Discrete Mathematics & Mathematical Reasoning
Primes and Greatest Common Divisors

Colin Stirling

Informatics

Some slides based on ones by Myrto Arapinis

Primes

Definition

A positive integer $p > 1$ is called prime iff the only positive factors of p are 1 and p. Otherwise it is called composite

Primes

Definition

A positive integer $p > 1$ is called prime iff the only positive factors of p are 1 and p. Otherwise it is called composite

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer greater than 1 *can be written uniquely as a prime or as the product of its prime factors, written in order of nondecreasing size*

Primes

Definition

A positive integer $p > 1$ is called prime iff the only positive factors of p are 1 and p. Otherwise it is called composite

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer greater than 1 *can be written uniquely as a prime or as the product of its prime factors, written in order of nondecreasing size*

$765 = 3 \cdot 3 \cdot 5 \cdot 17 = 3^2 \cdot 5 \cdot 17$

Proof of fundamental theorem

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer greater than 1 *can be written uniquely as a prime or as the product of its prime factors, written in order of nondecreasing size*

Proof of fundamental theorem

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer greater than 1 can be written uniquely as a prime or as the product of its prime factors, written in order of nondecreasing size

Showed by induction if $n > 1$ is an integer then n can be written as a product of primes

Proof of fundamental theorem

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer greater than 1 can be written uniquely as a prime or as the product of its prime factors, written in order of nondecreasing size

Showed by induction if $n > 1$ is an integer then n can be written as a product of primes

Missing is uniqueness

Proof of fundamental theorem

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer greater than 1 can be written uniquely as a prime or as the product of its prime factors, written in order of nondecreasing size

Showed by induction if $n > 1$ is an integer then n can be written as a product of primes

Missing is uniqueness

Lemma if p is prime and $p|a_1 a_2 \ldots a_n$ where each a_i is an integer, then $p|a_j$ for some $1 \leq j \leq n$

Proof of fundamental theorem

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer greater than 1 can be written uniquely as a prime or as the product of its prime factors, written in order of nondecreasing size

Showed by induction if $n > 1$ is an integer then n can be written as a product of primes

Missing is uniqueness

Lemma if p is prime and $p | a_1 a_2 \ldots a_n$ where each a_i is an integer, then $p | a_j$ for some $1 \leq j \leq n$

By induction too

Proof of fundamental theorem

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer greater than 1 can be written uniquely as a prime or as the product of its prime factors, written in order of nondecreasing size

Showed by induction if $n > 1$ is an integer then n can be written as a product of primes

Missing is uniqueness

Lemma if p is prime and $p|a_1 a_2 \ldots a_n$ where each a_i is an integer, then $p|a_j$ for some $1 \leq j \leq n$

By induction too

Now result follows

There are infinitely many primes

There are infinitely many primes

Lemma Every natural number greater than one is either prime or it has a prime divisor

There are infinitely many primes

Lemma Every natural number greater than one is either prime or it has a prime divisor

Follows from fundamental theorem

There are infinitely many primes

Lemma Every natural number greater than one is either prime or it has a prime divisor

Follows from fundamental theorem

Proof Suppose towards a contradiction that there are only finitely many primes $p_1, p_2, p_3, \ldots, p_k$. Consider the number $q = p_1 p_2 p_3 \ldots p_k + 1$, the product of all the primes plus one. By hypothesis q cannot be prime because it is strictly larger than all the primes. Thus, by the lemma, it has a prime divisor, p. Because $p_1, p_2, p_3, \ldots, p_k$ are all the primes, p must be equal to one of them, so p is a divisor of their product. So we have that p divides $p_1 p_2 p_3 \ldots p_k$, and p divides q, but that means p divides their difference, which is 1. Therefore $p \leq 1$. Contradiction. Therefore there are infinitely many primes.

The Sieve of Eratosthenes

How to find all primes between 2 and n?

The Sieve of Eratosthenes

How to find all primes between 2 and n?

A very inefficient method of determining if a number n is prime

Try every integer $i \leq \sqrt{n}$ and see if n is divisible by i

1. Write the numbers $2, \ldots, n$ into a list. Let $i := 2$

The Sieve of Eratosthenes

How to find all primes between 2 and n?

A very inefficient method of determining if a number n is prime

Try every integer $i \leq \sqrt{n}$ and see if n is divisible by i

1. Write the numbers $2, \ldots, n$ into a list. Let $i := 2$
2. Remove all strict multiples of i from the list

The Sieve of Eratosthenes

How to find all primes between 2 and n?

