Applications

Alexander S. Kulikov

Steklov Mathematical Institute at St. Petersburg, Russian Academy of Sciences
and
University of California, San Diego

Outline

Least Common Multiple

Diophantine Equations: Examples

Diophantine Equations: Theorem

Modular Division

Least Common Multiple

Definition

The least common multiple, $\operatorname{lcm}(a, b)$, of integers a and b (both different from zero) is the smallest positive integer that is divisible by both a and b

Least Common Multiple

Definition

The least common multiple, $\operatorname{lcm}(a, b)$, of integers a and b (both different from zero) is the smallest positive integer that is divisible by both a and b

Examples

$\operatorname{lcm}(24, 16) = 48$, $\operatorname{lcm}(9, 17) = 153$, $\operatorname{lcm}(239, 0)$ — undefined

Least Common Multiple

Definition

The least common multiple, $\mathrm{lcm}(a, b)$, of integers a and b (both different from zero) is the smallest positive integer that is divisible by both a and b

Examples

$\mathrm{lcm}(24, 16) = 48$, $\mathrm{lcm}(9, 17) = 153$,
$\mathrm{lcm}(239, 0)$ — undefined

Convention

We assume that a and b are positive

Working with Fractions

When adding or comparing simple fractions, we usually compute the lowest common denominator which is the least common multiple of the denominators:

Working with Fractions

When adding or comparing simple fractions, we usually compute the lowest common denominator which is the least common multiple of the denominators:

$$\frac{31}{177} + \frac{29}{118}$$

Working with Fractions

When adding or comparing simple fractions, we usually compute the lowest common denominator which is the least common multiple of the denominators:

$$\frac{31}{177} + \frac{29}{118}$$

$$\operatorname{lcm}(177, 118) = 354$$

Working with Fractions

When adding or comparing simple fractions, we usually compute the lowest common denominator which is the least common multiple of the denominators:

$$\frac{31}{177} + \frac{29}{118}$$

$$\text{lcm}(177, 118) = 354 = 2 \cdot 177 = 3 \cdot 118$$

Working with Fractions

When adding or comparing simple fractions, we usually compute the lowest common denominator which is the least common multiple of the denominators:

$$\frac{31}{177} + \frac{29}{118}$$

$$\text{lcm}(177, 118) = 354 = 2 \cdot 177 = 3 \cdot 118$$

$$\frac{31}{177} + \frac{29}{118}$$

Working with Fractions

When adding or comparing simple fractions, we usually compute the lowest common denominator which is the least common multiple of the denominators:

$$\frac{31}{177} + \frac{29}{118}$$

$$\mathrm{lcm}(177, 118) = 354 = 2 \cdot 177 = 3 \cdot 118$$

$$\frac{31}{177} + \frac{29}{118} = \frac{31 \cdot 2}{177 \cdot 2} + \frac{29 \cdot 3}{118 \cdot 3}$$

Working with Fractions

When adding or comparing simple fractions, we usually compute the lowest common denominator which is the least common multiple of the denominators:

$$\frac{31}{177} + \frac{29}{118}$$

$$\mathrm{lcm}(177, 118) = 354 = 2 \cdot 177 = 3 \cdot 118$$

$$\frac{31}{177} + \frac{29}{118} = \frac{31 \cdot 2}{177 \cdot 2} + \frac{29 \cdot 3}{118 \cdot 3} = \frac{149}{354}$$

Naive Algorithm

Clearly, $a \cdot b$ is divisible by a and b. To find the *least* common multiple, simply try all numbers up to $a \cdot b$ and select the smallest one

Naive Algorithm: Code

```
def lcm(a, b):
  assert a > 0 and b > 0

  for d in range(1, a * b + 1):
    if d % a == 0 and d % b == 0:
      return d
```

Naive Algorithm: Code

```
def lcm(a, b):
  assert a > 0 and b > 0

  for d in range(1, a * b + 1):
    if d % a == 0 and d % b == 0:
      return d
```

```
print(lcm(24, 16))
```

```
48
```

Naive Algorithm: Analysis

- If $\text{lcm}(a, b) = a \cdot b$, the algorithm will perform $a \cdot b$ divisions

Naive Algorithm: Analysis

- If $\text{lcm}(a, b) = a \cdot b$, the algorithm will perform $a \cdot b$ divisions
- Again, very slow: the call

```
print(lcm(531441, 262144))
```

will take more than one minute

Euclid's algorithm

Can we use efficient Euclid's algorithm to compute the least common multiple, too?

Euclid's algorithm

Can we use efficient Euclid's algorithm to compute the least common multiple, too?

