Primes and divisors

Discrete Mathematics

Courtesy of Andrei Bulatov

Previous Lecture

- *Integers*
- *Division, properties of divisibility*
- *The division algorithm*
- *Base b representation of numbers*
  - *Repeatedly divide by b and collect remainders*

$$
\begin{aligned}
n &= bq_0 + r_0 \\
q_0 &= bq_1 + r_1 \\
q_1 &= bq_2 + r_2 \\
&\dots \\
q_k &= bq_k + r_k
\end{aligned}
\quad \Rightarrow \quad
\begin{aligned}
n &= bq_0 + r_0 \\
&= b(bq_1 + r_1) + r_0 \\
&= b^2q_1 + br_1 + r_0 \\
&\dots \\
&= b^kr_k + \dots + b^3r_3 + b^2r_2 + br_1 + r_0
\end{aligned}
$$

Primes

- *Every integer n (except for 1 and -1) has at least 2 positive divisors, 1 and n itself (or -n).*
- *A positive number that does not have any other positive divisor is called prime.*
- *Examples:*

  Small primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, …

  Large primes: $2^{77232917} - 1$
- *Mersenne numbers are numbers of the form* $M_n = 2^n - 1$
- *Greatest known Mersenne prime is* $M_{77232917} = 2^{77232917} - 1$
- *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. (by contradiction)*

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, i.e. $r = uv$ for some positive integers u and v with $u < r$ and $v < r$.

But $u \notin S$, so 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 $\{p_1, p_2, \ldots, p_k\}$ *is the set of all prime numbers, and let*
  $$a = p_1 p_2 \ldots p_k + 1$$
  Since a *is greater than any member of the list,* a *is composite.*
  Hence a *has a non-trivial prime divisor* p_j
  Since $p_j \mid a$ *and,* $p_j \mid p_1 p_2 \ldots p_k$ *we have* $p_j \mid a - p_1 p_2 \ldots p_k = 1$
  So $p_j = 1$, *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 $4 \cdot 10^{18}$

- *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: $2{,}996{,}863{,}034{,}895 \cdot 2^{1{,}290{,}000} \pm 1$

The Greatest Common Divisor

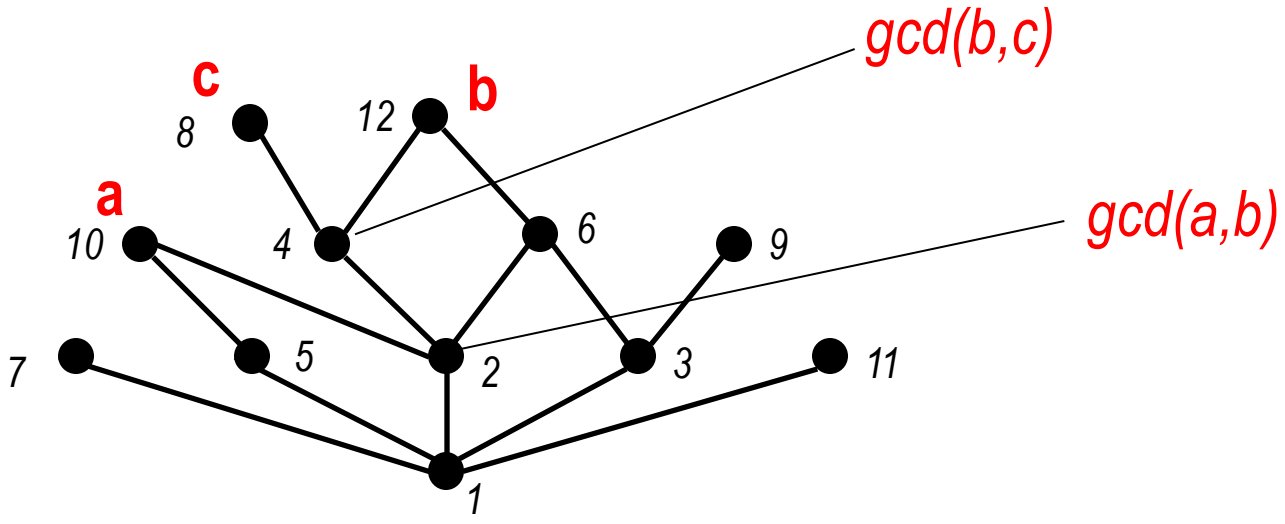
- *For integers a and b, a positive integer c is said to be a common divisor of a and b if* $c \mid a$ *and* $c \mid b$
- *Let a, b be integers such that* $a \neq 0$ *or* $b \neq 0$. *Then a positive integer c is called the greatest common divisor of a, b if*
  - *(a)* $c \mid a$ *and* $c \mid b$ *(that is c is a common divisor of a, b)*
  - *(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?* $42 = 2 \cdot 21 = 2 \cdot 3 \cdot 7$ $70 = 2 \cdot 5 \cdot 7$
- *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



