Lesson 8: The Power of Algebra—Finding Primes

Student Outcomes

- Students apply polynomial identities to the detection of prime numbers.

Lesson Notes

This lesson applies the identities students have been working with in previous lessons to finding prime numbers, a rich topic with a strong historical background. Many famous mathematicians have puzzled over prime numbers, and their work is the foundation for mathematics used today in the RSA encryption algorithm that provides for secure internet transmissions. This is an engaging topic for students and is readily accessible to them because of its current use in providing safe and secure electronic communications and transactions. Students will be actively engaging several mathematical practice standards during this lesson, including making sense of problems (MP.1), looking for patterns, and seeing the structure in expressions (MP.7 and MP.8), as they investigate patterns with prime numbers. The lesson includes many opportunities to prove conjectures (MP.3) as students gain experience using algebraic properties to prove statements about integers. Several excellent resources are available for students wishing to learn more about prime numbers, their history, and their application to encryption and decryption. A good starting place for additional exploration about prime numbers is the website The Prime Pages, http://primes.utm.edu/.

Classwork

Opening (10 minutes)

To motivate students, show the YouTube video on RSA encryption (http://www.youtube.com/watch?v=M7kEpw1tn50) to the class. This video will introduce students to encryption and huge numbers. Encryption algorithms are the basis of all secure internet transactions. Today, many encryption algorithms rely on very large prime numbers or very large composite numbers that are the product of two primes to create an encryption key. Often these numbers are Mersenne Primes—primes of the form $2^p - 1$, where p is itself prime. Interestingly, not all numbers in this form are prime. As of December 2013, only 43 Mersenne Primes have been discovered. Encourage students to research the following terms: Mersenne Primes, Data Encryption, and RSA. The Opening Exercise along with the first examples engage students in the exploration of large primes.

Mathematicians have tried for centuries to find a formula that always yields a prime number but have been unsuccessful in their quest. The search for large prime numbers and a formula that will generate all the prime numbers has provided fertile ground for work in number theory. The mathematician Pierre de Fermat (1601–1665, France) applied the difference of two squares identity to factor very large integers as the product of two prime numbers. Up to this point, we have worked with numbers that can be expressed as the difference of two perfect squares. If a prime number could be written as a difference of perfect squares $a^2 - b^2$, then it would have to be of the form $(a + b)(a - b)$, where a and b are consecutive whole numbers and $a + b$ is prime. The challenge is that not every pair of consecutive whole numbers yields a prime number when added. For example, $3 + 4 = 7$ is prime, but $4 + 5 = 9$ is not. This idea is further addressed in the last exercise and in the Problem Set.

Opening Exercise (10 minutes): When is $2^n - 1$ prime and when is it composite?

Before beginning this exercise, have students predict when an expression in this form will be prime and when it will be composite. Questions like this are ideal places to engage students in constructing viable arguments.

MP.3

- When will this expression be prime and when will it be composite?
  - *Student responses will vary. Some may say always prime or always composite. A response that goes back to the identity $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + 1)$ from the previous lesson is showing some good initial thinking.*

Students should work the Opening Exercise in small groups. After about seven minutes of group work, have one student from each group come up and fill in the table values and the supporting work. Then, lead a whole group discussion to debrief this problem.

Scaffolding:

For more advanced students, consider posing the question: Can you construct an expression what will always yield a prime number? Do this before starting the Opening Exercise and then ask them to test their expressions.

If students are having a hard time constructing an expression, consider asking the following questions: Can you construct an expression that will always yield an even number? Can you construct an expression that will always yield an odd number?

If n is an integer, then n is always an even number and $2n + 1$ is always an odd number.

