

# Some Number Theory

Art & Science of Mathematics

John E. Mitchell

Wednesday, October 26, 2011

# Introduction

- Number theory concerns the study of **integers**.
- It is over 2000 years old and is still being actively researched today.
- It is famous for simply stated conjectures that have eluded proof for hundreds of years, but the theory is also vital to various applications.
- For example, **data encryption** is based on theories, conjectures, and algorithms that arise from number theory; it is used every time you send your **credit card number over the internet**.
- It is not possible to understand how the data encryption algorithms work without knowing some number theory.

# Introduction

- Number theory concerns the study of **integers**.
- It is over 2000 years old and is still being actively researched today.
- It is famous for simply stated conjectures that have eluded proof for hundreds of years, but the theory is also vital to various applications.
- For example, **data encryption** is based on theories, conjectures, and algorithms that arise from number theory; it is used every time you send your **credit card number over the internet**.
- It is not possible to understand how the data encryption algorithms work without knowing some number theory.

# Introduction

- Number theory concerns the study of **integers**.
- It is over 2000 years old and is still being actively researched today.
- It is famous for simply stated conjectures that have eluded proof for hundreds of years, but the theory is also vital to various applications.
- For example, **data encryption** is based on theories, conjectures, and algorithms that arise from number theory; it is used every time you send your **credit card number over the internet**.
- It is not possible to understand how the data encryption algorithms work without knowing some number theory.

# Introduction

- Number theory concerns the study of **integers**.
- It is over 2000 years old and is still being actively researched today.
- It is famous for simply stated conjectures that have eluded proof for hundreds of years, but the theory is also vital to various applications.
- For example, **data encryption** is based on theories, conjectures, and algorithms that arise from number theory; it is used every time you send your **credit card number over the internet**.
- It is not possible to understand how the data encryption algorithms work without knowing some number theory.

# Introduction

- Number theory concerns the study of **integers**.
- It is over 2000 years old and is still being actively researched today.
- It is famous for simply stated conjectures that have eluded proof for hundreds of years, but the theory is also vital to various applications.
- For example, **data encryption** is based on theories, conjectures, and algorithms that arise from number theory; it is used every time you send your **credit card number over the internet**.
- It is not possible to understand how the data encryption algorithms work without knowing some number theory.

# Greatest Common Divisors

- Typically in number theory, we use the phrase “ $b$  divides  $a$ ” to mean that  $b$  divides  $a$  without remainder. That is, there exists an integer  $m$  with  $b \times m = a$ .
- The **greatest common divisor** of two positive integers  $c$  and  $d$  is the largest positive integer that divides both  $c$  and  $d$ .
- For example,  $\gcd(8, 12) = 4$ ,  $\gcd(12, 25) = 1$ ,  $\gcd(a, a) = a$ .
- **Exercise:** Compute  $\gcd(45, 75)$ ,  $\gcd(1, a)$ ,  $\gcd(a, 2a)$ .

# Greatest Common Divisors

- Typically in number theory, we use the phrase “ $b$  divides  $a$ ” to mean that  $b$  divides  $a$  without remainder. That is, there exists an integer  $m$  with  $b \times m = a$ .
- The **greatest common divisor** of two positive integers  $c$  and  $d$  is the largest positive integer that divides both  $c$  and  $d$ .
- For example,  $\gcd(8, 12) = 4$ ,  $\gcd(12, 25) = 1$ ,  $\gcd(a, a) = a$ .
- **Exercise:** Compute  $\gcd(45, 75)$ ,  $\gcd(1, a)$ ,  $\gcd(a, 2a)$ .

# Greatest Common Divisors

- Typically in number theory, we use the phrase “ $b$  divides  $a$ ” to mean that  $b$  divides  $a$  without remainder. That is, there exists an integer  $m$  with  $b \times m = a$ .
- The **greatest common divisor** of two positive integers  $c$  and  $d$  is the largest positive integer that divides both  $c$  and  $d$ .
- For example,  $\gcd(8, 12) = 4$ ,  $\gcd(12, 25) = 1$ ,  $\gcd(a, a) = a$ .
- **Exercise:** Compute  $\gcd(45, 75)$ ,  $\gcd(1, a)$ ,  $\gcd(a, 2a)$ .

