Lesson 8: The Power of Algebra—Finding Primes

Classwork

Opening Exercise: When is $2^n - 1$ prime and when is it composite?

Complete the table to investigate which numbers of the form $2^n - 1$ are prime and which are composite.

Exponent n	Expression $2^n - 1$	Value	Prime or Composite? Justify your answer if composite.
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			

What patterns do you notice in this table about which expressions are prime and which are composite?

Example 1: Proving a Conjecture

Conjecture: If m is a positive odd composite number, then $2^m - 1$ is a composite number.

Start with an identity: $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots x^1 + 1)$

In this case, $x = 2$, so the identity above becomes:

$$\begin{aligned} 2^m - 1 &= (2-1)(2^{m-1} + 2^{m-2} + \cdots + 2^1 + 1) \\ &= (2^{m-1} + 2^{m-2} + \cdots + 2^1 + 1), \end{aligned}$$

and it is not clear whether or not $2^m - 1$ is composite.

Rewrite the expression: Let $m = ab$ be a positive odd composite number. Then a and b must also be odd, or else the product ab would be even. The smallest such number m is 9, so we have $a \geq 3$ and $b \geq 3$.

Then we have

$$\begin{aligned} 2^m - 1 &= (2^a)^b - 1 \\ &= (2^a - 1)\underbrace{((2^a)^{b-1} + (2^a)^{b-2} + \cdots + (2^a)^1 + 1)}_{\text{Some number larger than 1}}. \end{aligned}$$

Since $a \geq 3$, we have $2^a \geq 8$; thus, $2^a - 1 \geq 7$. Since the other factor is also larger than 1, $2^m - 1$ is composite and we have proven our conjecture.

Exercises 1–3

For Exercises 1–3, find a factor of each expression using the method discussed in Example 1.

1. $2^{15} - 1$

2. $2^{99} - 1$

3. $2^{537} - 1$ (Hint: 537 is the product of two prime numbers that are both less than 50.)

Exercise 4: How quickly can a computer factor a very large number?

4. How long would it take a computer to factor some squares of very large prime numbers?

   The time in seconds required to factor an n-digit number of the form p^2, where p is a large prime, can roughly be approximated by $f(n) = 3.4 \times 10^{(n-13)/2}$. Some values of this function are listed in the table below.

p	p^2	Number of Digits	Time needed to factor the number (sec)
10,007	100,140,049	9	0.034
100,003	10,000,600,009	11	0.34
1,000,003	1,000,006,000,009	13	3.4
10,000,019	100,000,380,000,361	15	34
100,000,007	10,000,001,400,000,049	17	340
1000,000,007	1,000,000,014,000,000,049	19	3,400

   Use the function given above to determine how long it would take this computer to factor a number that contains 32 digits.

Problem Set

1. Factor $4^{12} - 1$ in two different ways using the identity $x^n - a^n = (x - a)(x^n + ax^{n-1} + a^2x^{n-2} + \cdots + a^n)$ and the difference of squares identity.

2. Factor $2^{12} + 1$ using the identity $x^n + a^n = (x + a)(x^n - ax^{n-1} + a^2x^{n-2} - \cdots + a^n)$ for odd numbers n.

3. Is $10{,}000{,}000{,}001$ prime? Explain your reasoning.

4. Explain why $2^n - 1$ is never prime if n is a composite number.

5. Fermat numbers are of the form $2^n + 1$ where n is positive integer.
   a. Create a table of Fermat numbers for odd values of n up to 9.

n	$2^n + 1$
1	
3	
5	
7	
9	

   b. Explain why if n is odd, the Fermat number $2^n + 1$ will always be divisible by 3.
   c. Complete the table of values for even values of n up to 12.

n	$2^n + 1$
2	
4	
6	
8	
10	
12	

   d. Show that if n can be written in the form $2k$ where k is odd, then $2^n + 1$ is divisible by 5.
   e. Which even numbers are not divisible by an odd number? Make a conjecture about the only Fermat numbers that might be prime.

6. Complete this table to explore which numbers can be expressed as the difference of two perfect squares.

Number	Difference of Two Squares	Number	Difference of Two Squares
1	$1^2 - 0^2 = 1 - 0 = 1$	11	
2	Not possible	12	
3	$2^2 - 1^2 = 4 - 1 = 3$	13	
4	$2^2 - 0^2 = 4 - 0 = 4$	14	
5		15	
6		16	
7		17	
8		18	
9		19	
10		20	

   a. For which odd numbers does it appear to be possible to write the number as the difference of two squares?
   b. For which even numbers does it appear to be possible to write the number as the difference of two squares?
   c. Suppose that n is an odd number that can be expressed as $n = a^2 - b^2$ for positive integers a and b. What do you notice about a and b?
   d. Suppose that n is an even number that can be expressed as $n = a^2 - b^2$ for positive integers a and b. What do you notice about a and b?

7. Express the numbers from 21 to 30 as the difference of two squares, if possible.

8. Prove this conjecture: Every positive odd number m can be expressed as the difference of the squares of two consecutive numbers that sum to the original number m.
   a. Let m be a positive odd number. Then for some integer n, $m = 2n + 1$. We will look at the consecutive integers n and $n + 1$. Show that $n + (n + 1) = m$.
   b. What is the difference of squares of $n + 1$ and n?
   c. What can you conclude from parts (a) and (b)?

9. Prove this conjecture: Every positive multiple of 4 can be expressed as the difference of squares of two numbers that differ by 2. Use the table below to organize your work for parts (a)–(c).

   a. Write each multiple of 4 in the table as a difference of squares.

n	$4n$	*Difference of squares* $a^2 - b^2$	a	b
1	4	$2^2 - 0^2$	2	0
2				
3				
4				
5				
n	$4n$	$(\quad)^2 - (\quad)^2$		

   b. What do you notice about the numbers a and b that are squared? How do they relate to the number n?

   c. Given a positive integer of the form $4n$, prove that there are integers a and b so that $4n = a^2 - b^2$ and that $a - b = 2$. (Hint: Refer to parts (a) and (b) for the relationship between n and a and b.)

10. The steps below prove that the only positive even numbers that can be written as a difference of square integers are the multiples of 4. That is, completing this exercise will prove that is it impossible to write a number of the form $4n - 2$ as a difference of square integers.

   a. Let m be a positive even integer that we can write as the difference of square integers $m = a^2 - b^2$. Then $m = (a + b)(a - b)$ for integers a and b. How do we know that either a and b are both even or a and b are both odd?

   b. Is $a + b$ even or odd? What about $a - b$? How do you know?

   c. Is 2 a factor of $a + b$? Is 2 a factor of $a - b$? Is 4 a factor of $(a + b)(a - b)$? Explain how you know.

   d. Is 4 a factor of any integer of the form $4n - 2$?

   e. What can you conclude from your work in parts (a)–(d)?

11. Explain why the prime number 17 can only be expressed as the difference of two squares in only one way, but the composite number 24 can be expressed as the difference of two squares in more than one way.

12. Explain why you cannot use the factors of 3 and 8 to rewrite 24 as the difference of two square integers.