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	$2^1 - 1$	1	*Prime*
2	$2^2 - 1$	3	*Prime*
3	$2^3 - 1$	7	*Prime*
4	$2^4 - 1$	15	*Composite* $(3 \cdot 5)$
5	$2^5 - 1$	31	*Prime*
6	$2^6 - 1$	63	*Composite* $(7 \cdot 9)$
7	$2^7 - 1$	127	*Prime*
8	$2^8 - 1$	255	*Composite (ends in a 5)*
9	$2^9 - 1$	511	*Composite* $(7 \cdot 73)$
10	$2^{10} - 1$	1023	*Composite* $(32 - 1)(32 + 1)$
11	$2^{11} - 1$	2047	*Composite* $(23 \cdot 89)$

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

Answers will vary. Suggested responses are in the discussion questions below.

MP.2 MP.7 & MP.8

Encourage students to use tools strategically as they work with these problems. They should have a calculator available to determine if the larger numbers are composite. When debriefing, point out the fact that students can use the difference of two squares identity to factor these expressions when the exponent is an even number.

Use these questions to lead a short discussion on the results of this Opening Exercise.

MP.2 MP.7 & MP.8

- What patterns do you notice about which expressions are composite and which are prime?
  - *When the exponent was an even number greater than 2, the result was composite and can be factored using this identity:* $2^{2n} - 1 = (2^n + 1)(2^n - 1)$.
  - *When the exponent is a prime number, the result is sometimes prime and sometimes not prime.* $2^{11} - 1$ *was the first number with a prime exponent that was composite.*
  - *When the exponent is a composite odd number, the expression appears to be composite but we have yet to prove that.*

The statements above are examples of the types of patterns students should notice as they complete the Opening Exercise. If your class was not able to prove that the case for even exponents resulted in a composite number, encourage them to consider the identities we learned in the last lesson involving the difference of two squares. See if they can solve the problem with that hint. Of course, that technique does not work when the exponent is odd. Make sure students have articulated the answer to the last problem. To transition to the next section, ask students how they might prove that $2^{ab} - 1$ is composite when the exponent ab is an odd composite number.

Example 1 (5 minutes): Proving a Conjecture

This example and the next exercise prove patterns students noticed in the table in the Opening Exercise. Some scaffolding is provided, but feel free to adjust as needed for your students. Give students who need less support the conjecture on the board for Example 1 (without the additional scaffolding on the student pages); others may need more assistance to get started.

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 (4 minutes)

In these exercises, students confirm the conjecture proven in Example 1. Emphasize that it does not really matter what the 2nd factor is once you know the first one. There is more than one way to solve each of these problems depending on how students decide to factor the exponent on the 2. Students should work in small groups on these exercises. Encourage them to use a calculator to determine the prime factors of 537 in Exercise 3. Have different groups present their results.

Exercises 1–3

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

1. $2^{15}-1$

$$(2^5)^3-1=(2^5-1)((2^5)^2+2^5+1)=(31)(\underbrace{32^2+32+1}_{\text{Some number larger than 1}})$$

Thus, 31 is a factor of $2^{15}-1$.

2. $2^{99}-1$

$$(2^3)^{33}=(2^3-1)(\underbrace{8^{32}+8^{31}+\cdots+8+1}_{\text{Some number larger than 1}})$$

Thus, 7 is a factor of $2^{99}-1$.

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

Using a calculator we see that $537=17\cdot 31$, *so*

$$(2^{17})^{31}-1=(2^{17}-1)(\underbrace{(2^{17})^{30}+\cdots+2^{17}+1}_{\text{Some number larger than 1}}).$$

Thus, $2^{17}-1$ is a factor of $2^{537}-1$.

Discussion (4 minutes)

Cryptography is the science of making codes, and *cryptanalysis* is the science of breaking codes. The rise of internet commerce has created a demand for encoding methods that are hard for unintended observers to decipher. One encryption method, known as RSA encryption, uses very large numbers with hundreds of digits that are the product of two primes; the product of the prime factors is called the *key*. The key itself is made public so anyone can encode using this system, but in order to break the code, you would have to know how to factor the key, and that is what is so difficult.