The Greatest Common Divisor (cntd)

- **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* $c = ax + by$.

  We show that $c = gcd(a,b)$

  Bezout's identity

  Step 1: $c \mid a$

  If $c \nmid a$, *by Euclidean division* $a = qc + r$, *where* $0 < r < c$.

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

  Hence we have a contradiction, so $c \mid a$. *Similar for* $c \mid b$

  Step 2: Is it the greatest common divisor?

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

Euclidean Algorithm: Small Example

- *To warm up, let us find the greatest common divisor of 287 and 91*
- *First let's divide 287 by 91:*

$$287 = 91 \cdot 3 + 14$$

- *Note that any common divisor of 91 and 14 also divides 287*
- *Also, $14 = 287 - 91 \cdot 3$, so any divisor of 287 and 91 also divides 14*
- *Thus, gcd(287,91) = gcd(91,14)!*
- *Now $91 = 14 \cdot 6 + 7$, so gcd(91,14) = gcd(14, 7)!*
- *Since 7 divides 14,*

$$gcd(14, 7) = 7 = gcd(287, 91)$$

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*

$$\begin{aligned} r_0 &= r_1 q_1 + r_2 & 0 < r_2 < r_1 \\ r_1 &= r_2 q_2 + r_3 & 0 < r_3 < r_2 \\ &\vdots \\ r_{k-2} &= r_{k-1} q_{k-1} + r_k & 0 < r_k < r_{k-1} \\ r_{k-1} &= r_k q_k \end{aligned}$$

- *Eventually, the remainder is zero, because the sequence of remainders $a = r_0 > r_1 > r_2 > \ldots \geq 0$ cannot contain infinitely many elements.*
- *Furthermore, $\gcd(a,b) = \gcd(r_0, r_1) = \cdots = \gcd(r_{k-2}, r_{k-1})$*

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

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

Greatest Common Divisor

- **Theorem**.

  If a, b are integers and d is their greatest common divisor, then there are integers u, v such that $d = au + bv$.

- **Proof**.

  We use the Euclidean algorithm and the notation $a = r_0,\ b = r_1,\ d = r_k$

  We have

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 \\
&\vdots \\
r_{k-3} &= r_{k-2} q_{k-2} + r_{k-1} \\
r_{k-2} &= r_{k-1} q_{k-1} + r_k \\
r_{k-1} &= r_k q_k
\end{aligned}$$

$$\begin{aligned}
d = r_k &= r_{k-2} - r_{k-1} q_{k-1} \\
&= r_{k-2} - (r_{k-3} - r_{k-2} q_{k-2}) q_{k-1} \\
&= (r_{k-4} - r_{k-3} q_{k-3}) - (r_{k-3} - (r_{k-4} - r_{k-3} q_{k-3}) q_{k-2}) q_{k-1} \\
&\vdots \\
&= r_0 u + r_1 v = au + bv
\end{aligned}$$

Example

- *Find d = gcd(821,123) and u and v such that d = 821u + 123v*

$821 = 6 \cdot 123 + 83$

$123 = 1 \cdot 83 + 40$

$83 = 2 \cdot 40 + 3$

$40 = 13 \cdot 3 + 1$

$3 = 3 \cdot 1 + 0$

$1 = 40 - 13 \cdot 3$

$= 40 - 13 \cdot (83 - 2 \cdot 40)$

$= 27 \cdot 40 - 13 \cdot 83$

$= 27 \cdot (123 - 1 \cdot 83) - 13 \cdot 83$

$= 27 \cdot 123 - 40 \cdot 83$

$= 27 \cdot 123 - 40 \cdot (821 - 6 \cdot 123)$

$= 267 \cdot 123 - 40 \cdot 821$

More Primes

- *Prime numbers have some very special properties with respect to division*
- **Properties of primes**.

