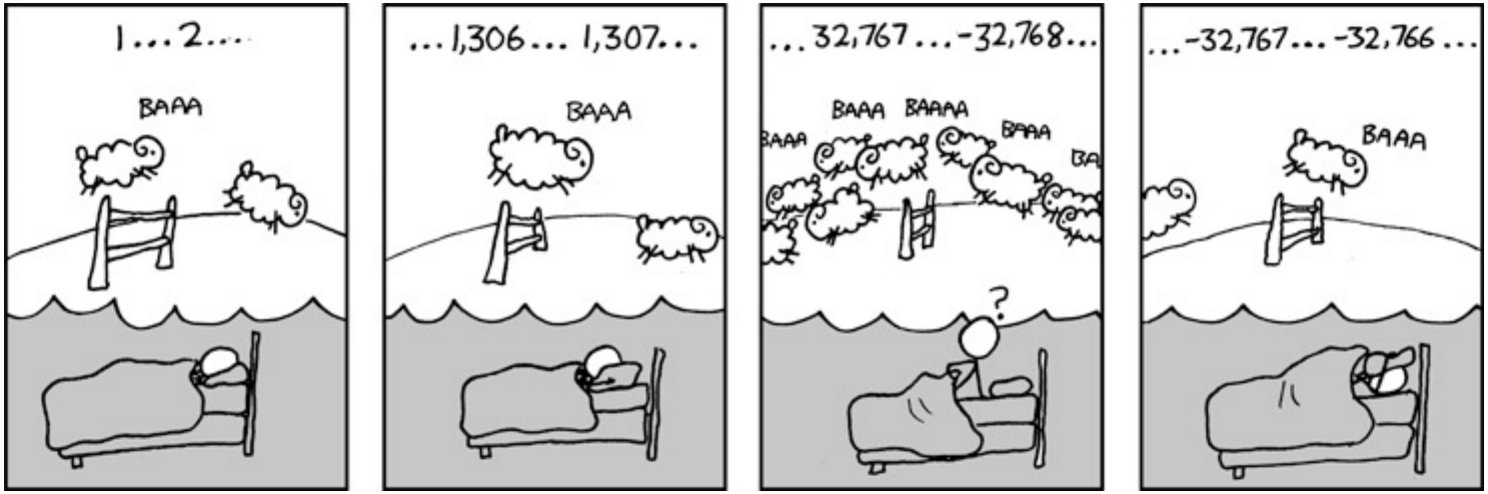
CSE 311: Foundations of Computing

Lecture 14: More number theory & modular arithmetic



Recap from last lecture

Definition: "a divides b"

For $a \in \mathbb{Z}, b \in \mathbb{Z}$ with $a \neq 0$:

$$a \mid b \leftrightarrow \exists k \in \mathbb{Z} \ (b = ka)$$

Definition: "a is congruent to b modulo m"

For $a, b, m \in \mathbb{Z}$ with $m > 0$

$$a \equiv b \ (\text{mod}\ m) \leftrightarrow m \mid (a - b)$$

- **Example:** $-1 \equiv 9 \ (mod\ 5)$

Recap from last lecture

Definition: "a divides b"

For $a \in \mathbb{Z}, b \in \mathbb{Z}$ with $a \neq 0$:

$$a \mid b \leftrightarrow \exists k \in \mathbb{Z}\ (b = ka)$$

Definition: "a is congruent to b modulo m"

For $a, b, m \in \mathbb{Z}$ with $m > 0$

$$a \equiv b \pmod{m} \leftrightarrow m \mid (a - b)$$

- **Example:** $-1 \equiv 9\ (mod\ 5)$
- **Division Theorem. Any integer a, d with $d \geq 1$, can write uniquely $a = (a\ div\ d) \cdot d + (a\ \%\ d)$ where $0 \leq a\ \%\ d < d$.**
- **Example:** $-1\ \%\ 5 = 4,\ \ 9\ \%\ 4 = 1$

Recap from last lecture

Definition: "a divides b"

For $a \in \mathbb{Z}, b \in \mathbb{Z}$ with $a \neq 0$:
$a \mid b \leftrightarrow \exists k \in \mathbb{Z}\ (b = ka)$

Definition: "a is congruent to b modulo m"

For $a, b, m \in \mathbb{Z}$ with $m > 0$
$a \equiv b \pmod{m} \leftrightarrow m \mid (a - b)$

