Modular Arithmetic, Multiplicative Inverse

Robert Y. Lewis

CS 0220 2023

March 3, 2023

Overview

GCD Linear Combination Theorem

A refresher from the end of last class:

Theorem: The greatest common divisor of a and b is a linear combination of a and b. That is, $\gcd(a, b) = s \cdot a + t \cdot b$ for some integers s and t.

Computing the linear combination

We can use this theorem as an algorithm to find the linear combination of a and b that produces their GCD. Returns (s, t, g) where g is the GCD of the input.

def gcdcombo(a, b):
    if $a = 0$: return$(0, 1, b)$
    else:
        $(s, t, g) =$ gcdcombo(rem$(b, a), a)$
        return$(t - s \cdot$ qcnt$(b, a), s, g)$

- gcdcombo$(0, 15) = (0, 1, 15)$
- gcdcombo$(10, 15) = (-1, 1, 5)$
- gcdcombo$(24, 64) = (3, -1, 8)$

Computing By Hand

a	b	q	s	t	g
24	64				

```
def gcdcombo(a, b):
    if a = 0: return(0, 1, b)
    else:
        (s, t, g) = gcdcombo(rem(b, a), a)
        return(t − s · qcnt(b, a), s, g)
```

Do the rems going down, then the qcnts going up. Note that, at every level: $sa + tb = g$ (sanity check!).

Computing By Hand

a	b	q	s	t	g
24	64	2	3	-1	8
16	24	1	-1	1	8
8	16	2	1	0	8
0	8		0	1	8

Do the rems going down, then the qcnts going up. Note that, at every level: $sa + tb = g$ (sanity check!).

Pulvarizing

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

Proof (for reference):
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: $sa + tb = (s - b)a + (t + a)b$.

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 of Lemma: 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 $p|a_1a_2\cdots a_n$, then p divides some a_i.

Proof: Every positive integer can be expressed as a product of primes. (Proved by strong induction!) We need to show this expression is unique. We proceed by contradiction: Assume there exist positive integers that can be written as products of primes in more than one way. Take the smallest such integer n and let $n = p_1p_2\cdots p_j = q_1q_2\cdots q_k$ 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 (n was the smallest).
Note that all the p_is are less than q_1. But $q_1|n$ and $n = p_1p_2\cdots p_j$, 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 always add or multiply each side by values that are congruent!

"Clock arithmetic".

Example

$$
\begin{array}{lll}
2x + 17 & \equiv x + 31 \pmod{12} & \\
2x & \equiv x + 14 \pmod{12} & \text{add } -17 \text{ to both sides} \\
2x & \equiv x + 2 \pmod{12} & \text{add } 0 \text{ to left and } -12 \text{ to right} \\
x & \equiv 2 \pmod{12} & \text{add } -x \text{ to both sides}
\end{array}
$$

Double check. $4 + 17 = 21$ vs. 33. Difference is 12, check!

$$
\begin{array}{lll}
3x + 4 & \equiv 27 \pmod{11} & \\
3x & \equiv 23 \pmod{11} & \text{add } -4 \text{ to both sides}
\end{array}
$$

Kind of stuck because we don't (yet) have a "divide both sides by 3" rule.

So, what about division?

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

$$7 \equiv 28 \pmod{3}$$
$$1 \equiv 4 \pmod{3} \quad \text{divide by } 7$$

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 (mod n) iff $\gcd(a, n) = 1$.

Back to solving

$$\begin{aligned} 3x + 4 &\equiv 27 \pmod{11} \\ 3x &\equiv 23 \pmod{11} \quad \text{add } -4 \text{ to both sides} \end{aligned}$$

Want to multiply both sides by $3^{-1} = 4$, since $3 \times 4 \equiv 1 \pmod{11}$.

$$\begin{aligned} 3x &\equiv 23 \pmod{11} \\ 4 \times 3x &\equiv 4 \times 23 \pmod{11} \quad \text{multiply both sides by 4} \\ 12x &\equiv 92 \pmod{11} \quad \text{simplify} \\ x &\equiv 4 \pmod{11} \quad \text{congruence} \end{aligned}$$

Double check: 16 vs. 5, 11 divides the difference!