Prime and Composite Numbers

MATH 100 *Survey of Mathematical Ideas*

J. Robert Buchanan

Department of Mathematics

Summer 2018

Number Theory

Number theory is a branch of mathematics devoted to the study of properties of the natural numbers.

Number Theory

Number theory is a branch of mathematics devoted to the study of properties of the natural numbers.

Definition

The natural number a is **divisible** by the natural number b if there exists a natural number k such that $a = b\,k$. If b divides a we write $b \mid a$.

Number Theory

Number theory is a branch of mathematics devoted to the study of properties of the natural numbers.

Definition

The natural number a is **divisible** by the natural number b if there exists a natural number k such that $a = b\,k$. If b divides a we write $b \mid a$.

Definition

A natural number greater than 1 that has only itself and 1 as divisors is called a **prime number**. A natural number greater than 1 that is not prime is called **composite**.

Sieve of Eratosthenes (1 of 2)

One method for determining if a natural number is prime.

1. List the natural numbers 2, 3, 4, . . . , N.
2. 2 is prime, strike out every higher multiple of 2.
3. 3 is prime, strike out every higher multiple of 3.
4. 5 is prime, strike out every higher multiple of 5.
5. Keep going until you reach the largest natural number less than $\sqrt{N}$.
6. All you have left is a list of prime numbers.

Sieve of Eratosthenes (2 of 2)

1. We would like to find all the prime numbers less than 50.
2. Start with a list of natural numbers 2, 3, . . . , 50.
3. Use the sieve procedure up to $\sqrt{50} \approx 7$.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Sieve of Eratosthenes (2 of 2)

1. We would like to find all the prime numbers less than 50.
2. Start with a list of natural numbers 2, 3, . . . , 50.
3. Use the sieve procedure up to $\sqrt{50} \approx 7$.

	2	3	5	7	9
11		13	15	17	19
21		23	25	27	29
31		33	35	37	39
41		43	45	47	49

Sieve of Eratosthenes (2 of 2)

1. We would like to find all the prime numbers less than 50.
2. Start with a list of natural numbers 2, 3, . . . , 50.
3. Use the sieve procedure up to $\sqrt{50} \approx 7$.

	2	3		5		7		
11		13				17		19
		23		25				29
31				35		37		
41		43				47		49

Sieve of Eratosthenes (2 of 2)

1. We would like to find all the prime numbers less than 50.
2. Start with a list of natural numbers 2, 3, . . . , 50.
3. Use the sieve procedure up to $\sqrt{50} \approx 7$.

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47		49	

Sieve of Eratosthenes (2 of 2)

1. We would like to find all the prime numbers less than 50.
2. Start with a list of natural numbers 2, 3, . . . , 50.
3. Use the sieve procedure up to $\sqrt{50} \approx 7$.

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47			

Sieve of Eratosthenes (2 of 2)

1. We would like to find all the prime numbers less than 50.
2. Start with a list of natural numbers 2, 3, . . . , 50.
3. Use the sieve procedure up to $\sqrt{50} \approx 7$.

	2	3		5					
11		13				17		19	
		23						29	
31						37			
41		43				47			
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

1. How many prime numbers are less than 100? Use your i>clicker to submit the count of primes less than 100.

Divisibility Tests

Divisible by	Test
2	Last digit is 0, 2, 4, 6, or 8.
3	Sum of the digits is divisible by 3.
4	Last two digits form a number divisible by 4.
5	Last digit is 0 or 5.
6	Number is divisible by 2 and 3.
8	Last three digits form a number divisible by 8.
9	Sum of the digits is divisible by 9.
10	Last digit is 0.
12	Number is divisible by 4 and 3.