- You had a hint in Exercise 3 that made it easier for you to factor a very large number, but what if you do not have any hints?
  - *It would be almost impossible to factor the number because you would have to check all the prime numbers up to the square root of the exponent to find the factors.*

If you know the key, then decoding is not particularly difficult. Programmers select a number that is almost impossible to factor without significant time and computing power and use this as the key to encode data and communications. The last exercise illuminates the logic behind modern encryption algorithms.

Exercise 4 (6 minutes): How quickly can a computer factor a very large number?

When we want to determine if a number m is prime, we can just try dividing by every prime number p that is less than $\sqrt{m}$. This will take the longest time if m happens to be a perfect square. In this exercise, students consider the speed it takes a certain computer algorithm to factor a square of a large prime number; this is the case where it should take the algorithm the longest to find the factorization. Actual algorithms used to factor large numbers are quicker than this, but it still takes a really long time and works to the advantage of people who want to encrypt information electronically using these large numbers. Introduce the problem and review the table as a whole class; then, have students answer the question in small groups. Have students working in groups apply the given function to estimate the time it would take to factor a 32-digit number. Make sure they convert their answer to years. Because we are using an exponential function, the factorization time grown very rapidly. Take the time after Exercise 4 to remind students that exponential functions increase very rapidly over intervals of equal length, ideas that were introduced in Algebra I and will be revisited in Module 3 of Algebra II.

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.

Using the given function, $f(32) = 1.08 \times 10^{10}$ seconds $= 1.80 \times 10^{8}$ minutes $= 3 \times 10^{6}$ hours $= 125,000$ days, which is about 342.5 years.

After allowing groups to take a few minutes to evaluate the function and convert their answer to years, connect this exercise to the context of this situation by summarizing the following points.

- Using a very fast personal computer with a straightforward algorithm, it would take about 342 years to factor a 32-digit number, making any secret message encoded with that number obsolete before it could be cracked with that computer.
- However, we have extremely fast computers (much faster than one personal computer) and very efficient algorithms designed for those computers for factoring numbers. These computers can factor a number thousands of times faster than the computer used above, but they are still not fast enough to factor huge composite numbers in a reasonable amount of time.
- In 2009, computer scientists were able to factor a 232-digit number in two years by distributing the work over hundreds of fast computers running at the same time. That means any message encoded using that 232-digit number would take two years to decipher, by which time the message would no longer be relevant. Numbers used to encode secret messages typically contain over 300 digits, and extremely important secret messages use numbers that have over 600 digits—a far bigger number than any bank of computers can currently factor in a reasonable amount of time.

Closing (2 minutes)

There are better ways of factoring numbers than just checking all of the factors, but even advanced methods take a long time to execute. Products of primes of the magnitude of 2^{2048} are almost impossible to factor in a reasonable amount of time, which is how mathematics is used to guarantee the security of electronic transactions. Give students a few minutes to summarize what they have learned in writing or by discussing it with a partner before starting the Exit Ticket.

- Polynomial identities can help us prove conjectures about numbers and make calculations easier.
- The field of number theory has contributed greatly to the fields of cryptography and cryptanalysis (code-making and code-breaking).

Exit Ticket (4 minutes)

Name _____ Date _____

Lesson 8: The Power of Algebra—Finding Primes

Exit Ticket

Express the prime number 31 in the form $2^p - 1$ where p is a prime number and as a difference of two perfect squares using the identity $(a + b)(a - b) = a^2 - b^2$.

Exit Ticket Sample Solutions

Express the prime number 31 in the form $2^p - 1$ where p is a prime number and as a difference of two perfect squares using the identity $(a+b)(a-b) = a^2 - b^2$.

$$31 = (16-15)(16+15)$$
$$= 16^2 - 15^2$$

$$31 = 2^5 - 1$$

Problem Set Sample Solutions

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.**

$$(4^6 - 1)(4^6 + 1)$$
$$(4-1)(4^{11} + 4^{10} + \ldots + 4 + 1)$$

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.**

$$(2^4)^3 + 1 = (2^4 + 1)((2^4)^2 - 2^4 + 1)$$

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

No, because it is of the form $10^{10} + 1$, which could be written as $(10^2)^5 + 1 = (10^2 + 1)((10^2)^4 - \cdots + 1)$.

