

Math 102: Number Theory

Dr. Richard Mikula

Fall 2009

Number Theory is the study of numbers and their properties, in particular the study of the *Natural Numbers*.

Given any natural number n , we may ask the question:

Can we write $n = p \cdot q$, for some natural numbers p, q ?

e.g. Given the number 6, we can do this in several ways:

$$2 \cdot 3, 1 \cdot 6.$$

However, for the number 3, we can only do this in the following way:

$$1 \cdot 3.$$

Given $n \in \mathbb{N}$, Clearly we can always write $n = p \cdot q$ if we are allowing either p or q to be 1 or n .

The numbers p, q are called **factors** of n . And we say that p and q **divide** n or are **divisors of** n . The notation for this is

$$p|n$$

which means p *divides* n . The process of finding such a p, q for a given n is called factoring.

Also, if

$$p|n,$$

we say that n is a **multiple** of p .

In the above example 1, 2, 3, 6 are divisors of 6.
However only 1, 3 are divisors of 3.

For any positive integer n , the numbers 1, n
are always divisors of n .

If $n \in \mathbb{N}$, $n > 1$ * has only $\{1, n\}$ as its set of
divisors, we say that n is a **prime number**.†

*1 is not considered a prime number!!

†Another characterization of prime numbers is: p is
prime if and only if $p|a \cdot b$ implies $p|a$ or $p|b$.

Thus, a prime number is an integer who is greater than one, and can only be written as a product of two natural numbers, in the form

$$n = 1 \cdot n \quad \text{or} \quad n = n \cdot 1.$$

If a natural number is not a prime, then it is called a **composite number**.

In our example, 3 is prime, but 6 is a composite number.

Given a natural number n , the natural numbers which are **multiples** of n are the following numbers

$$n, 2n, 3n, 4n, 5n, 6n, 7n, \dots$$

If a number p divides two numbers n, m then the number p divides the sum and difference

$$n + m, \quad n - m.$$

To see this we note

$$n = a \cdot p, \quad m = b \cdot p,$$

and thus

$$n \pm m = a \cdot p \pm b \cdot p = (a \pm b) \cdot p.$$

Divisibility Tests:

The natural numbers that are divisible by 2 are the so-called **even** natural numbers. By the Euclidean algorithm we may write a natural number n as

$$n = 10 \cdot q + d.$$

Thus, a number n is even if and only if d , the number's ones digit, is even*. That is

$$d \in \{0, 2, 4, 6, 8\}.$$

*since 2 clearly divides the $10 \cdot q$ term

Using the decimal representation again for n as $n = 10 \cdot q + d$, we see that n is divisible by 5 if and only if $d = 0$ or 5.

Thus

55,110,3465

are divisible by 5, but

11,2009,2346

are not.

Next, we will discuss the issue of divisibility by 11. Suppose that the decimal representation of a natural number n is

$$d_m d_{m-1} \cdots d_2 d_1 d_0,$$

that is

$$n = d_m \cdot 10^m + d_{m-1} \cdot 10^{m-1} + \cdots + d_2 \cdot 10^2 + d_1 \cdot 10 + d_0.$$

Writing each 10 as $(11 - 1)$ and expanding this representation, we see that for some whole number q we have

$$n = q \cdot 11 + (-1)^m d_m + (-1)^{m-1} d_{m-1} + \cdots + d_2 - d_1 + d_0.$$

Hence n is divisible by 11 if and only if

$$11 \mid [d_0 - d_1 + d_2 + \cdots + (-1)^m d_m].$$

Example:

11, 22, 33, 121, 132

are all divisible by 11 since 11 divides

$$1 - 1 = 0, \quad 2 - 2 = 0, \quad 3 - 3 = 0,$$

$$1 - 2 + 1 = 0, \quad 2 - 3 + 1 = 0.*$$

However, 134 is not divisible by 11, since

$$4 - 3 + 1 = 2$$

is not divisible by 11.

*Every natural number n divides 0 since $0 = 0 \cdot n$.

