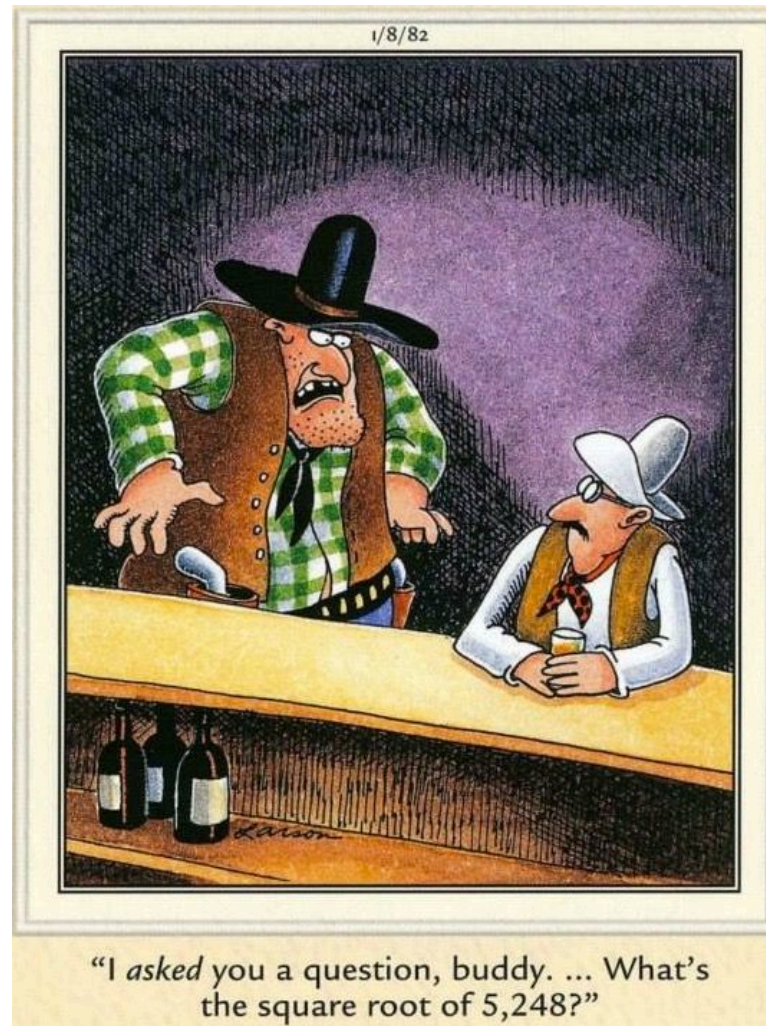


CSE 311: Foundations of Computing

Lecture 13: Modular Inverse, Exponentiation



Administrivia

HW5 will be released tomorrow (as usual)

but **MIGHT** be split two parts

- four problems + EC due by Friday (as usual)
- two problems due by Saturday (one day later)
 - of course, it is fine to finish those by Friday also
- giving more time since I may not finish lecturing on the material covered by those problems on Monday

Last time: Useful GCD Facts

If a and b are positive integers, then
$$\gcd(a, b) = \gcd(b, a \bmod b)$$

If a is a positive integer, $\gcd(a, 0) = a$.

Euclid's Algorithm

$$\text{gcd}(a, b) = \text{gcd}(b, a \bmod b)$$

$$\text{gcd}(a, 0) = a$$

```
int gcd(int a, int b){ /* Assumes: a >= b, b >= 0 */
    if (b == 0) {
        return a;
    } else {
        return gcd(b, a % b);
    }
}
```

Note: $\text{gcd}(b, a) = \text{gcd}(a, b)$

Euclid's Algorithm

Repeatedly use $\gcd(a, b) = \gcd(b, a \bmod b)$ to reduce numbers until you get $\gcd(g, 0) = g$.

