$	$9^4 \equiv 1$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Conjecture

If a and n are relatively prime, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Euler's Theorem Handout, Question 6

Question 6

Prove your conjecture. Here's an idea. Take any fixed a which is relatively prime to n. What happens to the values of $ax \pmod{n}$ *as x ranges through all number relatively prime to n? Try this explicitly for* $n = 9$, $n = 10$, *and* $n = 15$. *Notice that you'll get exactly the same product over all* $ax \pmod{n}$ *as you do when you take a product over all* $x \pmod{n}$ *when x ranges through all numbers relatively prime to n. Use this fact to prove your conjecture. This generalized version is known as Euler's Theorem.*

Conclusions

- Looking from a different point of view can reveal patterns.

Conclusions

- Looking from a different point of view can reveal patterns.
- Working collaboratively and discussion leads to understanding.

Conclusions

- Looking from a different point of view can reveal patterns.
- Working collaboratively and discussion leads to understanding.
- Finding patterns in numbers is fun!

Conclusions

- Looking from a different point of view can reveal patterns.
- Working collaboratively and discussion leads to understanding.
- Finding patterns in numbers is fun!