Lesson 8: The Power of Algebra—Finding Primes

Classwork

Opening Exercise: When is prime and when is it composite?

Complete the table to investigate which numbers of the form are prime and which are composite.

|  |  |  |  |
| --- | --- | --- | --- |
| Exponent | Expression | Value | Prime or Composite?Justify your answer if composite. |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

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

Example 1: Proving a Conjecture

Conjecture: If is a positive odd composite number, then is a composite number.

Start with an identity:

In this case, , so the identity above becomes:

and it is not clear whether or not is composite.

Rewrite the expression: Let be a positive odd composite number. Then and must also be odd, or else the product would be even. The smallest such number is , so we have and .

Then we have

Since , we have ; thus, . Since the other factor is also larger than 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. (Hint: is the product of two prime numbers that are both less than )

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

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

The time in seconds required to factor an -digit number of the form , where is a large prime, can roughly be approximated by . Some values of this function are listed in the table below.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | Number of Digits | Time needed to factor the number(sec) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

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

Problem Set

1. Factor in two different ways using the identity and the difference of squares identity.
2. Factor using the identity for odd numbers .
3. Is prime? Explain your reasoning.
4. Explain why is never prime if is a composite number.
5. Fermat numbers are of the form where is positive integer.
	1. Create a table of Fermat numbers for odd values of up to .

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

* 1. Explain why if is odd, the Fermat number will always be divisible by .
	2. Complete the table of values for even values of up to .

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

* 1. Show that if can be written in the form where is odd, then is divisible by .
	2. Which even numbers are not divisible by an odd number? Make a conjecture about the only Fermat numbers that might be prime.
1. 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 |
|  |  |  |  |
|  | Not possible |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

* 1. For which odd numbers does it appear to be possible to write the number as the difference of two squares?
	2. For which even numbers does it appear to be possible to write the number as the difference of two squares?
	3. Suppose that is an odd number that can be expressed as for positive integers and . What do you notice about and
	4. Suppose that is an even number that can be expressed as for positive integers and . What do you notice about and
1. Express the numbers from to as the difference of two squares, if possible.
2. Prove this conjecture: Every positive odd number can be expressed as the difference of the squares of two consecutive numbers that sum to the original number .
	1. Let be a positive odd number. Then for some integer , . We will look at the consecutive integers and . Show that .
	2. What is the difference of squares of and ?
	3. What can you conclude from parts (a) and (b)?
3. Prove this conjecture: Every positive multiple of can be expressed as the difference of squares of two numbers that differ by. Use the table below to organize your work for parts (a)–(c).
	1. Write each multiple of in the table as a difference of squares.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | *Difference of squares* |  |  |
|  |  |  |  | *0* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

* 1. What do you notice about the numbers and that are squared? How do they relate to the number ?
	2. Given a positive integer of the form , prove that there are integers and so that and that . (Hint: Refer to parts (a) and (b) for the relationship between and and .)
1. The steps below prove that the only positive even numbers that can be written as a difference of square integers are the multiples of That is, completing this exercise will prove that is it impossible to write a number of the form as a difference of square integers.
	1. Let be a positive even integer that we can write as the difference of square integers . Then for integers and . How do we know that either and are both even or and are both odd?
	2. Is even or odd? What about ? How do you know?
	3. Is a factor of ? Is a factor of ? Is a factor of ? Explain how you know.
	4. Is a factor of any integer of the form ?
	5. What can you conclude from your work in parts (a)–(d)?
2. Explain why the prime number can only be expressed as the difference of two squares in only one way, but the composite number can be expressed as the difference of two squares in more than one way.
3. Explain why you cannot use the factors of and to rewrite as the difference of two square integers.