Multiplicative Inverse, Fermat’s little Theorem

Michael L. Littman

CS 22 2020

February 21, 2020
Overview

Arithmetic with a Prime Modulus (8.6)
Multiplicative Inverses (8.6.1)
Cancellation (8.6.2)
Fermat’s Little Theorem (8.6.3)
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

<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 iff \( \gcd(a, n) = 1 \) or \( n \).
Inverse mod prime

If this rule holds, all values (except zero!) have inverses mod a prime.

**Lemma:** If $p$ is prime and $k$ is not a multiple of $p$, then $k$ has a multiplicative inverse modulo $p$.

**Proof:** Since $p$ is prime and $k$ is not a multiple of $p$, $\gcd(p, k) = 1$. Therefore, there are $s$ and $t$ such that $1 = sp + tk$. So, mod $p$, that’s $1 = tk$, or $t = k^{-1}$ mod $p$. QED.

Example: What’s the multiplicative inverse of 3 (mod 11)?

$\gcd\text{combo}(3, 11) = (4, -1, 1)$

So? 4 works. Because $1 = 4 \times 3 - 1 \cdot 11$, so, mod 11, that’s $1 = 4 \times 3$. 
Back to dividing both sides

Earlier, we saw:

\[ 7 \equiv 28 \pmod{3} \]
\[ 1 \equiv 4 \pmod{3} \] divide by 7

 Doesn’t actually work, in general:

\[ 12 \equiv 6 \pmod{3} \]
\[ 4 \not\equiv 2 \pmod{3} \] divide by 3

Why? Because we’re really talking about multiplying both sides by \( 0^{-1} \), which doesn’t exist.

Apart from dividing by 0, we can cancel.
Cancellation proof

If we have

\[ ak \equiv bk \pmod{p} \]

and \( p \) is prime and \( k \not\equiv 0 \pmod{p} \), then \( k^{-1} \pmod{p} \) exists. Multiply both sides by \( k^{-1} \) and congruence is maintained.
Never need to multiply big numbers

When doing multiplication mod $n$, we can always mod $n$ the numbers first.

Example:

$7415 \times 2993 \mod 3$

$= 22193095 \mod 3$

$= 1$

OR:

$(7415 \mod 3) \times (2993 \mod 3) \mod 3$

$(2 \times 2) \mod 3$

$= 1$. 
Proof

\[ ab \mod n = (a \mod n)(b \mod n) \mod n. \]

\[
\begin{align*}
  a &= q_1 n + r_1 \\
  b &= q_2 n + r_2 \\
  ab &= (q_1 n + r_1)(q_2 n + r_2) \\
  ab &= (q_1 q_2 n + q_1 r_2 + q_2 r_1)n + r_1 r_2
\end{align*}
\]
Solving an old equation

In an early lecture, we wanted to know if there’s an $n$ such that $n^2 \equiv 8 \pmod{10}$.

We don’t quite have the ability to take square roots to solve this equation. But, we now know that if it’s not true of $n$ from 0 to 9, it’s not true for any $n$. Why? Because you can take mod before multiplying.

Note also: Connor Jordan proved that the sequence of quadratic residuals (mods of squares $n$) will always be a length $n$ palindrome!

$x^2 \equiv (n - x)^2 \pmod{n}$

iff $x^2 \equiv n^2 - 2nx + x^2 \pmod{n}$

iff $x^2 \equiv x^2 \pmod{n}$. 
Permuting

**Corollary**: Suppose $p$ is prime and $k$ is not a multiple of $p$. Then, the sequence of remainders on division by $p$ of the sequence:

$$1 \cdot k, 2 \cdot k, \ldots, (p - 1) \cdot k$$

is a permutation of the sequence:

$$1, 2, \ldots, (p - 1).$$

Example, $k = 3$, $p = 11$:

<table>
<thead>
<tr>
<th>$i$</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>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\times k$</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td>15</td>
<td>18</td>
<td>21</td>
<td>24</td>
<td>27</td>
<td>30</td>
</tr>
<tr>
<td>mod $p$</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>10</td>
<td>2</td>
<td>5</td>
<td>8</td>
</tr>
</tbody>
</table>
Permutation proof

**Proof:** The sequence of remainders contains \( p - 1 \) numbers. Since \( i \times k \) is not divisible by \( p \) (neither contains a factor of \( p \)) for \( i = 1, \ldots, p - 1 \), all these remainders are in \([1, p)\) by the definition of remainder. Furthermore, the remainders are all different. That’s because no two numbers in \([1, p)\) are congruent modulo \( p \). By the Cancellation property, \( i \cdot k \equiv j \cdot k \pmod{p} \) iff \( i \equiv j \pmod{p} \). Thus, the sequence of remainders must be a permutation of the numbers from 1 to \( p - 1 \). QED.

It’s a magic shuffle function. Useful for randomization and sending secret messages!
Fermat’s little theorem

**Theorem:** Suppose $p$ is prime and $k$ is not a multiple of $p$. Then:

$$k^{p-1} \equiv 1 \pmod{p}.$$ 

\[ (p - 1)! \]
\[ = 1 \cdot 2 \cdots (p - 1) \]
\[ = \text{rem}(k, p) \cdot \text{rem}(2k, p) \cdots \text{rem}((p - 1)k, p) \]
\[ \equiv k \cdot 2k \cdots (p - 1)k \pmod{p} \]
\[ \equiv (p - 1)! k^{p-1} \pmod{p} \]

Note that $(p - 1)!$ is not a multiple of $p$ because none of $1, 2, \ldots, (p - 1)$ contain a factor of $p$. So, by the Cancellation lemma, we can cancel $(p - 1)!$ from the top and bottom, proving the claim. QED
Inverses from Fermat’s little theorem

Since \( k^{p-1} \equiv 1 \pmod{p} \) and \( k^{p-1} = k \cdot k^{p-2} \), that tells us that \( k^{p-2} \) is the multiplicative inverse for \( k \).

We can compute \( k^{p-2} \pmod{p} \) efficiently using a technique called exponentiation by repeated squaring.

Running time is 2 log \( p \), just like “gcdcombo”.
Exponentiation by Repeated Squaring Idea

Can always compute $a^k$ by $k - 1$ multiplications of $a$.

If $k$ is even, can compute it with $k/2 - 1$ multiplications of $a$ to get $a^{k/2}$. Then, $a^k = (a^{k/2})^2$. So, one more multiplication and we’re there.

If $k$ is odd, similar trick to get $a^{(k-1)/2}$, then square, then multiply one more $a$.

Repeating this idea, the number of multiplications is on the order of $2 \log k$. 
Exponentiation by Repeated Squaring

```python
def repsq(a, k):
    if k == 0: return(1)
    if k % 2 == 0:
        sqroot = repsq(a, k/2)
        return(sqroot*sqroot)
    sqrootdiva = repsq(a, (k-1)/2)
    return(sqrootdiva*sqrootdiva*a)
```
Exponentiation by Repeated Squaring Mod Style

```python
def repsqmodn(a, k, n):
    if k == 0: return(1)
    if k % 2 == 0:
        sqroot = repsqmodn(a, k/2, n)
        return((sqroot*sqroot) % n)
    sqrootdiva = repsqmodn(a, (k-1)/2, n)
    return((sqrootdiva*sqrootdiva*a) % n)
```