$\gcd(660, 126) =$

Euclid's Algorithm

Repeatedly use $\gcd(a, b) = \gcd(b, a \bmod b)$ to reduce numbers until you get $\gcd(g, 0) = g$.

$$\begin{aligned}\gcd(660, 126) &= \gcd(126, 660 \bmod 126) = \gcd(126, 30) \\ &= \gcd(30, 126 \bmod 30) = \gcd(30, 6) \\ &= \gcd(6, 30 \bmod 6) = \gcd(6, 0) \\ &= 6\end{aligned}$$

Euclid's Algorithm

Repeatedly use $\gcd(a, b) = \gcd(b, a \bmod b)$ to reduce numbers until you get $\gcd(g, 0) = g$.

Equations with recursive calls:

$$\begin{aligned}\gcd(660, 126) &= \gcd(126, 660 \bmod 126) = \gcd(126, 30) \\ &= \gcd(30, 126 \bmod 30) = \gcd(30, 6) \\ &= \gcd(6, 30 \bmod 6) = \gcd(6, 0) \\ &= 6\end{aligned}$$

Tableau form:

$$\begin{aligned}660 &= 5 * 126 + 30 \\ 126 &= 4 * 30 + \textcircled{6} \\ 30 &= 5 * 6 + 0\end{aligned}$$

Famous Algorithmic Problems

- **Primality Testing**
 - Given an integer n , determine if n is prime
- **Factoring**
 - Given an integer n , find an integer d (with $1 < d < n$) that divides n
- **Greatest Common Divisor**
 - Given integers a and b , find the largest integer d that divides them both

Bézout's theorem

If a and b are positive integers, then there exist integers s and t such that

$$\gcd(a,b) = sa + tb.$$

Extended Euclidean algorithm

- Can use Euclid's Algorithm to find s, t such that

$$\gcd(a, b) = sa + tb$$

Extended Euclidean algorithm

- Can use Euclid's Algorithm to find s, t such that

$$\gcd(a, b) = sa + tb$$

Step 1 (Compute GCD & Keep Tableau Information):

$$\begin{array}{cc} a & b \\ \gcd(35, 27) & = \gcd(27, 35 \bmod 27) & = \gcd(27, 8) \end{array}$$

$$\begin{array}{l} a = q * b + r \\ 35 = 1 * 27 + 8 \end{array}$$

Extended Euclidean algorithm

- Can use Euclid's Algorithm to find s, t such that

$$\gcd(a, b) = sa + tb$$

Step 1 (Compute GCD & Keep Tableau Information):

a	b	b	$a \bmod b = r$	b	r
$\gcd(35, 27)$	$= \gcd(27, 35 \bmod 27)$	$= \gcd(27, 8)$			
	$= \gcd(8, 27 \bmod 8)$	$= \gcd(8, 3)$			
	$= \gcd(3, 8 \bmod 3)$	$= \gcd(3, 2)$			
	$= \gcd(2, 3 \bmod 2)$	$= \gcd(2, 1)$			
	$= \gcd(1, 2 \bmod 1)$	$= \gcd(1, 0)$			

a	$=$	q	$*$	b	$+$	r
35	=	1	*	27	+	8
27	=	3	*	8	+	3
8	=	2	*	3	+	2
3	=	1	*	2	+	1

Extended Euclidean algorithm

- Can use Euclid's Algorithm to find s, t such that

$$\gcd(a, b) = sa + tb$$

Step 2 (Solve the equations for r):

$$a = q * b + r$$

$$35 = 1 * 27 + 8$$

$$27 = 3 * 8 + 3$$

$$8 = 2 * 3 + 2$$

$$3 = 1 * 2 + 1$$

$$r = a - q * b$$

$$8 = 35 - 1 * 27$$

Extended Euclidean algorithm

- Can use Euclid's Algorithm to find s, t such that

$$\gcd(a, b) = sa + tb$$

Step 2 (Solve the equations for r):