- **Example:** $-1 \equiv 9\ (mod\ 5)$
- **Division Theorem. Any integer** a, d **with** $d \geq 1$**, can write uniquely** $a = (a\ div\ d) \cdot d + (a\ \%\ d)$ **where** $0 \leq a\ \%\ d < d$**.**
- **Example:** $-1\ \%\ 5 = 4,\ \ 9\ \%\ 4 = 1$

Facts:

- $a \equiv b \pmod{m}$ **iff** $a\ \%\ m = b\ \%\ m$
- $(a \equiv b \pmod{m}) \land (b \equiv c \pmod{m}) \rightarrow a \equiv c \pmod{m}$
- $(a \equiv b \pmod{m}) \land (c \equiv d \pmod{m}) \rightarrow a + c \equiv b + d\ (mod\ m)$
- $(a \equiv b \pmod{m}) \land (c \equiv d \pmod{m}) \rightarrow ac \equiv bd \pmod{m}$

Example

Let $\boldsymbol{n}$ be an integer.
Prove that $\boldsymbol{n^2 \equiv 0 \pmod{4}}$ or $\boldsymbol{n^2 \equiv 1 \pmod{4}}$

Let's start by looking a small example:

$0^2 = 0 \equiv 0 \pmod{4}$
$1^2 = 1 \equiv 1 \pmod{4}$
$2^2 = 4 \equiv 0 \pmod{4}$
$3^2 = 9 \equiv 1 \pmod{4}$
$4^2 = 16 \equiv 0 \pmod{4}$

Example

Let $\boldsymbol{n}$ be an integer.
Prove that $\boldsymbol{n^2 \equiv 0 \pmod 4}$ or $\boldsymbol{n^2 \equiv 1 \pmod 4}$

Case 1 (n is even):

Let's start by looking a small example:

$0^2 = 0 \equiv 0 \pmod 4$
$1^2 = 1 \equiv 1 \pmod 4$
$2^2 = 4 \equiv 0 \pmod 4$
$3^2 = 9 \equiv 1 \pmod 4$
$4^2 = 16 \equiv 0 \pmod 4$

It looks like

$n \equiv 0 \pmod 2 \rightarrow n^2 \equiv 0 \pmod 4$, and
$n \equiv 1 \pmod 2 \rightarrow n^2 \equiv 1 \pmod 4$.

Example

Let $\boldsymbol{n}$ be an integer.
Prove that $\boldsymbol{n^2 \equiv 0 \pmod 4}$ or $\boldsymbol{n^2 \equiv 1 \pmod 4}$

Case 1 (n is even):

Suppose n is even.
Then, $n = 2k$ for some integer k.
So, $n^2 = (2k)^2 = 4k^2$.
So, by definition of congruence,
we have $n^2 \equiv 0 \pmod 4$.

Let's start by looking a small example:

$0^2 = 0 \equiv 0 \pmod 4$
$1^2 = 1 \equiv 1 \pmod 4$
$2^2 = 4 \equiv 0 \pmod 4$
$3^2 = 9 \equiv 1 \pmod 4$
$4^2 = 16 \equiv 0 \pmod 4$

It looks like

$n \equiv 0 \pmod 2 \rightarrow n^2 \equiv 0 \pmod 4$, and
$n \equiv 1 \pmod 2 \rightarrow n^2 \equiv 1 \pmod 4$.

Example

Let $\boldsymbol{n}$ be an integer.
Prove that $\boldsymbol{n^2 \equiv 0 \pmod 4}$ or $\boldsymbol{n^2 \equiv 1 \pmod 4}$

Case 1 (n is even): Done.

Case 2 (n is odd):

Let's start by looking a a small example:

$0^2 = 0 \equiv 0 \pmod 4$
$1^2 = 1 \equiv 1 \pmod 4$
$2^2 = 4 \equiv 0 \pmod 4$
$3^2 = 9 \equiv 1 \pmod 4$
$4^2 = 16 \equiv 0 \pmod 4$

It looks like

$n \equiv 0 \pmod 2 \rightarrow n^2 \equiv 0 \pmod 4$, and
$n \equiv 1 \pmod 2 \rightarrow n^2 \equiv 1 \pmod 4$.

