Number Theory: Euclidean Algorithm & Congruences Sections 4.3-4.4

CS261 Mathematical Foundations of CS
Professor Leah Buechley
Spring 2024
University of New Mexico

Greatest Common Divisor [1]

Definition: Let *a* and *b* be integers, not both zero. The largest integer *d* such that $d \mid a$ and also $d \mid b$ is called the greatest common divisor of *a* and *b*. The greatest common divisor of *a* and *b* is denoted by gcd(*a*,*b*).

One can find greatest common divisors of small numbers by inspection.

Example: What is the greatest common divisor of 24 and 36?

Solution: gcd(24, 36) = 12

Example: What is the greatest common divisor of 17 and 22?

Solution: gcd(17,22) = 1

Greatest Common Divisor 2

Definition: The integers *a* and *b* are *relatively prime* if their greatest common divisor is 1.

Example: 17 and 22.

Definition: The integers $a_1, a_2, \ldots, a_n$ are *pairwise relatively prime* if $\gcd(a_i, a_j) = 1$ whenever $1 \le i < j \le n$.

Example: Determine whether the integers 10, 17 and 21 are pairwise relatively prime.

Solution: Because gcd(10,17) = 1, gcd(10,21) = 1, and gcd(17,21) = 1, 10, 17, and 21 are pairwise relatively prime.

Example: Determine whether the integers 10, 19, and 24 are pairwise relatively prime.

Solution: Because gcd(10,24) = 2, 10, 19, and 24 are not pairwise relatively prime.

Finding the Greatest Common Divisor Using Prime Factorizations

Suppose the prime factorizations of *a* and *b* are:

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

where each exponent is a nonnegative integer, and where all primes occurring in either prime factorization are included in both. Then:

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

This formula is valid since the integer on the right (of the equals sign) divides both *a* and *b*. No larger integer can divide both *a* and *b*.

Example: $120 = 2^3 \cdot 3 \cdot 5 \qquad 500 = 2^2 \cdot 5^3$

$$\gcd(120,500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 3^0 \cdot 5^1 = 20$$

Finding the gcd of two positive integers using their prime factorizations is not efficient because there is no efficient algorithm for finding the prime factorization of a positive integer.

Least Common Multiple

Definition: The least common multiple of the positive integers *a* and *b* is the smallest positive integer that is divisible by both *a* and *b*. It is denoted by lcm(*a*,*b*).

The least common multiple can also be computed from the prime factorizations.

$$\text{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \ldots p_n^{\max(a_n,bn)},$$

This number is divided by both *a* and *b* and no smaller number is divided by *a* and *b*.

Example: $\text{lcm}\left(2^3 3^5 7^2, 2^4 3^3\right) = 2^{\max(3,4)} \, 3^{\max(5,3)} \, 7^{\max(2,0)} = 2^4 \, 3^5 \, 7^2$

The greatest common divisor and the least common multiple of two integers are related by:

Theorem 5: Let a and b be positive integers. Then

$ab = \gcd(a,b) \cdot \text{lcm}(a,b)$

(*proof is Exercise* 31)

Euclidean Algorithm 1

The Euclidian algorithm is an efficient method for computing the greatest common divisor of two integers. It is based on the idea that gcd(a,b) is equal to gcd(a,c) when $a > b$ and c is the remainder when a is divided by b.

Euclid
(325 B.C.E. – 265 B.C.E.)

Example: Find gcd(91, 287):

- $287 = 91 \cdot 3 + 14$ — Divide 287 by 91
- $91 = 14 \cdot 6 + 7$ — Divide 91 by 14
- $14 = 7 \cdot 2 + 0$ — Divide 14 by 7

Stopping condition

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

Euclidean Algorithm 2

The Euclidean algorithm expressed in pseudocode is:

```
procedure gcd(a, b: positive integers)
x := a
y := b
while  y ≠ 0
    r := x mod y
    x := y
    y := r
return x {gcd(a,b) is x}
```

In Section 5.3, we'll see that the time complexity of the algorithm is O (log b), where a > b.

Correctness of Euclidean Algorithm 1

Lemma 1: Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a,b) = \gcd(b,r)$.

Proof:

- Suppose that d divides both a and b. Then d also divides $a - bq = r$ (by Theorem 1 of Section 4.1). Hence, any common divisor of a and b must also be any common divisor of b and r.
- Suppose that d divides both b and r. Then d also divides $bq + r = a$. Hence, any common divisor of a and b must also be a common divisor of b and r.
- Therefore, $\gcd(a,b) = \gcd(b,r)$.

Correctness of Euclidean Algorithm 2

Suppose that a and b are positive integers with $a \geq b$.

Let $r_0 = a$ and $r_1 = b$.