Example

Consider the number 45815. Determine if it is divisible by

n	$(n \mid 45815)$?
2	
3	
4	
5	
6	
8	
9	
10	
12	

Example

Consider the number 45815. Determine if it is divisible by

n	$(n \mid 45815)$?
2	No
3	
4	No
5	
6	No
8	No
9	
10	No
12	No

Example

Consider the number 45815. Determine if it is divisible by

n	$(n \mid 45815)$?
2	No
3	No
4	No
5	
6	No
8	No
9	No
10	No
12	No

Example

Consider the number 45815. Determine if it is divisible by

n	$(n \mid 45815)$?
2	No
3	No
4	No
5	Yes
6	No
8	No
9	No
10	No
12	No

Leap Years

A leap year is a year which is divisible by 4 but not by 100 except if it is divisible by 400.

Leap Years	**Not Leap Years**
2012	2014
2000	1800
2104	2106
1532	1500
2224	2222

Leap Years

A leap year is a year which is divisible by 4 but not by 100 except if it is divisible by 400.

Which if the following years is/was/will be a leap year? Use your i>clicker to select “A” for leap year and “B” for not a leap year.

2. 1780

Leap Years

A leap year is a year which is divisible by 4 but not by 100 except if it is divisible by 400.

Which if the following years is/was/will be a leap year? Use your i>clicker to select “A” for leap year and “B” for not a leap year.

2. 1780
3. 1900

Leap Years

A leap year is a year which is divisible by 4 but not by 100 except if it is divisible by 400.

Which if the following years is/was/will be a leap year? Use your i>clicker to select “A” for leap year and “B” for not a leap year.

2. 1780
3. 1900
4. 2002

Leap Years

A leap year is a year which is divisible by 4 but not by 100 except if it is divisible by 400.

Which if the following years is/was/will be a leap year? Use your i>clicker to select “A” for leap year and “B” for not a leap year.

2. 1780
3. 1900
4. 2002
5. 2100

Leap Years

A leap year is a year which is divisible by 4 but not by 100 except if it is divisible by 400.

Which if the following years is/was/will be a leap year? Use your i>clicker to select “A” for leap year and “B” for not a leap year.

2. 1780
3. 1900
4. 2002
5. 2100
6. 2400

Fundamental Theorem of Arithmetic

Every natural number can be expressed in one and only one way as a product of primes (if the order of the factors is disregarded). This unique product of primes is called the **prime factorization** of the natural number.

Fundamental Theorem of Arithmetic

Every natural number can be expressed in one and only one way as a product of primes (if the order of the factors is disregarded). This unique product of primes is called the **prime factorization** of the natural number.

Example

Find the prime factorization of 885.

Fundamental Theorem of Arithmetic

Every natural number can be expressed in one and only one way as a product of primes (if the order of the factors is disregarded). This unique product of primes is called the **prime factorization** of the natural number.

Example

Find the prime factorization of 885.

$$885 = 3 \cdot 5 \cdot 59$$

How Many Numbers Divide N?

To determine the number of divisors of N:

1. Write N as a product of prime factors using exponents.
2. Add 1 to each exponent.
3. Multiply these augmented exponents.

How Many Numbers Divide N?

To determine the number of divisors of N:

1. Write N as a product of prime factors using exponents.
2. Add 1 to each exponent.
3. Multiply these augmented exponents.

Example

How many numbers divide 308?

How Many Numbers Divide N?

To determine the number of divisors of N:

1. Write N as a product of prime factors using exponents.
2. Add 1 to each exponent.
3. Multiply these augmented exponents.

Example

How many numbers divide 308?

$$\begin{aligned} 308 &= 2^2 \cdot 7 \cdot 11 = 2^2 \cdot 7^1 \cdot 11^1 \\ \text{Number of divisors} &= (2+1)(1+1)(1+1) = (3)(2)(2) = 12 \end{aligned}$$

How Many Numbers Divide 456?

$$456 = 2^3 \cdot 3^1 \cdot 19^1$$

How Many Numbers Divide 456?

$$\begin{aligned} 456 &= 2^3 \cdot 3^1 \cdot 19^1 \\ \text{Number of divisors} &= (3+1)(1+1)(1+1) = (4)(2)(2) = 16 \end{aligned}$$

Examples

Find the number of divisors of the following and submit that number using your i>clicker:

7. 2520

Examples

Find the number of divisors of the following and submit that number using your i>clicker:

7. 2520
8. 4050

Infinitude of the Primes

Theorem

There are infinitely many prime numbers.

