Multiplicative Inverse, Fermat's little Theorem

Robert Y. Lewis

CS 0220 2024

March 6, 2024

Overview

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

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

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

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

Double check: plug in 4 or 15 to the original formula.

Inverse mod prime

General rule for existence of multiplicative inverses? a has an inverse mod n iff $\gcd(a, n) = 1$.
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 $1 \equiv tk$, or $t \equiv k^{-1}$ mod p. QED.

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

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

So? 4 works. Because $1 = 4 \times 3 - 1 \cdot 11$, so, mod 11, that's $1 \equiv 4 \times 3$.

Back to dividing both sides

Earlier, we saw:

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

Doesn't actually work, in general:

$$\begin{aligned} 12 &\equiv 6 \pmod{3} \\ 4 &\not\equiv 2 \pmod{3} \quad \text{divide by 3} \end{aligned}$$

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

Cancellation

Theorem.
If we have

$$ak \equiv bk \pmod{p}$$

and p is prime and $k \not\equiv 0 \pmod{p}$, then $a \equiv b \pmod{p}$.

Proof. $k^{-1} \bmod p$ exists. So, multiply both sides by k^{-1} and congruence is maintained.

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, $k = 3, p = 11$:

i	1	2	3	4	5	6	7	8	9	10
$\times k$	3	6	9	12	15	18	21	24	27	30
$\bmod p$	3	6	9	1	4	7	10	2	5	8

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.

Claim: if $i \cdot k \equiv j \cdot k \pmod{p}$, then $i = j$. (Cancel k; since $1 \leq i < p$, $i (\bmod p) = i$, same for j.)

So, $i-1$ distinct values between 1 and $i-1$: it's a permutation.

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:

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

$$
\begin{array}{lll}
 & (p-1)! & \\
 & = 1 \cdot 2 \cdot \dots \cdot (p-1) & \text{Defn. of factorial} \\
\textbf{Proof}: & = \mathrm{rem}(k,p) \cdot \mathrm{rem}(2k,p) \cdots \mathrm{rem}((p-1)k,p) & \text{Permutation lemma} \\
 & \equiv k \cdot 2k \cdots (p-1)k \pmod{p} & \text{Congruence of mult.} \\
 & \equiv (p-1)! k^{p-1} \pmod{p} & \text{algebra}
\end{array}
$$

Note that $(p-1)!$ is not a multiple of p because none of $1, 2, \dots, (p-1)$ 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

```
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)
```

(Note: we're using the infix notation % to mean "remainder," often read out loud as "mod.")

Never need to multiply big numbers

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

Example:
$7415 \times 2993 \,\%\, 3$
$= 22193095 \,\%\, 3$
$= 1$

OR:
$(7415 \,\%\, 3) \times (2993 \,\%\, 3) \,\%\, 3$
$(2 \,\%\, 2) \,\%\, 3$
$= 1.$

Proof

Theorem. $ab \% n = (a \% n)(b \% n) \% n$.

Proof.

$$
\begin{aligned}
a &= q_1 n + r_1 \\
b &= q_2 n + r_2 \\
ab &= (q_1 n + r_1)(q_2 n + r_2) \\
ab &= (q_1 q_2 n + q_1 r_2 + q_2 r_1) n + r_1 r_2
\end{aligned}
$$

So, cancelling out the multiple of n, $ab \% n = r_1 r_2 \% n$.

Exponentiation by Repeated Squaring Mod Style

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