Modular Arithmetic, Multiplicative Inverse

Robert Y. Lewis

CS 0220 2022

March 4, 2022
Overview

1. Pulverizer (8.2.2)

2. Fundamental Theorem of Arithmetic (8.4)

3. Modular Arithmetic (8.5)

4. Arithmetic with a Prime Modulus (8.6)
   - Multiplicative Inverses (8.6.1)
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:
        $(s, t, g) = \text{gcdcombo}(\text{rem}(b, a), a)$
        return $(t - s \cdot \text{qcnt}(b, a), s, g)$

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

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>q</th>
<th>s</th>
<th>t</th>
<th>g</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>64</td>
<td>2</td>
<td>3</td>
<td>−1</td>
<td>8</td>
</tr>
<tr>
<td>16</td>
<td>24</td>
<td>1</td>
<td>−1</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>8</td>
<td>16</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>8</td>
</tr>
<tr>
<td>0</td>
<td>8</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>8</td>
</tr>
</tbody>
</table>

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

**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 \( a = k_1g \) and \( b = k_2g \) because \( g \) is a common divisor of \( a \) and \( b \). Any linear combination of \( a \) and \( b \) is a multiple of \( g \): \( s'a + t'b = s'(k_1g) + t'(k_2g) = (s'k_1 + t'k_2)g \).

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 $p \mid ab$, then $p \mid a$ or $p \mid b$.

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

Proof: Every positive integer can be expressed as a product of primes. (Challenge: strong induction!) 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 ($n$ was the smallest).

Note that all the $p_i$s 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 $p_i$s, 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,
\[ a = b \]
\[ a + c = b + c. \]

Can we do the same is congruence-land? \[ a \equiv b \pmod{n} \]
\[ a + c \equiv b + c \pmod{n}. \]

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

\[2x + 17 \equiv x + 31 \pmod{12}\]

\[2x \equiv x + 14 \pmod{12}\] add \(-17\) to both sides

\[2x \equiv x + 2 \pmod{12}\] add 0 to left and \(-12\) to right

\[x \equiv 2 \pmod{12}\] add \(-x\) to both sides

Double check. \(4 + 17 = 21\ vs.\ 33\). Difference is 12, check!

\[3x + 4 \equiv 27 \pmod{11}\]

\[3x \equiv 23 \pmod{11}\] add \(-4\) to both sides

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?
Multiplicative Inverses (8.6.1)

Example, mod 10

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>1</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>8</td>
<td>2</td>
<td>6</td>
<td>0</td>
<td>4</td>
<td>8</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>6</td>
<td>2</td>
<td>8</td>
<td>4</td>
<td>0</td>
<td>6</td>
<td>2</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>8</td>
<td>5</td>
<td>2</td>
<td>9</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>9</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

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

\[3x + 4 \equiv 27 \pmod{11}\]
\[3x \equiv 23 \pmod{11}\] add $-4$ to both sides

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

\[3x \equiv 23 \pmod{11}\]
\[4 \times 3x \equiv 4 \times 23 \pmod{11}\] multiply both sides by 4
\[12x \equiv 92 \pmod{11}\] simplify
\[x \equiv 4 \pmod{11}\] congruence

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