Infinitude of the Primes

Theorem

There are infinitely many prime numbers.

Proof.

- Suppose there were only finitely many primes, $p_1, p_2, \ldots, p_n$.
- Form the number $N = (p_1 \cdot p_2 \cdots p_n) + 1$
- $N > p_i$ for $i = 1, 2, \ldots, n$ but p_i does not divide N.
- N is either prime or there is another prime (not in the original list) which divides N.

□

Searching for Prime Numbers

Large prime numbers are useful in **cryptography.**

Definition

For $n = 1, 2, 3, \ldots$, the **Mersenne numbers** are those generated by the formula

$$M_n = 2^n - 1.$$

1. If n is composite, then M_n is also composite.
2. If n is prime, then M_n may be prime or composite.

The prime values of M_n are called the **Mersenne primes**.

Some Mersenne Numbers

n	M_n	Prime?
2	3	Prime
3	7	Prime
5	31	Prime
13	8,191	Prime
29	536,870,911	Composite
67	147,573,952,589,676,412,927	Composite

In 2018 the largest known Mersenne prime number is

$$2^{77,232,917} - 1 \approx 4.67333183359 \times 10^{23,249,424}$$

which has $23,249,425$ digits. It was discovered December 26, 2017 by Jon Pace (only the 50th Mersenne prime ever found).

Fermat Numbers

Pierre de Fermat (1601–1665) conjectured that the formula

$$F_n = 2^{2^n} + 1$$

would always produce a prime number. He checked $n = 0, 1, 2, 3, 4$.

Fermat Numbers

Pierre de Fermat (1601–1665) conjectured that the formula

$$F_n = 2^{2^n} + 1$$

would always produce a prime number. He checked $n = 0, 1, 2, 3, 4$.

n	F_n	**Prime?**
0	3	
1	5	
2	17	
3	257	
4	65537	
5	4294967297	

Fermat Numbers

Pierre de Fermat (1601–1665) conjectured that the formula

$$F_n = 2^{2^n} + 1$$

would always produce a prime number. He checked $n = 0, 1, 2, 3, 4$.

n	F_n	**Prime?**
0	3	Yes
1	5	Yes
2	17	Yes
3	257	Yes
4	65537	Yes
5	4294967297	

Fermat Numbers

Pierre de Fermat (1601–1665) conjectured that the formula

$$F_n = 2^{2^n} + 1$$

would always produce a prime number. He checked $n = 0, 1, 2, 3, 4$.

n	F_n	**Prime?**
0	3	Yes
1	5	Yes
2	17	Yes
3	257	Yes
4	65537	Yes
5	4294967297	(641)(6700417)

Euler's Formula

Leonhard Euler noted in 1732 that the formula

$$p(n) = n^2 - n + 41$$

always produces a prime number for $1 \leq n < 41$, but is composite when $n = 41$.

n	$p(n)$	n	$p(n)$	n	$p(n)$	n	$p(n)$
1	41	2	43	3	47	4	53
5	61	6	71	7	83	8	97
9	113	10	131	11	151	12	173
13	197	14	223	15	251	16	281
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
37	1373	38	1447	39	1523	40	1601

Escott's Formula

E.B. Escott offered in 1879 the formula

$$q(n) = n^2 - 79n + 1601$$

which always produces a prime number for $1 \leq n < 80$, but is composite when $n = 80$.

n	$q(n)$	n	$q(n)$	n	$q(n)$	n	$q(n)$
1	1523	2	1447	3	1373	4	1301
5	1231	6	1163	7	1097	8	1033
9	971	10	911	11	853	12	797
13	743	14	691	15	641	16	593
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
76	1373	77	1447	78	1523	79	1601