# Greatest Common Divisors

- Typically in number theory, we use the phrase “ $b$  divides  $a$ ” to mean that  $b$  divides  $a$  without remainder. That is, there exists an integer  $m$  with  $b \times m = a$ .
- The **greatest common divisor** of two positive integers  $c$  and  $d$  is the largest positive integer that divides both  $c$  and  $d$ .
- For example,  $\gcd(8, 12) = 4$ ,  $\gcd(12, 25) = 1$ ,  $\gcd(a, a) = a$ .
- **Exercise:** Compute  $\gcd(45, 75)$ ,  $\gcd(1, a)$ ,  $\gcd(a, 2a)$ .

# The Euclidean Algorithm

- One way to find **greatest common divisors** is to compute **all the factors** of each number, but that is very slow for large numbers.
- Find all the factors of 45 and 75:
- Much of the utility of number theory is derived from the fact that there is a **simple and fast algorithm** to find the greatest common divisor known as the **Euclidean Algorithm**.
- In general, for many large numbers, the Euclidean Algorithm is conjectured to be a million (or more) times faster than any algorithm that tries to find all the factors of each number individually.
- There are important data encryption algorithms that take advantage of this.

# The Euclidean Algorithm

- One way to find **greatest common divisors** is to compute **all the factors** of each number, but that is very slow for large numbers.
- Find all the factors of 45 and 75:

$$45 = 3 \times 3 \times 5, \quad 75 = 3 \times 5 \times 5$$

- Much of the utility of number theory is derived from the fact that there is a **simple and fast algorithm** to find the greatest common divisor known as the **Euclidean Algorithm**.
- In general, for many large numbers, the Euclidean Algorithm is conjectured to be a million (or more) times faster than any algorithm that tries to find all the factors of each number individually.
- There are important data encryption algorithms that take advantage of this.

# The Euclidean Algorithm

- One way to find **greatest common divisors** is to compute **all the factors** of each number, but that is very slow for large numbers.
- Find all the factors of 45 and 75:

$$45 = 3 \times 3 \times 5, \quad 75 = 3 \times 5 \times 5$$

- Much of the utility of number theory is derived from the fact that there is a **simple and fast algorithm** to find the greatest common divisor known as the **Euclidean Algorithm**.
- In general, for many large numbers, the Euclidean Algorithm is conjectured to be a million (or more) times faster than any algorithm that tries to find all the factors of each number individually.
- There are important data encryption algorithms that take advantage of this.

# The Euclidean Algorithm

- One way to find **greatest common divisors** is to compute **all the factors** of each number, but that is very slow for large numbers.
- Find all the factors of 45 and 75:

$$45 = 3 \times 3 \times 5, \quad 75 = 3 \times 5 \times 5$$

- Much of the utility of number theory is derived from the fact that there is a **simple and fast algorithm** to find the greatest common divisor known as the **Euclidean Algorithm**.
- In general, for many large numbers, the Euclidean Algorithm is conjectured to be a million (or more) times faster than any algorithm that tries to find all the factors of each number individually.
- There are important data encryption algorithms that take advantage of this.

# The Euclidean Algorithm

- One way to find **greatest common divisors** is to compute **all the factors** of each number, but that is very slow for large numbers.
- Find all the factors of 45 and 75:

$$45 = 3 \times 3 \times 5, \quad 75 = 3 \times 5 \times 5$$

- Much of the utility of number theory is derived from the fact that there is a **simple and fast algorithm** to find the greatest common divisor known as the **Euclidean Algorithm**.
- In general, for many large numbers, the Euclidean Algorithm is conjectured to be a million (or more) times faster than any algorithm that tries to find all the factors of each number individually.
- There are important data encryption algorithms that take advantage of this.

# The Euclidean Algorithm

- One way to find **greatest common divisors** is to compute **all the factors** of each number, but that is very slow for large numbers.
- Find all the factors of 45 and 75:

$$45 = 3 \times 3 \times 5, \quad 75 = 3 \times 5 \times 5$$

- Much of the utility of number theory is derived from the fact that there is a **simple and fast algorithm** to find the greatest common divisor known as the **Euclidean Algorithm**.
- In general, for many large numbers, the Euclidean Algorithm is conjectured to be a million (or more) times faster than any algorithm that tries to find all the factors of each number individually.
- There are important data encryption algorithms that take advantage of this.