Example

Let $\boldsymbol{n}$ be an integer.
Prove that $\boldsymbol{n^2 \equiv 0 \ (\mathrm{mod}\ 4)}$ or $\boldsymbol{n^2 \equiv 1 \ (\mathrm{mod}\ 4)}$

Let's start by looking a a small example:

$0^2 = 0 \equiv 0 \ (\mathrm{mod}\ 4)$
$1^2 = 1 \equiv 1 \ (\mathrm{mod}\ 4)$
$2^2 = 4 \equiv 0 \ (\mathrm{mod}\ 4)$
$3^2 = 9 \equiv 1 \ (\mathrm{mod}\ 4)$
$4^2 = 16 \equiv 0 \ (\mathrm{mod}\ 4)$

It looks like

$n \equiv 0 \ (\mathrm{mod}\ 2) \longrightarrow n^2 \equiv 0 \ (\mathrm{mod}\ 4)$, and
$n \equiv 1 \ (\mathrm{mod}\ 2) \longrightarrow n^2 \equiv 1 \ (\mathrm{mod}\ 4)$.

Case 1 (n is even): Done.

Case 2 (n is odd):

Suppose n is odd.
Then, $n = 2k + 1$ for some integer k.
So, $n^2 = (2k+1)^2$
$= 4k^2 + 4k + 1$
$= 4(k^2 + k) + 1$.
So, by the earlier property of mod,
we have $n^2 \equiv 1 \ (\mathrm{mod}\ 4)$.

Result follows by "proof by cases": n is either even or not even (odd)

n-bit Unsigned Integer Representation

- Represent integer x as sum of powers of 2:

  If $\sum_{i=0}^{n-1} b_i 2^i$ where each $b_i \in \{0,1\}$

  then representation is $b_{n-1} \ldots b_2 \, b_1 \, b_0$

99 = 64 + 32 + 2 + 1

18 = 16 + 2

- For n = 8:

  99: 0110 0011

  18: 0001 0010

Sign-Magnitude Integer Representation

n-bit signed integers

Suppose that $-2^{n-1} < x < 2^{n-1}$

First bit as the sign, $n-1$ bits for the value

99 = 64 + 32 + 2 + 1

18 = 16 + 2

For n = 8:

99: 0110 0011

-18: 1001 0010

Any problems with this representation?

Two's Complement Representation

n bit signed integers, first bit will still be the sign bit

Suppose that $0 \le x < 2^{n-1}$,
x is represented by the binary representation of x
Suppose that $0 \le x \le 2^{n-1}$,
$-x$ is represented by the binary representation of $2^n - x$

Key property: Twos complement representation of any number $\boldsymbol{y}$ is equivalent to $\boldsymbol{y}$, $\mathbf{mod}\ \mathbf{2^n}$ so arithmetic works $\mathbf{mod}\ \mathbf{2^n}$

99 = 64 + 32 + 2 + 1
18 = 16 + 2

For n = 8:
99: 0110 0011
-18: 1110 1110

Sign-Magnitude vs. Two's Complement

-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7
1111	1110	1101	1100	1011	1010	1001	0000	0001	0010	0011	0100	0101	0110	0111

Sign-bit

-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7
1000	1001	1010	1011	1100	1101	1110	1111	0000	0001	0010	0011	0100	0101	0110	0111

Two's complement

Two's Complement Representation

- For $0 < x \leq 2^{n-1}$, $-x$ is represented by the binary representation of $2^n - x$
  - That is, the two's complement representation of any number y has the same value as y modulo 2^n.

- To compute this: Flip the bits of x then add 1:
  - All 1's string is $2^n - 1$, so

    Flip the bits of x $\equiv$ replace x by $2^n - 1 - x$

    Then add 1 to get $2^n - x$

Basic Applications of mod

- Hashing
- Pseudo random number generation
- Simple cipher

Hashing

Scenario:

Map a small number of data values from a large domain $\{0, 1, \dots, M - 1\}$ …

…into a small set of locations $\{0,1, \dots, n - 1\}$ so one can quickly check if some value is present

- $\text{hash}(x) = x \,\%\, p$ for p a prime close to n
  - or $\text{hash}(x) = (ax + b)\% \,p$
- Depends on all of the bits of the data
  - helps avoid collisions due to similar values
  - need to manage them if they occur

Pseudo-Random Number Generation

Linear Congruential method

$$x_{n+1} = (ax_n + c)\ \%\ m$$

Choose random x_0, a, c, m and produce a long sequence of x_n's

Simple Ciphers

- **Caesar cipher**, A = 1, B = 2, . . .
  - HELLO WORLD
- **Shift cipher**
  - $f(p) = (p + k) \% 26$
  - $f^{-1}(p) = (p - k) \% 26$
- **More general**
  - $f(p) = (ap + b) \% 26$

Primality

An integer *p* greater than 1 is called *prime* if the only positive factors of *p* are 1 and *p*.

