

Primes and Relatively Primes

Discrete Mathematics
Evgeny Skvortsov

Previous Lecture

- Integers
- Division
- Representation of integers

Primes

- Every integer n (except for 1 and -1) has at least 2 positive divisors, 1 and n (or $-n$).
- A positive number that does not have any other positive divisor is called **prime**
- Prime numbers: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, ...
- Mersenne numbers are the numbers of the form $M_n = 2^n - 1$
- There are many prime numbers among Mersenne numbers. The greatest known prime number is $M_{32582657} = 2^{32582657} - 1$
- The next candidate is $M_{M_{61}} = 2^{2305843009213693951} - 1$
- A positive number that is not prime is called **composite**

Composite Numbers

- Every composite number has a prime divisor.

- Proof.

Let S be the set of all composite numbers that do not have a prime divisor

Since $S \subseteq \mathbb{N}$, by the Well-Ordering Principle, it has a least element r .

As r is not prime, it has a divisor, therefore, $r = uv$ for some positive integers u and v .

$u < r$ and $v < r$. Therefore $u \notin S$, and u has a prime divisor p .

Since $p \mid u$ and $u \mid r$, we conclude that $p \mid r$, a contradiction.

How many prime numbers are there?

- **Theorem** (Euclid)

There are infinitely many prime numbers.

- **Proof.**

By contradiction. Suppose that $\{p_1, p_2, \dots, p_k\}$ is the set of all prime numbers, and let $a = p_1 p_2 \dots p_k + 1$

Since a is greater than any member of the list, a is composite.

By the previous statement, a has a prime divisor, that is for some p_j we have $p_j \mid a$

Since $p_j \mid a$ and $p_j \mid p_1 p_2 \dots p_k$ we have $p_j \mid a - p_1 p_2 \dots p_k = 1$

A contradiction.

- If n is a positive integer, then there are approximately $\frac{n}{\ln n}$ prime numbers not exceeding n

Open Problems about Primes

● Goldbach's Conjecture

Every positive even number can be represented as the sum of two prime numbers.

For example: $4 = 2 + 2$, $8 = 5 + 3$, $42 = 37 + 5$

Goldbach's conjecture is known to be true for even numbers up to 2×10^{17}

● The Twin Prime Conjecture

Twin primes are primes that differ by 2, such as 3 and 5, 5 and 7, 11 and 13, etc.

The Twin Prime Conjecture asserts that there are infinitely many twin primes.

The record twin primes:

$$16,896,987,339,975 \times 2^{171,960} \pm 1$$

The Greatest Common Divisor

- For integers a and b , a positive integer c is said to be a **common divisor of a and b** if $c \mid a$ and $c \mid b$
- Let a, b be integers such that $a \neq 0$ or $b \neq 0$. Then a positive integer c is called the **greatest common divisor of a, b** if
 - $c \mid a$ and $c \mid b$ (that is c is a common divisor of a, b)
 - for any common divisor d of a and b , we have $d \mid c$
- What are the common divisors, and the greatest common divisor of 42 and 70?
- The greatest common divisor of a and b is denoted by $\gcd(a, b)$

The Greatest Common Divisor (cntd)

● Theorem

For any positive integers a and b , there is a unique positive integer c such that c is the greatest common divisor of a and b

● Proof. Given a, b , let $S = \{as + bt \mid s, t \in \mathbb{Z}, as + bt > 0\}$.

Since $S \neq \emptyset$, it has a least element c . We show that $c = \gcd(a, b)$

We have $c = ax + by$ for some integers x and y .

If $d \mid a$ and $d \mid b$, then $d \mid ax + by = c$.

If $c \nmid a$, we can use the division algorithm to find $a = qc + r$, where q, r are integers and $0 < r < c$.

Then $r = a - qc = a - q(ax + by) = a(1 - qx) + b(-qy) \in S$, a contradiction

Therefore $c \mid a$, and by a similar argument $c \mid b$.

Finally, if c and d are greatest common divisors, then $c \mid d$ and $d \mid c$. Thus $c = d$.

Euclidean Algorithm: Small Example

- To warm up, let us find the greatest common divisor of 287 and 91
$$287 = 91 \cdot 3 + 14$$

Note that any common divisor of 287 and 91 is also a divisor of $14 = 287 - 91 \cdot 3$.

Conversely, every common divisor of 91 and 14 is also a divisor of $287 = 91 \cdot 3 + 14$. Thus $\gcd(287, 91) = \gcd(91, 14)$.

Next $91 = 14 \cdot 6 + 7$.

By the same argument $\gcd(91, 14) = \gcd(14, 7)$.

Finally, since $7 \mid 14$, $\gcd(14, 7) = 7$.

Thus, $\gcd(287, 91) = 7$.

Euclidean Algorithm: Key Property

● Lemma.

Let $a = bq + r$, where a , b , q , and r are integers.
Then $\gcd(a,b) = \gcd(b,r)$

● Proof

Let d be a common divisor of a and b . Then d also divides $r = a - bq$. Thus, d is a common divisor of b and r .

Now, let d be a common divisor of b and r . Then d also divides $a = bq + r$.

Therefore the pairs a,b and b,r have the same common divisors.
Hence, $\gcd(a,b) = \gcd(b,r)$.

Euclidean Algorithm: The Algorithm

- Let a and b be positive integers with $a \geq b$. Set $r_0 = a$ and $r_1 = b$. Successively apply the division algorithm until the remainder is 0

$$r_0 = r_1 q_1 + r_2 \quad 0 \leq r_2 < r_1$$

$$r_1 = r_2 q_2 + r_3 \quad 0 \leq r_3 < r_2$$

$$\vdots$$

$$r_{k-2} = r_{k-1} q_{k-1} + r_k \quad 0 \leq r_k < r_{k-1}$$

- Eventually, the remainder is zero, because the sequence of remainders $a = r_0 > r_1 > r_2 > \dots \geq 0$ cannot contain more than a elements.

- Furthermore, $\gcd(a, b) = \gcd(r_0, r_1) = \dots = \gcd(r_{k-2}, r_{k-1})$

$$= \gcd(r_{k-1}, r_k) = \gcd(r_k, 0) = r_k$$

- Hence $\gcd(a, b)$ is the last nonzero remainder in the sequence

Euclidean Algorithm: Pseudocode

- The Euclidean algorithm expressed in pseudocode:

```
procedure gcd(a, b: positive integers)
  x := a
  y := b
  while y  $\neq$  0 do
    r := x mod y
    x := y
    y := r
  end      { gcd(a,b) is x }
```

Homework

Exercises from the Book:

No. 1ab, 4, 5, 10, 15 (page 237)

No. 1ab, 5, 7, 9 (page 241)