# The Euclidean Algorithm:

- Let  $a$  and  $b$  be two positive integers with  $a \geq b$ .
- Divide  $b$  into  $a$  and find the remainder  $r_1$ .
- Divide  $r_1$  into  $b$  and find the remainder  $r_2$ .
- Divide  $r_2$  into  $r_1$  and find the remainder  $r_3$ .
- While the remainder is nonzero, divide the last remainder into the previous one to get a new remainder.
- The last nonzero remainder is  $\gcd(a, b)$ .

# The Euclidean Algorithm:

- Let  $a$  and  $b$  be two positive integers with  $a \geq b$ .
- Divide  $b$  into  $a$  and find the remainder  $r_1$ .
- Divide  $r_1$  into  $b$  and find the remainder  $r_2$ .
- Divide  $r_2$  into  $r_1$  and find the remainder  $r_3$ .
- While the remainder is nonzero, divide the last remainder into the previous one to get a new remainder.
- The last nonzero remainder is  $\gcd(a, b)$ .

# The Euclidean Algorithm:

- Let  $a$  and  $b$  be two positive integers with  $a \geq b$ .
- Divide  $b$  into  $a$  and find the remainder  $r_1$ .
- Divide  $r_1$  into  $b$  and find the remainder  $r_2$ .
- Divide  $r_2$  into  $r_1$  and find the remainder  $r_3$ .
- While the remainder is nonzero, divide the last remainder into the previous one to get a new remainder.
- The last nonzero remainder is  $\gcd(a, b)$ .

# The Euclidean Algorithm:

- Let  $a$  and  $b$  be two positive integers with  $a \geq b$ .
- Divide  $b$  into  $a$  and find the remainder  $r_1$ .
- Divide  $r_1$  into  $b$  and find the remainder  $r_2$ .
- Divide  $r_2$  into  $r_1$  and find the remainder  $r_3$ .
- While the remainder is nonzero, divide the last remainder into the previous one to get a new remainder.
- The last nonzero remainder is  $\gcd(a, b)$ .

# The Euclidean Algorithm:

- Let  $a$  and  $b$  be two positive integers with  $a \geq b$ .
- Divide  $b$  into  $a$  and find the remainder  $r_1$ .
- Divide  $r_1$  into  $b$  and find the remainder  $r_2$ .
- Divide  $r_2$  into  $r_1$  and find the remainder  $r_3$ .
- While the remainder is nonzero, divide the last remainder into the previous one to get a new remainder.
- The last nonzero remainder is  $\gcd(a, b)$ .

# The Euclidean Algorithm:

- Let  $a$  and  $b$  be two positive integers with  $a \geq b$ .
- Divide  $b$  into  $a$  and find the remainder  $r_1$ .
- Divide  $r_1$  into  $b$  and find the remainder  $r_2$ .
- Divide  $r_2$  into  $r_1$  and find the remainder  $r_3$ .
- While the remainder is nonzero, divide the last remainder into the previous one to get a new remainder.
- The last nonzero remainder is  $\gcd(a, b)$ .

## Example:

Find the greatest common divisor of  $a = 252$  and  $b = 198$ :

- Divide 198 into 252, get remainder  $r_1 = 252 - 198 = 54$ .
- Divide 54 into 198, get remainder  $r_2 = 198 - 3 \times 54 = 36$ .
- Divide 36 into 54, get remainder  $r_3 = 54 - 36 = 18$ .
- Divide 18 into 36, get remainder  $r_4 = 36 - 2 \times 18 = 0$ .
- Since we have a remainder of zero, the last nonzero remainder is the greatest common divisor, that is,  $\gcd(252, 198) = 18$ .
- Check:  $252 = 14 \times 18$  and  $198 = 11 \times 18$ .

**Exercise:** Use the Euclidean Algorithm to find  $\gcd(57, 133)$  and  $\gcd(981, 1234)$ .

## Example:

Find the greatest common divisor of  $a = 252$  and  $b = 198$ :

- Divide 198 into 252, get remainder  $r_1 = 252 - 198 = 54$ .
- Divide 54 into 198, get remainder  $r_2 = 198 - 3 \times 54 = 36$ .
- Divide 36 into 54, get remainder  $r_3 = 54 - 36 = 18$ .
- Divide 18 into 36, get remainder  $r_4 = 36 - 2 \times 18 = 0$ .
- Since we have a remainder of zero, the last nonzero remainder is the greatest common divisor, that is,  $\gcd(252, 198) = 18$ .
- Check:  $252 = 14 \times 18$  and  $198 = 11 \times 18$ .