A **very inefficient** method of determining if a number n is prime

Try every integer $i \leq \sqrt{n}$ and see if n is divisible by i

1. Write the numbers $2, \ldots, n$ into a list. Let $i := 2$
2. Remove all strict multiples of i from the list
3. Let k be the smallest number present in the list s.t. $k > i$ and let $i := k$

The Sieve of Eratosthenes

How to find all primes between 2 and n?

A very inefficient method of determining if a number n is prime

Try every integer $i \leq \sqrt{n}$ and see if n is divisible by i

1. Write the numbers $2, \ldots, n$ into a list. Let $i := 2$
2. Remove all strict multiples of i from the list
3. Let k be the smallest number present in the list s.t. $k > i$ and let $i := k$
4. If $i > \sqrt{n}$ then stop else go to step 2

The Sieve of Eratosthenes

How to find all primes between 2 and n?

A very inefficient method of determining if a number n is prime

Try every integer $i \leq \sqrt{n}$ and see if n is divisible by i

1. Write the numbers $2, \ldots, n$ into a list. Let $i := 2$
2. Remove all strict multiples of i from the list
3. Let k be the smallest number present in the list s.t. $k > i$ and let $i := k$
4. If $i > \sqrt{n}$ then stop else go to step 2

Testing if a number is prime can be done efficiently in polynomial time [Agrawal-Kayal-Saxena 2002], i.e., polynomial in the number of bits used to describe the input number. Efficient randomized tests had been available previously.

Greatest common divisor

Definition

Let $a, b \in \mathbb{Z}^+$.The largest integer d such that $d|a$ and $d|b$ is called the greatest common divisor of a and b, written $\gcd(a, b)$

Greatest common divisor

Definition

Let $a, b \in \mathbb{Z}^+$.The largest integer d such that $d|a$ and $d|b$ is called the greatest common divisor of a and b, written $\gcd(a, b)$

$\gcd(24, 36) = 12$

Greatest common divisor

Definition

Let $a, b \in \mathbb{Z}^+$.The largest integer d such that $d|a$ and $d|b$ is called the greatest common divisor of a and b, written $\gcd(a, b)$

$\gcd(24, 36) = 12$

Definition

The integers a and b are relatively prime (coprime) iff $\gcd(a, b) = 1$

Greatest common divisor

Definition

Let $a, b \in \mathbb{Z}^+$.The largest integer d such that $d|a$ and $d|b$ is called the greatest common divisor of a and b, written $\gcd(a, b)$

$\gcd(24, 36) = 12$

Definition

The integers a and b are relatively prime (coprime) iff $\gcd(a, b) = 1$

9 and 22 are coprime (both are composite)

Gcd by prime factorisations

Suppose that the prime factorisations of *a* and *b* are

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \qquad\qquad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

where each exponent is a nonnegative integer (possibly zero)

Gcd by prime factorisations

Suppose that the prime factorisations of a and b are

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \qquad\qquad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

where each exponent is a nonnegative integer (possibly zero)

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$$

Gcd by prime factorisations

Suppose that the prime factorisations of a and b are

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \qquad\qquad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

where each exponent is a nonnegative integer (possibly zero)

$$\gcd(a, b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$$

This number clearly divides a and b. No larger number can divide both a and b. Proof by contradiction and the prime factorisation of a postulated larger divisor.

Gcd by prime factorisations

Suppose that the prime factorisations of a and b are

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \qquad\qquad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

where each exponent is a nonnegative integer (possibly zero)

$$\gcd(a, b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$$

This number clearly divides a and b. No larger number can divide both a and b. Proof by contradiction and the prime factorisation of a postulated larger divisor.

Factorisation is a very inefficient method to compute gcd

Euclidian algorithm: efficient for computing gcd

Euclidian algorithm

```
algorithm gcd(x,y)
    if y = 0
    then return(x)
    else return(gcd(y,x mod y))
```

Euclidian algorithm: efficient for computing gcd

Euclidian algorithm

```
algorithm gcd(x,y)
    if y = 0
    then return(x)
    else return(gcd(y,x mod y))
```

The Euclidian algorithm relies on

$$\forall x, y \in \mathbb{Z}\ (x > y \rightarrow \mathrm{gcd}(x, y) = \mathrm{gcd}(y, x \bmod y))$$

Euclidian algorithm (proof of correctness)

Lemma

If $a = bq + r$, where a, b, q, and r are positive integers, then $\gcd(a, b) = \gcd(b, r)$

Euclidian algorithm (proof of correctness)

Lemma

If $a = bq + r$, where a, b, q, and r are positive integers, then $\gcd(a, b) = \gcd(b, r)$

Proof.