Yes!

$$\mathrm{lcm}(a, b) \cdot \gcd(a, b) = a \cdot b$$

lcm and gcd

Lemma

If $a, b > 0$, then $\mathrm{lcm}(a, b) = ab/\gcd(a, b)$

lcm and gcd

Lemma

If $a, b > 0$, then $\operatorname{lcm}(a, b) = ab/\gcd(a, b)$

Proof

- Let $d = \gcd(a, b)$, $a = dp$, $b = dq$

$\square$

lcm and gcd

Lemma

If $a, b > 0$, then $\mathrm{lcm}(a, b) = ab/\mathrm{gcd}(a, b)$

Proof

- Let $d = \mathrm{gcd}(a, b)$, $a = dp$, $b = dq$
- Then $m = ab/d = pb = qa$ is a multiple of a and b

$\square$

lcm and gcd

Lemma

If $a, b > 0$, then $\mathrm{lcm}(a, b) = ab/\gcd(a, b)$

Proof

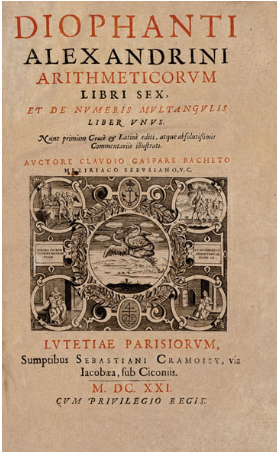
- Let $d = \gcd(a, b)$, $a = dp$, $b = dq$
- Then $m = ab/d = pb = qa$ is a multiple of a and b
- If there was a smaller multiple $\overline{m} < m$, then $\bar{d} = ab/\overline{m} > d$ would be a common divisor: $a/\bar{d} = \overline{m}/b$, $b/\bar{d} = \overline{m}/a$

$\square$

Outline

Diophantine Equations

A Diophantine equation is an equation where only integer solutions are allowed


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque abſolutiſſimis
Commentariis illuſtrati.
AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, V.C.
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via
Iacobæa, ſub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

Diophantine Equations: Examples

- 1 apple costs 22 pesos

Diophantine Equations: Examples

- 1 apple costs 22 pesos
- You only have 3-peso bills

Diophantine Equations: Examples

- 1 apple costs 22 pesos
- You only have 3-peso bills
- The cashier only has 5-peso bills

Diophantine Equations: Examples

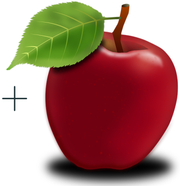
- 1 apple costs 22 pesos
- You only have 3-peso bills
- The cashier only has 5-peso bills
- $3x = 22 + 5y$, x, y are non-negative integers

Diophantine Equations: Examples

- 1 apple costs 22 pesos
- You only have 3-peso bills
- The cashier only has 5-peso bills
- $3x = 22 + 5y$, x, y are non-negative integers

$\times 9 \quad =$

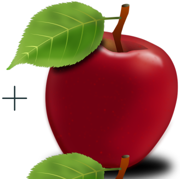
$\times 1 +$



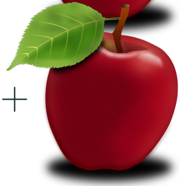
Diophantine Equations: Examples

- 1 apple costs 22 pesos
- You only have 3-peso bills
- The cashier only has 5-peso bills
- $3x = 22 + 5y$, x, y are non-negative integers

$\times 9 =$


$\times 1 +$


$\times 14 =$


$\times 4 +$


Diophantine Equations: Examples

RECEIPT

[redacted] Lamps

Each	$49.36
Total	$[redacted]7.28

Diophantine Equations: Examples

RECEIPT	
[redacted] Lamps	
Each	\$49.36
Total	[redacted]7.28

- x lamps, each 4936 ¢

Diophantine Equations: Examples

RECEIPT

[illegible] Lamps

Each	\$49.36
Total	\$[illegible]7.28

- x lamps, each 4936 ¢
- $100 \le y < 1000$

Diophantine Equations: Examples

RECEIPT

[illegible] Lamps

Each	\$49.36
Total	\$[illegible]7.28

- x lamps, each 4936 ¢
- $100 \leq y < 1000$
- Total: $1000y + 728$ ¢

Diophantine Equations: Examples

RECEIPT

[illegible] Lamps

Each	$49.36
Total	$[illegible]7.28

- x lamps, each 4936 ¢
- $100 \leq y < 1000$
- Total: $1000y + 728$ ¢
- $4936x = 1000y + 728$, x, y are non-negative integers, $100 \leq y < 1000$