$$a = q * b + r$$

$$35 = 1 * 27 + 8$$

$$27 = 3 * 8 + 3$$

$$8 = 2 * 3 + 2$$

$$3 = 1 * 2 + \textcircled{1}$$

$$r = a - q * b$$

$$8 = 35 - 1 * 27$$

$$3 = 27 - 3 * 8$$

$$2 = 8 - 2 * 3$$

$$1 = 3 - 1 * 2$$

Extended Euclidean algorithm

- Can use Euclid's Algorithm to find s, t such that

$$\gcd(a, b) = sa + tb$$

Step 3 (Backward Substitute Equations):

$$8 = 35 - 1 * 27$$

$$3 = 27 - 3 * 8$$

$$2 = 8 - 2 * 3$$

$$1 = 3 - 1 * 2$$

$$\begin{aligned} 1 &= 3 - 1 * (8 - 2 * 3) \\ &= 3 - 8 + 2 * 3 \\ &= (-1) * 8 + 3 * 3 \end{aligned}$$

Plug in the def of 2

Re-arrange into
3's and 8's

Extended Euclidean algorithm

- Can use Euclid's Algorithm to find s, t such that

$$\gcd(a, b) = sa + tb$$

Step 3 (Backward Substitute Equations):

$$8 = 35 - 1 * 27$$

$$3 = 27 - 3 * 8$$

$$2 = 8 - 2 * 3$$

$$1 = 3 - 1 * 2$$

$$1 = 3 - 1 * (8 - 2 * 3)$$

$$= 3 - 8 + 2 * 3$$

$$= (-1) * 8 + 3 * 3$$

$$= (-1) * 8 + 3 * (27 - 3 * 8)$$

$$= (-1) * 8 + 3 * 27 + (-9) * 8$$

$$= 3 * 27 + (-10) * 8$$

Plug in the def of 2

Re-arrange into
3's and 8's

Plug in the def of 3

Re-arrange into
8's and 27's

Extended Euclidean algorithm

- Can use Euclid's Algorithm to find s, t such that

$$\gcd(a, b) = sa + tb$$

Step 3 (Backward Substitute Equations):

$$8 = 35 - 1 * 27$$

$$3 = 27 - 3 * 8$$

$$2 = 8 - 2 * 3$$

$$1 = 3 - 1 * 2$$

Re-arrange into
27's and 35's

$$1 = 3 - 1 * (8 - 2 * 3)$$

$$= 3 - 8 + 2 * 3$$

$$= (-1) * 8 + 3 * 3$$

$$= (-1) * 8 + 3 * (27 - 3 * 8)$$

$$= (-1) * 8 + 3 * 27 + (-9) * 8$$

$$= 3 * 27 + (-10) * 8$$

$$= 3 * 27 + (-10) * (35 - 1 * 27)$$

$$= 3 * 27 + (-10) * 35 + 10 * 27$$

$$= 13 * 27 + (-10) * 35$$

Plug in the def of 2

Re-arrange into
3's and 8's

Plug in the def of 3

Re-arrange into
8's and 27's

Multiplicative inverse mod m

Let $0 \leq a, b < m$. Then, b is the *multiplicative inverse of a (modulo m)* iff $ab \equiv 1 \pmod{m}$.

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

mod 7

x	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

mod 10

Multiplicative inverse mod m

Suppose $\gcd(a, m) = 1$

By Bézout's Theorem, there exist integers s and t such that $sa + tm = 1$.

s is the multiplicative inverse of a (modulo m):

$$1 = sa + tm \equiv sa \pmod{m}$$

So... we can compute multiplicative inverses with the extended Euclidean algorithm

These inverses let us solve modular equations...