Example The number

1010101010101010101010101

is divisible by 11 by our divisibility test, since

$$1 - 0 + 1 - 0 + 1 - 0 + 1 - 0 + 1 - 0 + 1 - 0 + 1 - 0 + 1 - 0 + 1 - 0 + 1 - 0 + 1 - 0 + 1 - 0 + 1 - 0 + 1 = 11.$$

Moreover,

$$1010101010101010101010101 = 11 \cdot 9182736455463728191.$$

Using the decimal representation for a natural number n

$$d_m d_{m-1} \cdots d_2 d_1 d_0,$$

that is

$$n = d_m \cdot 10^m + d_{m-1} \cdot 10^{m-1} + \cdots + d_2 \cdot 10^2 + d_1 \cdot 10 + d_0,$$

and writing each 10 as $(9 + 1)$ and expanding this representation, we see that for some whole number q we have

$$n = q \cdot 9 + d_m + d_{m-1} + \cdots + d_2 + d_1 + d_0.$$

Hence n is divisible by 9 if and only if

$$9 \mid [d_0 + d_1 + d_2 + \cdots + d_m].$$

Likewise, 3 divides a natural number n with decimal representation $d_m \cdots d_2 d_1 d_0$ if and only $3 \mid [d_0 + d_1 + d_2 + \cdots + d_m]$.

Example: Thus, we see that 9 divides

81, 45, 135, 81117, 111111111

because 9 divides

$$8 + 1 = 9, \quad 4 + 5 = 9, \quad 1 + 3 + 4 = 9,$$

$$8 + 1 + 1 + 1 + 7 = 18$$

and

$$1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 = 9.$$

However, 9 does not divide

22, 82, 4567,

since

$$2 + 2 = 4, \quad 8 + 2 = 10, \quad 4 + 5 + 6 + 7 = 22$$

are not divisible by 9.

Also, 3 divides

21, 42, 54, 123,

since

$$2+1 = 3, \quad 4+2 = 6, \quad 5+4 = 9, \quad 1+2+3 = 6.$$

However 3 does not divide

22, 43, 67, 1112,

since

$$2 + 2 = 4, \quad 4 + 3 = 7, \quad 6 + 7 = 13,$$

$$1 + 1 + 1 + 2 = 5$$

are not divisible by 3

Given a natural number n with a decimal representation

$$d_m d_{m-1} \cdots d_2 d_1 d_0,$$

that is

$$n = d_m \cdot 10^m + d_{m-1} \cdot 10^{m-1} + \cdots + d_2 \cdot 10^2 + d_1 \cdot 10 + d_0,$$

we see that by the Euclidean algorithm we may write

$$n = q \cdot 100 + r,$$

where r has decimal representation $d_1 d_0$. Thus $4|n$ if and only if 4 divides the number who is given by the last two digits* in the decimal representation of n .

*that is, in the ones and tens places

Example: 4 divides

12, 112, 1312

because $4|12$. Likewise $4|28$ implies 4 divides

128, 55628, 11111128.

However 4 does not divide

123421

since 4 does not divide 21.

Some Homework Exercises:

1. Determine whether or not 2 divides the following numbers:

2, 3, 4, 8, 127, 2461, 2228.

Answer: 2 divides 2, 4, 8, 228.

2. Determine whether or not 3 divides the following numbers:

2, 3, 402, 127, 24615, 22283.

Answer: 3 divides 3, 402, 127, 24615.

3. Determine whether or not 4 divides the following numbers:

2, 4, 8, 127, 128, 2476, 2226, 2228.

Answer: 4 divides 4, 8, 128, 2476, 2228.

4. Determine whether or not 5 divides the following numbers:

2, 10, 65, 70, 83, 127, 2460, 2225.

Answer: 5 divides 10, 65, 70, 2460, 2225.

5. Determine whether or not 9 divides the following numbers:

8, 126, 2461, 3258.

Answer: 9 divides 126, 3258.

6. Determine whether or not 11 divides the following numbers:

121, 127, 2461, 27715, 30404, 30405.

Answer: 11 divides 121, 27715, 30404.

The Sieve of Eratosthenes:

We will make a list of the naturals

1, 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, 51, 52, 53,...

The process we shall describe is called the **Sieve of Eratosthenes**.

First we cross out every other number – here I will put bars over them – skipping over 2. These are the even numbers, or the multiples of 2, and 2 is prime.

1, 2, 3, $\bar{4}$, 5, $\bar{6}$, 7, $\bar{8}$,
9, $\bar{10}$, 11, $\bar{12}$, 13, $\bar{14}$, 15,
 $\bar{16}$, 17, $\bar{18}$, 19, $\bar{20}$, 21, $\bar{22}$, 23,
 $\bar{24}$, 25, $\bar{26}$, 27, $\bar{28}$, 29, $\bar{30}$, 31,
 $\bar{32}$, 33, $\bar{34}$, 35, $\bar{36}$, 37, $\bar{38}$, 39,
 $\bar{40}$, 41, $\bar{42}$, 43, $\bar{44}$, 45, $\bar{46}$, 47,
 $\bar{48}$, 49, $\bar{50}$, 51, $\bar{52}$, 53, ...