Diophantine Equations: Examples

RECEIPT	
98 Lamps	
Each	\$49.36
Total	\$4837.28

- x lamps, each 4936 ¢
- $100 \leq y < 1000$
- Total: $1000y + 728$ ¢
- $4936x = 1000y + 728$, x, y are non-negative integers, $100 \leq y < 1000$

Diophantine Equations: Examples

- $187x + 55y = 121$, x and y are integers

Diophantine Equations: Examples

- $187x + 55y = 121$, x and y are integers
    - $187 \cdot 3 + 55 \cdot (-8) = 121$

Diophantine Equations: Examples

- $187x + 55y = 121$, x and y are integers
  - $187 \cdot 3 + 55 \cdot (-8) = 121$
  - $187 \cdot (-2) + 55 \cdot 9 = 121$

Diophantine Equations: Examples

- $187x + 55y = 121$, x and y are integers
  - $187 \cdot 3 + 55 \cdot (-8) = 121$
  - $187 \cdot (-2) + 55 \cdot 9 = 121$
  - Infinitely many solutions!

Diophantine Equations: Examples

- $187x + 55y = 121$, x and y are integers
  - $187 \cdot 3 + 55 \cdot (-8) = 121$
  - $187 \cdot (-2) + 55 \cdot 9 = 121$
  - Infinitely many solutions!
- $187x + 55y = 45$, x and y are integers

Diophantine Equations: Examples

- $187x + 55y = 121$, x and y are integers
    - $187 \cdot 3 + 55 \cdot (-8) = 121$
    - $187 \cdot (-2) + 55 \cdot 9 = 121$
    - Infinitely many solutions!
- $187x + 55y = 45$, x and y are integers
    - No solutions!

Diophantine Equations: Examples

- $187x + 55y = 121$, x and y are integers
  - $187 \cdot 3 + 55 \cdot (-8) = 121$
  - $187 \cdot (-2) + 55 \cdot 9 = 121$
  - Infinitely many solutions!
- $187x + 55y = 45$, x and y are integers
  - No solutions!

When does a Diophantine equation have solutions?

Outline

Solutions of Diophantine Equations

Theorem

Given integers a, b, c (at least one of a and $b \neq 0$), the Diophantine equation

$$ax + by = c$$

has a solution (where x and y are integers) if and only if

$$\gcd(a, b) \mid c\,.$$

Proof of Theorem

Proof

Let $d = \gcd(a, b)$

Proof of Theorem

Proof

$$
\begin{aligned}
& \text{Let } d = \gcd(a, b) \\
\Rightarrow\ & a = dp \text{ and } b = dq \text{, thus,} \\
& c = ax + by = d(px + qy)
\end{aligned}
$$

Proof of Theorem

Proof

$$
\begin{aligned}
& \text{Let } d = \gcd(a, b) \\
\Rightarrow\ & a = dp \text{ and } b = dq\text{, thus,} \\
& c = ax + by = d(px + qy) \\
\Leftarrow\ & \text{Extended Euclid's algorithm:} \\
& a\bar{x} + b\bar{y} = d
\end{aligned}
$$

Proof of Theorem

Proof

Let $d = \gcd(a, b)$

$\Rightarrow$ $a = dp$ and $b = dq$, thus,

$c = ax + by = d(px + qy)$

$\Leftarrow$ Extended Euclid's algorithm:

$a\bar{x} + b\bar{y} = d$

If $c = td$, then $x = t \cdot \bar{x}, y = t \cdot \bar{y}$:

$ax + by = t(a\bar{x} + b\bar{y}) = td = c$ $\square$

Finding a Solution

- $10x + 6y = 14$

Finding a Solution

- $10x + 6y = 14$
  - Extended Euclid's algorithm: $\gcd(10, 6) = 2 = 10 \cdot (-1) + 6 \cdot 2$

Finding a Solution

- $10x + 6y = 14$
  - Extended Euclid's algorithm: $\gcd(10, 6) = 2 = 10 \cdot (-1) + 6 \cdot 2$
  - $14 = 10 \cdot (-1) \cdot 7 + 6 \cdot 2 \cdot 7$

Finding a Solution

- $10x + 6y = 14$
  - Extended Euclid's algorithm: $\gcd(10, 6) = 2 = 10 \cdot (-1) + 6 \cdot 2$
  - $14 = 10 \cdot (-1) \cdot 7 + 6 \cdot 2 \cdot 7$
  - $x = -7, y = 14$

Finding a Solution

- $10x + 6y = 14$
  - Extended Euclid's algorithm: $\gcd(10, 6) = 2 = 10 \cdot (-1) + 6 \cdot 2$
  - $14 = 10 \cdot (-1) \cdot 7 + 6 \cdot 2 \cdot 7$
  - $x = -7, y = 14$
- $391x + 299y = -69$

