Backtracking, Modular Arithmetic, Multiplicative Inverse

Michael L. Littman

CS 22 2020

February 19, 2020

Overview

Pulvarizing

Corollary: An integer is a linear combination of a and b iff it is a multiple of $\gcd(a, b)$.

Proof:
Let $g = \gcd(a, b)$. We showed $g = sa + tb$ for some s and t. Any multiple of g is a linear combination of a and b:
$kg = k(sa + tb) = (ks)a + (kt)b$.

We know $a = k_1 g$ and $b = k_2 g$ because g is a common divisor of a and b. Any linear combination of a and b is a multiple of g:
$s'a + t'b = s'(k_1 g) + t'(k_2 g) = (s'k_1 + t'k_2)g$.

Mixing a and b in different combinations, we can only make multiples of g.

Note: The combinations are not unique: $sa + tb = (s - b)a + (t + a)b$.

How to make four

$(2, -1, 1) = \text{gcdcombo}(3, 5)$.

So, $2 \cdot 3 - 1 \cdot 5 = 1$.
To make 4: $8 \cdot 3 - 4 \cdot 5 = 4. = 3 \cdot 3 - 1 \cdot 5 = 4. = -2 \cdot 3 + 2 \cdot 5 = 4.$

Fill 2 cups of size 5, then empty out 2 cups of size 3.

Simple recipe

Actually, even simpler. Repeat until target reached:

1. Fill the smaller jug.
2. Pour all the water in the smaller jug into the larger jug. If, at any time, the larger jug becomes full, empty it out, and continue.

Eventually reaches all possible values. Bomb defused!

Fundamental Theorem of Arithmetic

Theorem: Every integer greater than 1 is a product of a unique non-increasing sequence of primes.

Lemma: If p is a prime and $p|ab$, then $p|a$ or $p|b$.

Proof: Left as proof-by-induction exercise.

Proof of Theorem: One case is if $\gcd(a, p) = p$. Then, the claim holds, because a is a multiple of p.

Otherwise, $\gcd(a, p) \neq p$. In this case, $\gcd(a, p)$ must be 1, since 1 and p are the only positive divisors of p. Since $\gcd(a, p)$ is a linear combination of a and p, we have $1 = sa + tp$ for some s, t. Then, $b = s(ab) + (tb)p$; that is, b is a linear combination of ab and p. Since p divides both ab and p, it also divides their linear combination, b. QED.

Proof of Fundamental Theorem of Arithmetic

Lemma: Let p be a prime. If $p|a_1 a_2 \cdots a_n$, then p divides some a_i.

Proof: We've seen that every positive integer can be expressed as a product of primes. We need to show this expression is unique. We proceed by contradiction: Assume there exists positive integers that can be written as products of primes in more than one way. Take the smallest such integer n and let $n = p_1 p_2 \cdots p_j = q_1 q_2 \cdots q_k$ be the two decompositions. Arrange them in non-increasing order and assume without loss of generality that $p_1 \leq q_1$. If $p_1 = q_1$, the remaining part of the product is smaller than n and different, which is a contradiction. Note that all the p_is are less than q_1. But, $q_1|n$ and $n = p_1 p_2 \cdots p_j$, so q_1 divides one of the p_is, which contradicts the fact that q_1 is bigger than all them. QED.

Congruence definition

Definition: a is *congruent to* b modulo n iff $\text{rem}(b, n) = \text{rem}(a, n)$. Equivalently, $n|(a - b)$.

We write $a \equiv b \pmod{n}$.

$29 \equiv 15 \pmod{7}$ because $7|(29 - 15)$, namely 14. Both have a remainder of 1 when divided by 7.

Equivalence relation—partitions the integers.

Transitivity, reflexivity, symmetry.

Basic modular algebra

In regular algebra,

$$\begin{aligned} a &= b \\ a + c &= b + c. \end{aligned}$$

Can we do the same is congruence-land?

$$\begin{aligned} a &\equiv b \pmod{n} \\ a + c &\equiv b + c \pmod{n}. \end{aligned}$$

Yes!

$a \equiv b \pmod{n}$ iff $n|(a - b)$ iff $\exists k, kn = a - b$ iff
$\exists k, kn = a - b + (c - c)$ iff $\exists k, kn = (a + c) - (b + c)$ iff
$n|((a + c) - (b + c))$ iff $a + c \equiv b + c \pmod{n}$.

Multiplication is repeated addition, so we can also multiply both sides by a constant. By transitivity, we can alway add or multiply each side by values that are congruent! "Clock arithmetic".

What about division?

If $a \equiv b \pmod{n}$, can we divide both sides by c?

$$\begin{aligned} 7 &\equiv 28 \pmod{3} \\ 1 &\equiv 4 \pmod{3} \quad \text{divide by } 7 \end{aligned}$$

So, maybe? At least if the answers are integers?

Is division even meaningful more generally?

Back to basics

Definition: The *multiplicative inverse* of a number x is a number x^{-1} such that: $x \cdot x^{-1} = 1$.

Division by x is really multiplication by x^{-1}.

Over the reals, what values have inverses? Everybody but zero.

Over the integers, what values have inverses? Only 1 and -1.

Over the integers mod n, what values have inverses?

Example, mod 10

	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

What specific values have inverses? 1, 3, 7, 9.

What specific values do not have inverses? 0, 2, 4, 5, 6, 8.

General rule? a has an inverse iff $\gcd(a, n) = 1$ or n.