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

If n is composite, then it can be written in the form $n = ab$, where a and b are integers larger than 1. Then $2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)((2^a)^{b-1} + \cdots + 2^a + 1)$. For $a > 1$, this number will be composite because $2^a - 1$ will be larger than 1.

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	$2^1 + 1 = 3$
3	$2^3 + 1 = 9$
5	$2^5 + 1 = 33$
7	$2^7 + 1 = 129$
9	$2^9 + 1 = 513$

   b. **Explain why if n is odd, the Fermat number $2^n + 1$ will always be divisible by 3.**

The Fermat number $2^n + 1$ will factor as $(2+1)(2^{n-1} - 2^{n-2} + \cdots + 1)$ using the identity in Exercise 2.

c. Complete the table of values for even values of n up to 12.

n	$2^n + 1$
2	$2^2 + 1 = 5$
4	$2^4 + 1 = 17$
6	$2^6 + 1 = 65$
8	$2^8 + 1 = 257$
10	$2^{10} + 1 = 1,025$
12	$2^{12} + 1 = 4,097$

d. Show that if n can be written in the form $2k$ where k is odd, then $2^n + 1$ is divisible by 5.

Let $n = 2k$, where k is odd. Then $2^n + 1 = 2^{2k} + 1 = (2^2)^k + 1 = (2^2 + 1)\underbrace{((2^2)^{k-1} + \cdots + 2^2 + 1)}_{\text{number larger than 1}}$.

Since $2^2 + 1 = 5$, we know that 5 is a factor of $2^n + 1$. This only holds when k is an odd number because that is the only case when we can factor expressions of the form $x^k + 1$.

e. Which even numbers are not divisible by an odd number? Make a conjecture about the only Fermat numbers that might be prime.

The powers of 2 are the only positive integers that are not divisible by any odd numbers. This implies that when the exponent n in $2^n + 1$ is a power of 2, the Fermat number $2^n + 1$ 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	$6^2 - 5^2 = 36 - 25 = 11$
2	Not possible	12	$4^2 - 2^2 = 16 - 4 = 12$
3	$2^2 - 1^2 = 4 - 1 = 3$	13	$7^2 - 6^2 = 49 - 36 = 13$
4	$2^2 - 0^2 = 4 - 0 = 4$	14	*Not possible*
5	$3^2 - 2^2 = 9 - 4 = 5$	15	$8^2 - 7^2 = 64 - 49 = 15$
6	*Not possible*	16	$5^2 - 3^2 = 25 - 9 = 16$
7	$4^2 - 3^2 = 16 - 9 = 7$	17	$9^2 - 8^2 = 81 - 64 = 17$
8	$3^2 - 1^2 = 9 - 1 = 8$	18	*Not possible*
9	$5^2 - 4^2 = 25 - 16 = 9$	19	$10^2 - 9^2 = 100 - 81 = 19$
10	*Not possible*	20	$6^2 - 4^2 = 36 - 16 = 20$

a. For which odd numbers does it appear to be possible to write the number as the difference of two squares?

It appears that we can write any positive odd 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?

It appears that we can write any multiple of 4 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?

When n is odd, a and b are consecutive whole numbers and $a + b = n$.

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?

When n is an even number that can be written as a difference of squares, then n is a multiple of 4, and a and b are either consecutive even integers or consecutive odd integers. We also have $a + b = \frac{n}{2}$.

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

This is not possible for 22, 26, and 30. Otherwise we have the following.

$21 = 11^2 - 10^2$
$23 = 12^2 - 11^2$
$24 = 7^2 - 5^2$
$25 = 13^2 - 12^2$
$27 = 14^2 - 13^2$
$28 = 8^2 - 6^2$
$29 = 15^2 - 14^2$

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 $n + (n + 1) = m$.

$$\begin{aligned} n + (n + 1) &= n + n + 1 \\ &= 2n + 1 \\ &= m \end{aligned}$$

b. What is the difference of squares of $n + 1$ and n?

