Miscellaneous

CS 220 — Applied Discrete Mathematics

May 6, 2024

Intervals of Real Numbers

The following notations are used for *real* intervals:

$$
\begin{aligned}
[a, b] &= \{x \mid x \in \mathbb{R},\ a \leq x \leq b\} \\
(a, b) &= \{x \mid x \in \mathbb{R},\ a < x < b\} \\
[a, b) &= \{x \mid x \in \mathbb{R},\ a \leq x < b\} \\
(a, b] &= \{x \mid x \in \mathbb{R},\ a < x \leq b\}
\end{aligned}
$$

That is, a square bracket means “include that endpoint” and a parenthesis means “don’t include that endpoint”.

- An interval $[a, b]$ is called a **closed interval**.
- An interval (a, b) is called an **open interval**.
- Intervals of the form $[a, b)$ and $(a, b]$ are called **half-open intervals**.

Intervals of Integers

The following notations are used for integers:

$$[a\mathinner{..}b] = \{n \mid n \in \mathbb{Z},\ a \le n \le b\}$$
$$\{a, \ldots, b\} = \{n \mid n \in \mathbb{Z},\ a \le n \le b\}$$

There is no standard notation for open or half-open integer intervals, but one might describe the range of values of i in the following loop as the half-open interval from 0 (inclusive) to n (exclusive):

```
for (int i = 0; i < n; ++i) { ... }
```

Examples

$[4\mathinner{..}8] = \{4, 5, 6, 7, 8\}$ $\quad [7\mathinner{..}7] = \{7\}$ $\quad [4\mathinner{..}3] = \emptyset$

The Fundamental Theorem of Arithmetic, Revisited

Recall this theorem:

Theorem (The Fundamental Theorem of Arithmetic)

Every positive integer greater than 1 can be uniquely expressed as a product of primes, where the prime factors are written in increasing size. (A prime may occur more than once in the product.)

Let’s write each prime factor once with an exponent.

Examples

$$\begin{aligned} 24 &= 2^3 \cdot 3^1 \\ 180 &= 2^2 \cdot 3^2 \cdot 5^1 \\ 525 &= 2^0 \cdot 3^1 \cdot 5^2 \cdot 7^1 \end{aligned}$$

Greatest Common Divisor and Least Common Multiple

Recall these definitions:

Definitions

Let $a, b \in \mathbb{Z}^+$.

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

The least common multiple (LCM) of a and b, written $\operatorname{lcm}(a, b)$, is the least $m \in \mathbb{Z}^+$ such that $a|m$ and $b|m$.

The GCD and LCM can both be calculated from the prime factorizations:

- For the GCD, take the *minimum* of the exponents of a and b for each prime factor.
- For the LCM, take the *maximum* of the exponents of a and b for each prime factor.

Examples: GCD and LCM

Examples

$$
\begin{aligned}
\gcd(24, 180) &= \gcd((2^3 \cdot 3^1),\ (2^2 \cdot 3^2 \cdot 5^1)) \\
&= 2^{\min(3,2)} \cdot 3^{\min(1,2)} \cdot 5^{\min(0,1)} \\
&= 2^2 \cdot 3^1 \cdot 5^0 = 12 \\
\operatorname{lcm}(24, 180) &= \operatorname{lcm}((2^3 \cdot 3^1),\ (2^2 \cdot 3^2 \cdot 5^1)) \\
&= 2^{\max(3,2)} \cdot 3^{\max(1,2)} \cdot 5^{\max(0,1)} \\
&= 2^3 \cdot 3^2 \cdot 5^1 = 360
\end{aligned}
$$

Euclid's Algorithm

There is a better algorithm for finding the GCD of two integers that dates back to Euclid's *Elements*, from around 300 BC.

Euclid's Algorithm

Given $a, b \in \mathbb{N}$, we want $\gcd(a, b)$. Suppose $a \geq b$. There are two cases:

- **Case $b > 0$:** We divide a by b to get the remainder r. Then we recur on b and r. That is, $\gcd(a, b)$ is equal to $\gcd(b, r)$, where $r = a \bmod b$.
- **Case $b = 0$:** Then we stop, because $\gcd(a, 0) = a$.