($\Rightarrow$) Suppose that d divides both a and b. Then d also divides $a - bq = r$. Hence, any common divisor of a and b must also be a common divisor of b and r

($\Leftarrow$) Suppose that d divides both b and r. Then d also divides $bq + r = a$. Hence, any common divisor of b and r must also be a common divisor of a and b.

Therefore, $\gcd(a, b) = \gcd(b, r)$ □

Gcd as a linear combination

Theorem (Bézout's theorem)

If x and y are positive integers, then there exist integers a and b such that $gcd(x, y) = ax + by$

Gcd as a linear combination

Theorem (Bézout's theorem)

If x and y are positive integers, then there exist integers a and b such that $gcd(x, y) = ax + by$

Proof.

Let S be the set of positive integers of the form $ax + by$ (where a or b may be a negative integer); clearly, S is non-empty as it includes $x + y$. By the well-ordering principle S has a least element c. So $c = ax + by$ for some a and b. If $d|x$ and $d|y$ then $d|ax$ and $d|by$ and so $d|(ax + by)$, that is $d|c$. We now show $c|x$ and $c|y$ which means that $c = \gcd(x, y)$. Assume $c \not| x$. So $x = qc + r$ where $0 < r < c$. Now $r = x - qc = x - q(ax + by)$. That is, $r = (1 - qa)x + (-qb)y$, so $r \in S$ which contradicts that c is the least element in S as $c < r$. The same argument shows $c|y$. □

Computing Bézout coefficients

$2 = \gcd(6, 14) = (-2) \cdot 6 + 1 \cdot 14$

Computing Bézout coefficients

$2 = \gcd(6, 14) = (-2) \cdot 6 + 1 \cdot 14$

Extended Euclidian algorithm

```
algorithm extended-gcd(x,y)
    if y = 0
    then return(x, 1, 0)
    else
     (d, a, b) := extended-gcd(y, x mod y)
     return((d, b, a - ((x div y) * b)))
```

Further properties

Theorem

If a, b, c are positive integers such that $gcd(a, b) = 1$ and $a|bc$ then $a|c$

Further properties

Theorem

If a, b, c are positive integers such that $\gcd(a, b) = 1$ and $a|bc$ then $a|c$

Proof.

Because $\gcd(a, b) = 1$, by Bézout's theorem there are integers s and t such that $sa + tb = 1$. So, $sac + tbc = c$. Assume $a|bc$. Therefore, $a|tbc$ and $a|sac$, so $a|(sac + tbc)$; that is, $a|c$. □

Further properties

Theorem

If a, b, c are positive integers such that $gcd(a, b) = 1$ and $a|bc$ then $a|c$

Proof.

Because $\gcd(a, b) = 1$, by Bézout's theorem there are integers s and t such that $sa + tb = 1$. So, $sac + tbc = c$. Assume $a|bc$. Therefore, $a|tbc$ and $a|sac$, so $a|(sac + tbc)$; that is, $a|c$. □

Theorem

Let m be a positive integer and let a, b, c be integers. If $ac \equiv bc \pmod{m}$ and $gcd(c, m) = 1$ then $a \equiv b \pmod{m}$

Further properties

Theorem

If a, b, c are positive integers such that $gcd(a, b) = 1$ and $a|bc$ then $a|c$

Proof.

Because $\gcd(a, b) = 1$, by Bézout's theorem there are integers s and t such that $sa + tb = 1$. So, $sac + tbc = c$. Assume $a|bc$. Therefore, $a|tbc$ and $a|sac$, so $a|(sac + tbc)$; that is, $a|c$. □

Theorem

Let m be a positive integer and let a, b, c be integers. If $ac \equiv bc \pmod{m}$ and $gcd(c, m) = 1$ then $a \equiv b \pmod{m}$

Proof.

Because $ac \equiv bc \pmod{m}$, it follows $m|(ac - bc)$; so, $m|c(a - b)$. By the result above because $\gcd(c, m) = 1$, it follows that $m|(a - b)$. □