Example

Solve: $7x \equiv 1 \pmod{26}$

Example

Solve: $7x \equiv 1 \pmod{26}$

$$\gcd(26, 7) = \gcd(7, 5) = \gcd(5, 2) = \gcd(2, 1) = 1$$

Example

Solve: $7x \equiv 1 \pmod{26}$

$$\gcd(26, 7) = \gcd(7, 5) = \gcd(5, 2) = \gcd(2, 1) = 1$$

$$26 = 3 * 7 + 5$$

$$7 = 1 * 5 + 2$$

$$5 = 2 * 2 + 1$$

Example

Solve: $7x \equiv 1 \pmod{26}$

$$\gcd(26, 7) = \gcd(7, 5) = \gcd(5, 2) = \gcd(2, 1) = 1$$

$$26 = 3 * 7 + 5 \qquad 5 = 26 - 3 * 7$$

$$7 = 1 * 5 + 2 \qquad 2 = 7 - 1 * 5$$

$$5 = 2 * 2 + 1 \qquad 1 = 5 - 2 * 2$$

Example

Solve: $7x \equiv 1 \pmod{26}$

$$\gcd(26, 7) = \gcd(7, 5) = \gcd(5, 2) = \gcd(2, 1) = 1$$

$$26 = 3 * 7 + 5 \qquad 5 = 26 - 3 * 7$$

$$7 = 1 * 5 + 2 \qquad 2 = 7 - 1 * 5$$

$$5 = 2 * 2 + 1 \qquad 1 = 5 - 2 * 2$$

$$\begin{aligned} 1 &= 5 - 2 * (7 - 1 * 5) \\ &= (-2) * 7 + 3 * 5 \\ &= (-2) * 7 + 3 * (26 - 3 * 7) \\ &= (-11) * 7 + 3 * 26 \end{aligned}$$

Example

Solve: $7x \equiv 1 \pmod{26}$

$$\gcd(26, 7) = \gcd(7, 5) = \gcd(5, 2) = \gcd(2, 1) = 1$$

$$26 = 3 * 7 + 5 \qquad 5 = 26 - 3 * 7$$

$$7 = 1 * 5 + 2 \qquad 2 = 7 - 1 * 5$$

$$5 = 2 * 2 + 1 \qquad 1 = 5 - 2 * 2$$

$$1 = 5 - 2 * (7 - 1 * 5)$$

$$= (-2) * 7 + 3 * 5$$

$$= (-2) * 7 + 3 * (26 - 3 * 7)$$

$$= (-11) * 7 + 3 * 26$$

Multiplicative inverse of 7 mod 26

Now $(-11) \pmod{26} = 15$. So, $x = 15 + 26k$ for $k \in \mathbb{Z}$.

Example of a more general equation

Now solve: $7y \equiv 3 \pmod{26}$

We already computed that 15 is the multiplicative inverse of 7 modulo 26. That is, $7 \cdot 15 \equiv 1 \pmod{26}$

If y is a solution, then multiplying by 15 we have

$$15 \cdot 7 \cdot y \equiv 15 \cdot 3 \pmod{26}$$

Multiplying the second congruence by y gives

$$y \equiv 15 \cdot 7 \cdot y \pmod{26}$$

So together we have $y \equiv 15 \cdot 3 \equiv 19 \pmod{26}$.

This shows that every solution is congruent to 19.

Example of a more general equation

Now solve: $7y \equiv 3 \pmod{26}$

We already computed that 15 is the multiplicative inverse of 7 modulo 26. That is, $7 \cdot 15 \equiv 1 \pmod{26}$

By the multiplicative property of mod we have

$$7 \cdot 15 \cdot 3 \equiv 3 \pmod{26}$$

So $y = 15 \cdot 3$ and, more generally, any $y \equiv 19 \pmod{26}$, is a solution.

Thus, the set of numbers of the form $y = 19 + 26k$, for any k , are exactly solutions of this equation.

Math mod a prime is especially nice

$\gcd(a, m) = 1$ if m is prime and $0 < a < m$ so
can always solve these equations mod a prime.

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

mod 7