Successive applications of the division algorithm yields:

$$
\begin{array}{ll}
r_0 = r_1 q_1 + r_2 & 0 \leq r_2 < r_1, \\
r_1 = r_2 q_2 + r_3 & 0 \leq r_3 < r_2, \\
\cdot & \\
\cdot & \\
\cdot & \\
r_{n-2} = r_{n-1} q_{n-1} + r_2 & 0 \leq r_n < r_{n-1}, \\
r_{n-1} = r_n q_n. &
\end{array}
$$

Eventually, a remainder of zero occurs in the sequence of terms: $a = r_0 > r_1 > r_2 > \cdots \geq 0$. The sequence can't contain more than a terms.

By Lemma 1

$$\gcd(a,b) = \gcd(r_0, r_1) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n.$$

Hence the greatest common divisor is the last nonzero remainder in the sequence of divisions.

gcds as Linear Combinations

Étienne Bézout

(1730-1783)

Bézout's Theorem: If a and b are positive integers, then there exist integers s and t such that $\gcd(a,b) = sa + tb$.

(*proof in exercises of Section* 5.2)

Definition: If a and b are positive integers, then integers s and t such that $\gcd(a,b) = sa + tb$ are called *Bézout coefficients* of a and b. The equation $\gcd(a,b) = sa + tb$ is called *Bézout's identity.*

By Bézout's Theorem, the gcd of integers a and b can be expressed in the form $sa + tb$ where s and t are integers. This is a *linear combination* with integer coefficients of a and b.

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

Graphs of Functions

Example: Express gcd(252,198) = 18 as a linear combination of 252 and 198.

Solution: First use the Euclidean algorithm to show gcd(252,198) = 18

i. $252 = 1 \cdot 198 + 54$

ii. $198 = 3 \cdot 54 + 36$

iii. $54 = 1 \cdot 36 + 18$

iv. $36 = 2 \cdot 18$

Now working backwards, from iii and i above

- $18 = 54 - 1 \cdot 36.$
- $36 = 198 - 3 \cdot 54.$

Substituting the 2nd equation into the 1st yields:

- $18 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198.$

Substituting 54 = 252 − 1 ·198 (from i)) yields:

- $18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198.$

This method illustrated above is a two pass method. It first uses the Euclidian algorithm to find the gcd and then works backwards to express the gcd as a linear combination of the original two integers. A one pass method, called the *extended Euclidean algorithm*, is developed in the exercises.

Consequences of Bézout's Theorem

Lemma 2: If a, b, and c are positive integers such that gcd(a, b) = 1 and $a \mid bc$, then $a \mid c$.

Proof: Assume gcd(a, b) = 1 and $a \mid bc$

- Since gcd(a, b) = 1, by Bézout's Theorem there are integers s and t such that $sa + tb = 1$.
- Multiplying both sides of the equation by c, yields $sac + tbc = c$.
- From Theorem 1 of Section 4.1:
  $a \,/\, tbc$ (part ii) and a divides $sac + tbc$ since $a \,/\, sac$ and $a \,/\, tbc$ (part i)
- We conclude $a \,/\, c$, since $sac + tbc = c$.

Lemma 3: If p is prime and $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_i$ for some i. (*proof uses mathematical induction; see Exercise* 64 *of Section* 5.1)

Lemma 3 is crucial in the proof of the uniqueness of prime factorizations.

Uniqueness of Prime Factorization

We will prove that a prime factorization of a positive integer where the primes are in nondecreasing order is unique. (This part of the fundamental theorem of arithmetic. The other part, which asserts that every positive integer has a prime factorization into primes, will be proved in Section 5.2.)

Proof: (*by contradiction*) Suppose that the positive integer *n* can be written as a product of primes in two distinct ways:

$$n = p_1 p_2 \cdots p_s \text{ and } n = q_1 q_2 \cdots p_t .$$

- Remove all common primes from the factorizations to get.
- By Lemma 3, it follows that divides, for some *k,* contradicting the assumption that and are distinct primes.
- Hence, there can be at most one factorization of *n* into primes in nondecreasing order.

Dividing Congruences by an Integer

Dividing both sides of a valid congruence by an integer does not always produce a valid congruence (see Section 4.1).

But dividing by an integer relatively prime to the modulus does produce a valid congruence:

Theorem 7: Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c,m) = 1$, then $a \equiv b \pmod{m}$.

Proof: Since $ac \equiv bc \pmod{m}$, $m \mid ac - bc = c(a - b)$ by Lemma 2 and the fact that $\gcd(c,m) = 1$, it follows that $m \mid a - b$. Hence, $a \equiv b \pmod{m}$.

Solving Congruences

Section 4.4

Section Summary 4

Linear Congruences.