Example

Suppose we want to find $\gcd(287, 91)$.

$$\begin{aligned}
\gcd(287, 91) &= \gcd(91, 14) && \text{because } 287 = 3 \cdot 91 + 14 \\
&= \gcd(14, 7) && \text{because } 91 = 6 \cdot 14 + 7 \\
&= \gcd(7, 0) && \text{because } 14 = 2 \cdot 7 + 0 \\
&= 7
\end{aligned}$$

Correctness of Euclid's Algorithm

Lemma

Let $a, b \in \mathbb{N}$ with $a \geq b$ and $b \neq 0$. Then $\gcd(a, b) = \gcd(b, a \bmod b)$.

Proof.

A general property of divisibility is that for all $x, y, z \in \mathbb{Z}$, if $x|y$ and $x|z$, then $x|(y + z)$.

By division, there are q, r such that $a = qb + r$, where $r = a \bmod b$.

- By applying the divisibility property above to the equation for a, we see that any common divisor of b and $a \bmod b$ must also be a divisor of a.
- By rewriting the equation to $a \bmod b = a + (-q)b$ and applying the divisibility property again, we see that any common divisor of a and b is also a divisor of $a \bmod b$.

Since a, b have exactly the same common divisors as b and $a \bmod b$, their greatest common divisor must be the same. That is, $\gcd(a, b) = \gcd(b, a \bmod b)$. □

Euclid's Algorithm

In pseudocode, the algorithm can be implemented as follows:

Algorithm 1 $\mathrm{gcd}(a, b)$

Require: $a, b \in \mathbb{Z}^+$

$x := a$
$y := b$
while $y \neq 0$ **do**
    $r := x \bmod y$
    $x := y$
    $y := r$
end while
return x

The Extended Euclidean Algorithm

The GCD of x and y can be expressed as a linear combination of x and y. That is, $gcd(x, y) = sx + ty$ for some integers s and t.

We can use an extended version of the Euclidean algorithm to find s and t.

Example

Previously: $\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = \gcd(7, 0) = 7$.

$$\begin{aligned}
287 &= 3 \cdot 91 + 14 & \rightarrow && 14 &= 287 - 3 \cdot 91 \\
91 &= 6 \cdot 14 + 7 & \rightarrow && 7 &= 91 - 6 \cdot 14 \\
14 &= 2 \cdot 7 + 0
\end{aligned}$$

If we substitute backwards using the equations on the right:

$$\begin{aligned}
7 &= 91 - 6 \cdot 14 && \text{by 2nd equation} \\
&= 91 - 6 \cdot (287 - 3 \cdot 91) && \text{by 1st equation} \\
&= -6 \cdot 287 + 19 \cdot 91 && \text{by algebra}
\end{aligned}$$

The Multiplicative Inverse in Modular Arithmetic

Definition (Multiplicative Inverse)

Let $m \in \mathbb{Z}^+$, and let $x \in \mathbb{N}$. Then the **multiplicative inverse** of $x \pmod{m}$ is a number $y \in \{0, \ldots, m-1\}$ such that $xy \equiv 1 \pmod{m}$.

The multiplicative inverse is not guaranteed to exist.

Examples

- 3 is the multiplicative inverse of $7 \pmod{10}$ because $3 \cdot 7 = 21 \equiv 1 \pmod{10}$
- 7 is the multiplicative inverse of $7 \pmod{8}$ because $7 \cdot 7 = 49 \equiv 1 \pmod{8}$
- 4 does not have a multiplicative inverse $\pmod{6}$ 4 times anything is even, and no even number is $\equiv 1 \pmod{6}$.

Calculating the Multiplicative Inverse

We can use the extended Euclidean Algorithm to find the multiplicative inverse of $x \pmod{m}$:

- If $gcd(x, m) \neq 1$ then the multiplicative inverse does not exist.
- Otherwise (if x and m are relatively prime), the algorithm computes s and t such that $sx + tm = 1$.

  Thus $sx - 1 = -tm$, and thus $sx \equiv 1 \pmod{m}$ (by definition).

Example

We could use the extended Euclidean algorithm to calculate

$$\gcd(31, 43) = 1 = -18 \cdot 31 + 13 \cdot 43$$

Therefore, the multiplicative inverse of $31 \pmod{43}$ is $-18 \bmod 43 = 25$.

Final Exam Information

The final exam will be Wednesday, May 15, 3:00pm–6:00pm.

- Written exam. (Bring something to write with!)
- Notes: handwritten notes only (40 pages)
  No printouts, no photocopies, no books, etc.

Final Exam Topics

The final exam is **cumulative**:

- covers topics from entire semester
- emphasis on topics since midterm exam

New Topics

- Synthesis
- Proofs
- Recursion and Induction
- Computation (through slide 14)
- Counting
- Probability
- Graphs (through slide 27)
- Misc