Common Divisors

Discrete Mathematics
Andrei Bulatov

Previous Lecture

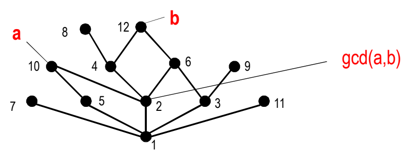
- Representation of numbers
- Prime and composite numbers

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 | a and c | 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 | a and c | b (that is c is a common divisor of a, b)
  - (b) for any common divisor d of a and b, we have d | 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
- First try:
  Take the largest common divisor, in the sense of usual order
  Does not work: Why every other common divisor divides it?



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. We show that c = gcd(a,b)
  We have c = ax + by for some integers x and y.
  If d | a and d | b, then d | 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 | a, and by a similar argument c | b.

The Greatest Common Divisor (cntd)

- **Proof.** (cntd)
  Finally, if c and d are greatest common divisors, then c | d and d | c. Thus c = d.

  Q. E. 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 | 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 $a \ge b$. Set $r_0 = a$ and $r_1 = b$ Successively apply the division algorithm until the remainder is 0

$$\begin{array}{ll} r_0 = r_1q_1 + r_2 & 0 \le r_2 < r_1 \\ r_1 = r_2q_2 + r_3 & 0 \le r_3 < r_2 \\ \vdots & \\ r_{k-2} = r_{k-1}q_{k-1} + r_k & 0 \le r_k < r_{k-1} \\ r_{k-1} = r_kq_k & \end{array}$$

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

$$\begin{array}{l} r_0 = r_1q_1 + r_2 \\ \vdots \\ r_{k-3} = r_{k-2}q_{k-2} + r_{k-1} \\ r_{k-2} = r_{k-1}q_{k-1} + r_k \\ r_{k-1} = r_kq_k \end{array}$$

$$\begin{aligned} d = r_k &= r_{k-2} - r_{k-1}q_{k-1} \\ &= r_{k-2} - (r_{k-3} - r_{k-2}q_{k-2})q_{k-1} \\ &= (r_{k-4} - r_{k-3}q_{k-3}) - (r_{k-3} - (r_{k-4} - r_{k-3}q_{k-3})q_{k-2})q_{k-1} \\ &\vdots \\ &= r_0u + r_1v = au + bv \end{aligned}$$

Example

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

  d = 821u + 123v

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 | ab then p | a or p | b.

  (2) Let a_i be an integer for $1 \le i \le n$, and p is prime and $p \mid a_1a_2\ldots a_n$ 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 as a product of primes uniquely, 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 980,220

Least Common Multiple

- A positive integer c is called a common multiple of integers a and b if $a \mid c$ and $b \mid c$
- The number c is called the least common multiple of a and b, denoted $\mathrm{lcm}(a,b)$ if it is a common multiple and for any common multiple d we have $c \mid d$
- **Theorem**.
  For any integers a and b, the least common multiple exists.

Least Common Multiple (cntd)

- Find lcm(231,455).
- **Theorem**
  For any integers a and b we have $ab = \mathrm{lcm}(a,b) \cdot \gcd(a,b)$

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 $\varphi(n)$ 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, $\varphi(p) = p - 1$.
- **Lemma**.
  If a and b are relatively prime then $\varphi(ab) = \varphi(a) \cdot \varphi(b)$
- **Corollary**.
  If $n = p_1^{s_1} p_2^{s_2} \dots p_u^{s_u}$ is the prime factorization of n, then

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

Homework

Exercises from the Book:
No. 1ab, 4, 5, 10, 15 (page 237)
No. 1ab, 5, 7, 9 (page 241)