The Chinese Remainder Theorem.

Computer Arithmetic with Large Integers (*not currently included in slides, see text*).

Fermat's Little Theorem.

Pseudorandom.

Primitive Roots and Discrete Logarithms.

Linear Congruences

Definition: A congruence of the form

$ax \equiv b(\bmod m)$,

where *m* is a positive integer, *a* and *b* are integers, and *x* is a variable, is called a *linear congruence*.

The solutions to a linear congruence $ax \equiv b(\bmod m)$ are all integers *x* that satisfy the congruence.

Definition: An integer $\bar{a}$ such that $\bar{a}a \equiv 1(\bmod m)$ is said to be an *inverse* of *a* modulo *m*.

Example: 5 is an inverse of 3 modulo 7 since $5 \cdot 3 = 15 \equiv 1(\bmod 7)$.

One method of solving linear congruences makes use of an inverse $\bar{a}$, if it exists. Although we can not divide both sides of the congruence by *a*, we can multiply by $\bar{a}$ to solve for *x*.

Inverse of a modulo m

The following theorem guarantees that an inverse of a modulo m exists whenever a and m are relatively prime. Two integers a and b are relatively prime when $\gcd(a,b) = 1$.

Theorem 1: If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m. (This means that there is a unique positive integer $\bar{a}$ less than m that is an inverse of a modulo m and every other inverse of a modulo m is congruent to $\bar{a}$ modulo m.)

Proof: Since $\gcd(a,m) = 1$, by Theorem 6 of Section 4.3, there are integers s and t such that $sa + tm = 1$.

- Hence, $sa + tm \equiv 1 \pmod{m}$.
- Since $tm \equiv 0 \pmod{m}$, it follows that $sa \equiv 1 \pmod{m}$.
- Consequently, s is an inverse of a modulo m.
- The uniqueness of the inverse is Exercise 7.

Finding Inverses [1]

The Euclidean algorithm and Bézout coefficients gives us a systematic approaches to finding inverses.

Example: Find an inverse of 3 modulo 7.

Solution: Because gcd(3,7) = 1, by Theorem 1, an inverse of 3 modulo 7 exists.

- Using the Euclidian algorithm: $7 = 2 \cdot 3 + 1$.
- From this equation, we get $-2 \cdot 3 + 1 \cdot 7 = 1$, and see that −2 and 1 are Bézout coefficients of 3 and 7.
- Hence, −2 is an inverse of 3 modulo 7.
- Also every integer congruent to −2 modulo 7 is an inverse of 3 modulo 7, i.e., 5, −9, 12, etc.

Finding Inverses 2

Example: Find an inverse of 101 modulo 4620.

Solution: First use the Euclidian algorithm to show that gcd(101,4620) = 1.

$42620 = 45 \cdot 101 + 75$

$101 = 1 \cdot 75 + 26$

$75 = 2 \cdot 26 + 23$

$26 = 1 \cdot 23 + 3$

$23 = 7 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1$

Since the last nonzero remainder is 1, gcd(101,4260) = 1

Working Backwards:

$1 = 3 - 1 \cdot 2$

$1 = 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3$

$1 = -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23$

$1 = 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = 26 \cdot 26 - 9 \cdot 75$

$1 = 26 \cdot (101 - 1 \cdot 75) - 9 \cdot 75$

$= 26 \cdot 101 - 35.75$

$1 = 26 \cdot 101 - 35 \cdot (42620 - 45 \cdot 101)$

$= -35 \cdot 42620 + 1601 \cdot 101$

Bézout coefficients : − 35 and 1601

1601 is an inverse of 101 modulo 42620

Using Inverses to Solve Congruences

We can solve the congruence $ax \equiv b(\bmod m)$ by multiplying both sides by $\bar{a}$.

Example: What are the solutions of the congruence $3x \equiv 4(\bmod 7)$.

Solution: We found that −2 is an inverse of 3 modulo 7 (two slides back). We multiply both sides of the congruence by −2 giving

$$-2 \cdot 3x \equiv -2 \cdot 4(\bmod 7).$$

Because $-6 \equiv 1 \pmod 7$ and $-8 \equiv 6 \pmod 7$, it follows that if x is a solution, then $x \equiv -8 \equiv 6 \pmod 7$

We need to determine if every x with $x \equiv 6 \pmod 7$ is a solution. Assume that $x \equiv 6 \pmod 7$. By Theorem 5 of Section 4.1, it follows that $3x \equiv 3$.
$6 = 18 \equiv 4(\bmod 7)$ which shows that all such x satisfy the congruence.

The solutions are the integers x such that $x \equiv 6 \pmod 7$, namely, $6, 13, 20 \ldots$ and $-1, -8, -15, \ldots$