**Exercise:** Use the Euclidean Algorithm to find  $\gcd(57, 133)$  and  $\gcd(981, 1234)$ .

## Example:

Find the greatest common divisor of  $a = 252$  and  $b = 198$ :

- Divide 198 into 252, get remainder  $r_1 = 252 - 198 = 54$ .
- Divide 54 into 198, get remainder  $r_2 = 198 - 3 \times 54 = 36$ .
- Divide 36 into 54, get remainder  $r_3 = 54 - 36 = 18$ .
- Divide 18 into 36, get remainder  $r_4 = 36 - 2 \times 18 = 0$ .
- Since we have a remainder of zero, the last nonzero remainder is the greatest common divisor, that is,  $\gcd(252, 198) = 18$ .
- Check:  $252 = 14 \times 18$  and  $198 = 11 \times 18$ .

**Exercise:** Use the Euclidean Algorithm to find  $\gcd(57, 133)$  and  $\gcd(981, 1234)$ .

## Example:

Find the greatest common divisor of  $a = 252$  and  $b = 198$ :

- Divide 198 into 252, get remainder  $r_1 = 252 - 198 = 54$ .
- Divide 54 into 198, get remainder  $r_2 = 198 - 3 \times 54 = 36$ .
- Divide 36 into 54, get remainder  $r_3 = 54 - 36 = 18$ .
- Divide 18 into 36, get remainder  $r_4 = 36 - 2 \times 18 = 0$ .
- Since we have a remainder of zero, the last nonzero remainder is the greatest common divisor, that is,  $\gcd(252, 198) = 18$ .
- Check:  $252 = 14 \times 18$  and  $198 = 11 \times 18$ .

**Exercise:** Use the Euclidean Algorithm to find  $\gcd(57, 133)$  and  $\gcd(981, 1234)$ .

## Example:

Find the greatest common divisor of  $a = 252$  and  $b = 198$ :

- Divide 198 into 252, get remainder  $r_1 = 252 - 198 = 54$ .
- Divide 54 into 198, get remainder  $r_2 = 198 - 3 \times 54 = 36$ .
- Divide 36 into 54, get remainder  $r_3 = 54 - 36 = 18$ .
- Divide 18 into 36, get remainder  $r_4 = 36 - 2 \times 18 = 0$ .
- Since we have a remainder of zero, the last nonzero remainder is the greatest common divisor, that is,  $\gcd(252, 198) = 18$ .
- Check:  $252 = 14 \times 18$  and  $198 = 11 \times 18$ .

**Exercise:** Use the Euclidean Algorithm to find  $\gcd(57, 133)$  and  $\gcd(981, 1234)$ .

## Example:

Find the greatest common divisor of  $a = 252$  and  $b = 198$ :

- Divide 198 into 252, get remainder  $r_1 = 252 - 198 = 54$ .
- Divide 54 into 198, get remainder  $r_2 = 198 - 3 \times 54 = 36$ .
- Divide 36 into 54, get remainder  $r_3 = 54 - 36 = 18$ .
- Divide 18 into 36, get remainder  $r_4 = 36 - 2 \times 18 = 0$ .
- Since we have a remainder of zero, the last nonzero remainder is the greatest common divisor, that is,  $\gcd(252, 198) = 18$ .
- **Check:**  $252 = 14 \times 18$  and  $198 = 11 \times 18$ .

**Exercise:** Use the Euclidean Algorithm to find  $\gcd(57, 133)$  and  $\gcd(981, 1234)$ .

# The Game of Euclid:

This is a game played by two people. Beginning with **two positive integers**, the players alternate turns making moves of the following type:

*A player can move from the **pair of positive integers**  $\{x, y\}$  with  $x \geq y$  to any of the pairs  $\{x - ty, y\}$  where  $t \geq 1$  is an integer and  $x - ty \geq 0$ . Thus, you can **subtract any multiple of the smaller number from the larger number**, provided you still have two nonnegative numbers.*

The winner is the one that first makes one element zero.

# Exercises

**Exercise:** Play the game of Euclid with a partner and for different starting pairs of integers  $\{a, b\}$ . Verify that you **always end up with the pair  $\{0, \gcd(a, b)\}$**  at the end of the game. Can you prove that this is always the case?

**Strategies:** Can player 1 always win the game of Euclid? Can player 2 always win? What is the best strategy?