A positive integer that is greater than 1 and is not prime is called *composite*.

Fundamental Theorem of Arithmetic

Every positive integer greater than 1 has a unique prime factorization

$48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3$

$591 = 3 \cdot 197$

$45{,}523 = 45{,}523$

$321{,}950 = 2 \cdot 5 \cdot 5 \cdot 47 \cdot 137$

$1{,}234{,}567{,}890 = 2 \cdot 3 \cdot 3 \cdot 5 \cdot 3{,}607 \cdot 3{,}803$

Lecture 14 Activity

- You will be assigned to **breakout rooms**. Please:
- Introduce yourself
- Choose someone to share screen, showing this PDF
- Complete the following proof:

(Euclid's Theorem): There are an infinite number of primes.

Proof: Suppose for the sake of contradiction that there are only a finite number of primes and call the full list $p_1, p_2, \ldots, p_n$.

Define the number $P = p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_n$ and let $Q = P + 1$. (Note that $Q > 1$.)

- Case 1: Q is prime: ......
- Case 2: Q is composite: ......

Both cases are contradictions, so the assumption is false.

Fill out a poll everywhere for **Activity Credit**!
Go to pollev.com/thomas311 and login
with your UW identity

Famous Algorithmic Problems

- Primality Testing
  - Given an integer n, determine if n is prime
- Factoring
  - Given an integer n, determine the prime factorization of n

Factoring

Factor the following 232 digit number [RSA768]:

1230186684530117755130494958384962720772
853569595334792197322452151726400507263
657518745202199786469389956474942774063
845925192557326303453731548268507917026
122142913461670429214311602221240479274
737794080665351419597459856902143413

1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469389956474942774063845925192557326303453731548268507917026122142913461670429214311602221240479274737794080665351419597459856902143413

=

3347807169895689878604416984821269081770479498371376856891243138898288379387800228761471165253174308773781446799948 9

×

3674604366679959042824463379962795263227915816434308764267603228381573966651127923337341714339681027009279873630891 7

Greatest Common Divisor

GCD(a, b):

Largest integer d such that $d \mid a$ and $d \mid b$

- GCD(100, 125) =
- GCD(17, 49) =
- GCD(11, 66) =
- GCD(13, 0) =
- GCD(180, 252) =

GCD and Factoring

$a = 2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 = 46{,}200$

$b = 2 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 13 = 204{,}750$

$$\mathrm{GCD}(a, b) = 2^{\min(3,1)} \cdot 3^{\min(1,2)} \cdot 5^{\min(2,3)} \cdot 7^{\min(1,1)} \cdot 11^{\min(1,0)} \cdot 13^{\min(0,1)}$$

Factoring is expensive!

Can we compute GCD(a,b) without factoring?

Useful GCD Fact

If a and b are positive integers, then

$$\gcd(a,b) = \gcd(b,\ a \ \% \ b)$$

Useful GCD Fact

If *a* and *b* are positive integers, then
gcd(*a*,*b*) = gcd(*b*, *a* % *b*)

Proof:

By definition of %, $a = qb + (a \% b)$ for some integer $q = a \text{ div } b$.

Let $d = \gcd(a, b)$. Then $d|a$ and $d|b$ so $a = kd$ and $b = jd$ for some integers k and j.

Therefore $(a \% b) = a - qb = kd - qjd = (k - qj)d$.
So, $d|(a \% b)$ and since $d|b$ we must have $d \leq \gcd(b, a \% b)$.

Useful GCD Fact

If *a* and *b* are positive integers, then
gcd(*a*,*b*) = gcd(*b*, *a* % *b*)

Proof:

By definition of %, $a = qb + (a \% b)$ for some integer $q = a \text{ div } b$.