Next we cross out every third number – here I will put bars over them as well – skipping over 3, and they are all multiples of 3, which is prime. *

1, 2, 3, $\bar{4}$, 5, $\bar{6}$, 7, $\bar{8}$,
 $\bar{9}$, $\bar{10}$, 11, $\bar{12}$, 13, $\bar{14}$, $\bar{15}$,
 $\bar{16}$, 17, $\bar{18}$, 19, $\bar{20}$, $\bar{21}$, $\bar{22}$, 23,
 $\bar{24}$, 25, $\bar{26}$, $\bar{27}$, $\bar{28}$, 29, $\bar{30}$, 31,
 $\bar{32}$, $\bar{33}$, $\bar{34}$, 35, $\bar{36}$, 37, $\bar{38}$, $\bar{39}$,
 $\bar{40}$, 41, $\bar{42}$, 43, $\bar{44}$, $\bar{45}$, $\bar{46}$, 47,
 $\bar{48}$, 49, $\bar{50}$, $\bar{51}$, $\bar{52}$, 53, ...

*Note that in each step the first number n that is not crossed out is prime, and in this step we are crossing out the multiples of this

$$2n, 3n, 4n, \dots$$

Next we cross out every fifth number – here I will put bars over them as well – skipping over 5, and they are all multiples of 5, which is prime. *

1, 2, 3, $\bar{4}$, 5, $\bar{6}$, 7, $\bar{8}$,
 $\bar{9}$, $\bar{10}$, 11, $\bar{12}$, 13, $\bar{14}$, $\bar{15}$,
 $\bar{16}$, 17, $\bar{18}$, 19, $\bar{20}$, $\bar{21}$, $\bar{22}$, 23,
 $\bar{24}$, $\bar{25}$, $\bar{26}$, $\bar{27}$, $\bar{28}$, 29, $\bar{30}$, 31,
 $\bar{32}$, $\bar{33}$, $\bar{34}$, $\bar{35}$, $\bar{36}$, 37, $\bar{38}$, $\bar{39}$,
 $\bar{40}$, 41, $\bar{42}$, 43, $\bar{44}$, $\bar{45}$, $\bar{46}$, 47,
 $\bar{48}$, 49, $\bar{50}$, $\bar{51}$, $\bar{52}$, 53, ...

*Note that we choose 5 because it is the first number after 3 that doesn't have a bar over it!

Next we cross out every seventh number – here I will put bars over them as well – skipping over 7, and they are all multiples 7, which is prime.

1, 2, 3, $\bar{4}$, 5, $\bar{6}$, 7, $\bar{8}$,
 $\bar{9}$, $\bar{10}$, 11, $\bar{12}$, 13, $\bar{14}$, $\bar{15}$,
 $\bar{16}$, 17, $\bar{18}$, 19, $\bar{20}$, $\bar{21}$, $\bar{22}$, 23,
 $\bar{24}$, $\bar{25}$, $\bar{26}$, $\bar{27}$, $\bar{28}$, 29, $\bar{30}$, 31,
 $\bar{32}$, $\bar{33}$, $\bar{34}$, $\bar{35}$, $\bar{36}$, 37, $\bar{38}$, $\bar{39}$,
 $\bar{40}$, 41, $\bar{42}$, 43, $\bar{44}$, $\bar{45}$, $\bar{46}$, 47,
 $\bar{48}$, $\bar{49}$, $\bar{50}$, $\bar{51}$, $\bar{52}$, $\bar{53}, \dots$

It turns out that if a number n is composite, then it must have a prime factor p with $p \leq \sqrt{n}$, i.e. $p^2 \leq n$.

That is, suppose n is a natural number, and k is the smallest natural number so that

$$n < k \times k.$$

If there is no prime number less than k that is a factor of n , then n is a prime number.

Hence, since

$$7 \cdot 7 < 53 < 8 \cdot 8,$$

and 8 is not prime and 7 is prime, we have found all the primes between 1 and 53. Thus we see that for the numbers

$$1, 2, \dots, 53$$

the primes are

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37$$

$$41, 43, 47, 53.$$

There Are Infinitely Many Primes:

An important fact is that there are infinitely many primes. Let us now see why:

Suppose there were finitely many primes, let us suppose that we listed them in increasing order

$$2, 3, 5, 7, 11, 13, 17, 19, \dots, p_n$$

or simply

$$p_1, p_2, \dots, p_n$$

We claim that we can create a number larger than p_n to which none of the primes in our list p_1, \dots, p_n will divide. If this is possible, then this number must also be prime, contradicting the completeness of our list.

Let us define

$$P = p_1 \cdot p_2 \cdots p_n + 1.$$

Clearly, $P > p_n$.