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

c. What can you conclude from parts (a) and (b)?

We can write any positive odd number m as the difference of squares of two consecutive numbers that sum to m.

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	8	$3^2 - 1^2$	3	1
3	12	$4^2 - 2^2$	4	2
4	16	$5^2 - 3^2$	5	3
5	20	$6^2 - 4^2$	6	4
n	$4n$	$(\quad)^2 - (\quad)^2$	$n + 1$	$n - 1$

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

The values of a and b in the differences of two squares differ by 2 every time. They are one larger and one smaller than n; that is, $a = n + 1$ and $b = n - 1$.

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.)

Define $a = n + 1$ and $b = n - 1$. Then we can calculate $a^2 - b^2$ as follows.

$$\begin{aligned} a^2 - b^2 &= (n+1)^2 - (n-1)^2 \\ &= \big((n+1) + (n-1)\big)\big((n+1) - (n-1)\big) \\ &= (2n)(2) \\ &= 4n \end{aligned}$$

We can also see that

$$\begin{aligned} a - b &= (n+1) - (n-1) \\ &= n + 1 - n + 1 \\ &= 2. \end{aligned}$$

Thus every positive multiple of 4 can be written as a difference of squares of two integers that differ by 2.

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?

If one of a and b is even and the other one is odd, then one of a^2 and b^2 is even and the other one is odd. Since the difference of an odd and an even number is odd, this means that $m = a^2 - b^2$ would be odd. Since we know that m is even, it must be 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?

Since a and b are either both odd or both even, we know that both $a + b$ and $a - b$ are even.

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.

Because $a + b$ and $a - b$ are both even, 2 is a factor of both $a + b$ and $a - b$. Thus, $2^2 = 4$ is a factor of $(a + b)(a - b)$.

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

No. If 4 were a factor of $4n - 2$, we could factor it out: $4n - 2 = 4\left(n - \frac{1}{2}\right)$. But this means that $n - \frac{1}{2}$ is an integer, which it clearly is not. This means that 4 is not a factor of any number of the form $4n - 2$.

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

If m is a positive even integer and m can be written as the difference of two square integers, then m cannot be of the form $4n - 2$ for any integer n. Another way to say this is that the positive integers of the form $4n - 2$ for some integer n cannot be written as the difference of two square integers.

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.**

Since every odd number can be expressed as the difference of two squares, $a^2 - b^2 = (a + b)(a - b)$, the number 17 must fit this pattern. Because 17 is prime, there is only one way to factor 17, which is $17 = 1 \cdot 17$.

Let $a + b = 17$ and $a - b = 1$. The two numbers that satisfy this system of equations are 8 and 9. Thus,

$$\begin{aligned} 17 &= 1 \cdot 17 \\ &= (9 - 8)(9 + 8) \\ &= 9^2 - 8^2. \end{aligned}$$

A composite number has more than one factorization, not all of which will lead to writing the number as the difference of squares of two integers. For the number 24, you could use

MP.3

$$\begin{aligned} 24 &= 2 \cdot 12 \\ &= (7 - 5)(7 + 5) \\ &= 7^2 - 5^2. \end{aligned}$$

Or, you could use

$$\begin{aligned} 24 &= 4 \cdot 6 \\ &= (5 - 1)(5 + 1) \\ &= 5^2 - 1^2. \end{aligned}$$

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

If $24 = 3 \cdot 8$, then $a - b = 3$ and $a + b = 8$. The solution to this system of equations is $(5.5, 2.5)$. If we are restricting this problem to the set of whole numbers, then you cannot apply the identity to rewrite 24 as the difference of two perfect squares where a and b are whole numbers. It certainly is true that $24 = (5.5 - 2.5)(5.5 + 2.5) = 5.5^2 - 2.5^2$, but this is not necessarily an easy way to calculate 24.