Let $d = \gcd(a, b)$. Then $d|a$ and $d|b$ so $a = kd$ and $b = jd$ for some integers k and j.

Therefore $(a \% b) = a - qb = kd - qjd = (k - qj)d$.
So, $d|(a \% b)$ and since $d|b$ we must have $d \leq \gcd(b, a \% b)$.

Now, let $e = \gcd(b, a \% b)$. Then $e|b$ and $e|(a \% b)$ so $b = me$ and $(a \% b) = ne$ for some integers m and n.

Therefore $a = qb + (a \% b) = qme + ne = (qm + n)e$.
So, $e|a$ and since $e|b$ we must have $e \leq \gcd(a, b)$.

It follows that $\gcd(a, b) = \gcd(b, a \% b)$. ∎

Another simple GCD fact

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

Euclid's Algorithm

gcd(a, b) = gcd(b, a mod b), gcd(a,0)=a

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

Example: GCD(660, 126)

Euclid's Algorithm

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

gcd(660,126) =

Euclid’s Algorithm

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

gcd(660,126) = gcd(126, 660 % 126) = gcd(126, 30)
= gcd(30, 126 % 30) = gcd(30, 6)
= gcd(6, 30 % 6) = gcd(6, 0)
= 6

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) = gcd(126, 660 % 126) = gcd(126, 30)
= gcd(30, 126 % 30) = gcd(30, 6)
= gcd(6, 30 % 6) = gcd(6, 0)
= 6

In tableau form:

660 = 5 * 126 + 30
126 = 4 * 30 + 6
30 = 5 * 6 + 0

Bézout's theorem

If a and b are positive integers, then there exist integers $\boldsymbol{s}$ and $\boldsymbol{t}$ such that

$$\gcd(a,b) = \boldsymbol{s}a + \boldsymbol{t}b.$$

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):

a b b a mod b = r b r

$$\gcd(35, 27) = \gcd(27, 35 \bmod 27) = \gcd(27, 8)$$

a = q * b + r

$$35 = 1 * 27 + 8$$

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 mod 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

$35 = 1 * 27 + 8$

$27 = 3 * 8 \quad + 3$

$8 \quad = 2 * 3 \quad + 2$

$3 \quad = 1 * 2 \quad + 1$

$2 \quad = 2 * 1 \quad + 0$

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

$35 = 1 * 27 + 8$

$27 = 3 * 8 + 3$

$8 = 2 * 3 + 2$

$3 = 1 * 2 + 1$

$2 = 2 * 1 + 0$

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):

$8 = 35 - 1 * 27$

$3 = 27 - 3 * 8$

$2 = 8 - 2 * 3$

$1 = 3 - 1 * 2$

Plug in the def of 2

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

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):

$8 = 35 - 1 * 27$

$3 = 27 - 3 * 8$

$2 = 8 - 2 * 3$

$1 = 3 - 1 * 2$

Plug in the def of 2

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

Re-arrange into 3's and 8's

Plug in the def of 3

$$= (-1) * 8 + 3 * (27 - 3 * 8)$$
$$= (-1) * 8 + 3 * 27 + (-9) * 8$$
$$= 3 * 27 + (-10) * 8$$

Re-arrange into 8's and 27's

$$= 3 * 27 + (-10) * (35 - 1 * 27)$$
$$= 3 * 27 + (-10) * 35 + 10 * 27$$
$$= 13 * 27 + (-10) * 35$$

Re-arrange into 27's and 35's

Multiplicative inverse $\bmod m$

Suppose $\mathrm{GCD}(a, m) = 1$

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

$s \,\%\, m$ is the multiplicative inverse of a:

$$1 = (sa + tm) \,\%\, m = sa \,\%\, m$$

Example

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

Example

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

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

$$26 = 7 * 3 + 5 \qquad 5 = 26 - 7 * 3$$
$$7 = 5 * 1 + 2 \qquad 2 = 7 - 5 * 1$$
$$5 = 2 * 2 + 1 \qquad 1 = 5 - 2 * 2$$

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

Multiplicative inverse of 7 mod 26

Now $(-11) \bmod 26 = 15$. **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, $7 \cdot 15 \equiv 1 \pmod{26}$

By the multiplicative property of mod we have

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

So any $y \equiv 15 \cdot 3 \pmod{26}$ is a solution.

That is, $y = 19 + 26k$ for any integer k is a solution.

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