(1) If a,b are integers and p is prime such that $p \mid ab$ then $p \mid a$ or $p \mid b$.

(2) Let a_i be an integer for $1 \le i \le n$, and p is prime and $p \mid a_1 a_2 \ldots a_n$ then $p \mid a_i$ for some $1 \le i \le n$

The Fundamental Theorem of Arithmetic

- **Theorem**.

  Every integer $n > 1$ can be represented uniquely as a product of primes, up to the order of the primes.

- **Proof**.

- *Existence*

  By contradiction. Suppose that there is an $n > 1$ that cannot be represented as a product of primes, and let m be the smallest such number.

  m is not prime, therefore $m = st$ for some s and t

  But then s and t can be written as products of primes, because $s < m$ and $t < m$.

  Therefore m is a product of primes

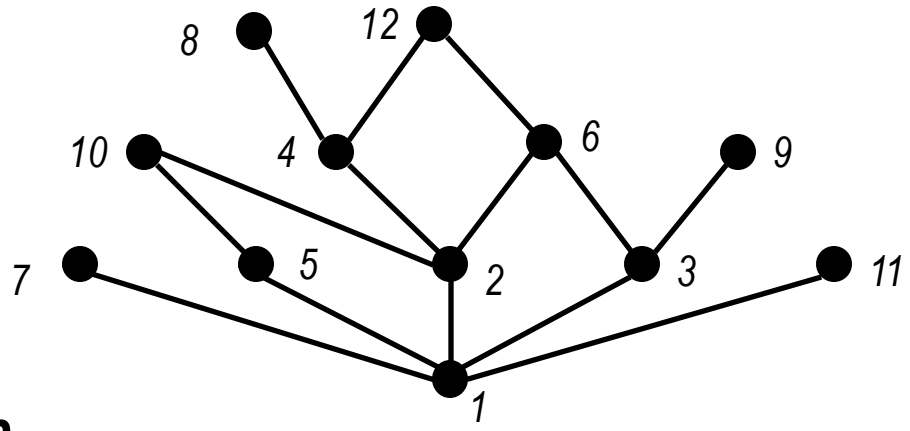
Example

- *Find the prime factorization of 4270*

Least Common Multiple

- *A positive integer c is called a common multiple of integers a and b if a | c and b | c*

- *The number c is called the least common multiple of a and b, denoted lcm(a,b) if it is a common multiple and for any common multiple d we have c | d*



- **Theorem.**
  For any integers a and b, the least common multiple exists.

Least Common Multiple (cntd)

- *Find lcm(15,21).*

- **Theorem**

  For any integers a and b we have $ab = lcm(a,b) \cdot gcd(a,b)$

Relatively Prime

- *Numbers a and b such that gcd(a,b) = 1 are called relatively prime*
- *How many relatively prime numbers are there?*
- *Euler's totient function φ(n) is the number of numbers k such that 0 < k < n and n and k are relatively prime.*
- *If p is prime then every k < p is relatively prime with p. Hence, φ(p) = p – 1.*
- **Lemma**.

  If a and b are relatively prime then φ(ab) = φ(a) · φ(b)
- **Corollary**.

  If $n = p_1^{s_1} p_2^{s_2} \ldots p_u^{s_u}$ *is the prime factorization of n, then*

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right)^{s_1} \left(1 - \frac{1}{p_2}\right)^{s_2} \cdots \left(1 - \frac{1}{p_u}\right)^{s_u}$$

Practice

Exercises from the Book:

7th edition: 2ef, 3ef, 5, 22, 24b, 26, 31, 33cd (page 272 – 273)

8th edition: 2ef, 3ef, 5, 22, 24b, 26, 31, 33cd (page 288 – 289)