Since P is greater than every prime, it must be composite. Thus suppose $p_i | P$ for some prime p_i in our list.

Then $P = k \cdot p_i$ for some number $1 < k < P$.

However, this yields

$$1 = k \cdot p_i - p_1 \cdots p_i \cdots p_n$$

and thus

$$1 = p_i(k - p_1 \cdots p_{i-1} \cdot p_{i+1} \cdots p_n)$$

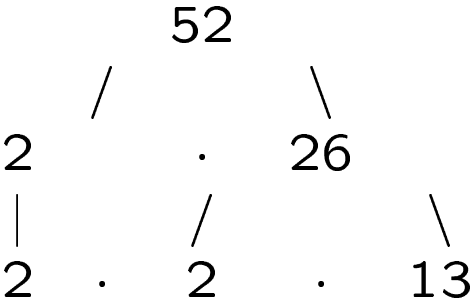
This implies that $p_i | 1$. This cannot happen!

Thus none of the primes p_1, \dots, p_n divide P , and hence P is prime. However, we assumed p_n is the largest prime. Now we have produced $P > p_n$ which is prime. This is a contradiction. Thus, there are infinitely many primes.

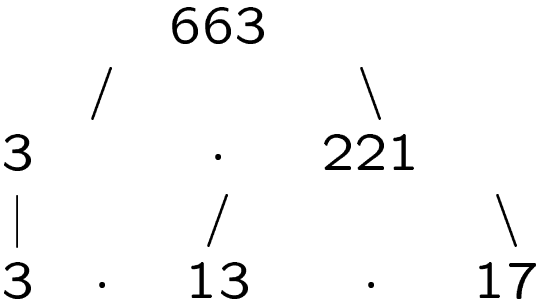
Factoring Composite Numbers:

Every composite number can be factored into a product of prime numbers, and this factorization is unique. This result is called **the Fundamental Theorem of Arithmetic**.

Example:



Example:



Some Homework Exercises:

1. Perform the Sieve of Eratosthenes to find the primes less than 100.
2. Using that $23^2 = 529$ are the following numbers prime?

420, 421, 365, 367, 89, 47, 23

If they are composite, find the prime factorizations. **Answer:** 23, 47, 89, 367, 421 are prime. $365 = 5 \cdot 73$, $420 = 2^2 \cdot 3 \cdot 5 \cdot 7$.

3. Explain why the following statement is true: if p is prime, then $p + 3$ cannot be prime.
4. Factor the following numbers into products of primes:

187, 1496, 226

Answer: $226 = 2 \cdot 113$, $187 = 11 \cdot 17$,
 $1496 = 2^3 \cdot 11 \cdot 17$.

Least Common Multiple and Greatest Common Divisor:

Given 2 integers m, n , the **least common multiple** (lcm) of m, n is the smallest natural number which is divisible by both m and n

The **greatest common divisor** (gcd) of m, n is the largest natural number that is a both a divisor of m and of n .

You may find the greatest common divisor and the least common multiple of two numbers by examining their prime factorizations.

Here we will use the notation

$$a^n = \underbrace{a \cdot a \cdots a}_{n \text{ times}}.$$

Example:

Recall that

$$52 = 2 \cdot 2 \cdot 13 = 2^2 \cdot 13, \quad 663 = 3 \cdot 13 \cdot 17.$$

The gcd of 52 and 663 is 13 and the lcm is $2^2 \cdot 3 \cdot 13 \cdot 17 = 2652$.

Example:

$$20 = 2 \cdot 10 = 2 \cdot 2 \cdot 5, \quad 36 = 2 \cdot 18 = 2 \cdot 2 \cdot 9 = 2 \cdot 2 \cdot 3 \cdot 3$$

Therefore, we have that the gcd of 20 and 36 is

$$= 2^2 = 4,$$

and the lcm of 20 and 36 is

$$2^2 \cdot 3^2 \cdot 5 = 180.$$

Example:

$$240 = 2^4 \cdot 3 \cdot 5, \quad 285 = 3 \cdot 5 \cdot 19$$

Thus the gcd of 240 and 285 is

$$3 \cdot 5 = 15,$$

and the lcm of 240 and 285 is

$$2^4 \cdot 3 \cdot 5 \cdot 19 = 4560.$$

Another useful property to keep in mind that links the gcd and lcm of two numbers a, b is:

$$a \cdot b = \text{gcd} \cdot \text{lcm}.$$

Some Homework Exercises:

Find the greatest common factor and the least common multiple of the following pairs on natural numbers:

1. 10 and 18 **Answer:** 2; 90.

2. 120 and 220 **Answer:** 20; 1320.

3. 731 and 952 **Answer:** 17; 40,936.