Finding a Solution

- $10x + 6y = 14$
    - Extended Euclid's algorithm: $\gcd(10, 6) = 2 = 10 \cdot (-1) + 6 \cdot 2$
    - $14 = 10 \cdot (-1) \cdot 7 + 6 \cdot 2 \cdot 7$
    - $x = -7, y = 14$
- $391x + 299y = -69$
    - Extended Euclid's Algorithm: $\gcd(391, 299) = 23 = 391 \cdot (-3) + 299 \cdot 4$

Finding a Solution

- $10x + 6y = 14$
  - Extended Euclid's algorithm: $\gcd(10, 6) = 2 = 10 \cdot (-1) + 6 \cdot 2$
  - $14 = 10 \cdot (-1) \cdot 7 + 6 \cdot 2 \cdot 7$
  - $x = -7, y = 14$
- $391x + 299y = -69$
  - Extended Euclid's Algorithm: $\gcd(391, 299) = 23 = 391 \cdot (-3) + 299 \cdot 4$
  - $-69 = 391 \cdot (-3) \cdot (-3) + 299 \cdot 4 \cdot (-3)$

Finding a Solution

- $10x + 6y = 14$
  - Extended Euclid's algorithm: $\gcd(10, 6) = 2 = 10 \cdot (-1) + 6 \cdot 2$
  - $14 = 10 \cdot (-1) \cdot 7 + 6 \cdot 2 \cdot 7$
  - $x = -7, y = 14$
- $391x + 299y = -69$
  - Extended Euclid's Algorithm: $\gcd(391, 299) = 23 = 391 \cdot (-3) + 299 \cdot 4$
  - $-69 = 391 \cdot (-3) \cdot (-3) + 299 \cdot 4 \cdot (-3)$
  - $x = 9, y = -12$

Finding a Solution

- $10x + 6y = 14$
  - Extended Euclid's algorithm: $\gcd(10, 6) = 2 = 10 \cdot (-1) + 6 \cdot 2$
  - $14 = 10 \cdot (-1) \cdot 7 + 6 \cdot 2 \cdot 7$
  - $x = -7, y = 14$
- $391x + 299y = -69$
  - Extended Euclid's Algorithm: $\gcd(391, 299) = 23 = 391 \cdot (-3) + 299 \cdot 4$
  - $-69 = 391 \cdot (-3) \cdot (-3) + 299 \cdot 4 \cdot (-3)$
  - $x = 9, y = -12$
  - But $x = -4, y = 5$ is also a solution. How do we find all solutions?

Euclid’s Lemma

Euclid’s Lemma

If $n \mid ab$ and $\gcd(a, n) = 1$, then $n \mid b$.

Euclid's Lemma

Euclid's Lemma

If $n \mid ab$ and $\gcd(a, n) = 1$, then $n \mid b$.

Proof

- From Extended Euclid's algorithm (a, n):

Euclid's Lemma

Euclid's Lemma

If $n \mid ab$ and $\gcd(a, n) = 1$, then $n \mid b$.

Proof

- From Extended Euclid's algorithm (a, n):
- $ax + ny = 1$

Euclid's Lemma

Euclid's Lemma

If $n \mid ab$ and $\gcd(a, n) = 1$, then $n \mid b$.

Proof

- From Extended Euclid's algorithm (a, n):
- $ax + ny = 1$
- $axb + nyb = b$

Euclid's Lemma

Euclid's Lemma

If $n \mid ab$ and $\gcd(a, n) = 1$, then $n \mid b$.

Proof

- From Extended Euclid's algorithm (a, n):
- $ax + ny = 1$
- $axb + nyb = b$
- From $ab = kn$,
  $b = axb + nyb = n(xk + yb)$ $\square$

Finding All Solution

Theorem

Let $\gcd(a, b) = d$, $a = dp$, $b = dq$. If (x_0, y_0) is a solution of the Diophantine equation $ax + by = c$:

$$ax_0 + by_0 = c\,,$$

then all the solutions have the form

$$a(x_0 + tq) + b(y_0 - tp) = c\,,$$

where t is an arbitrary integer.

Proof of Theorem

Proof

- $a = dp, b = dq, ax_0 + by_0 = c$

Proof of Theorem

Proof

- $a = dp, b = dq, ax_0 + by_0 = c$
- For any integer t,

$$\begin{aligned} &a(x_0 + tq) + b(y_0 - tp) \\ &= ax_0 + by_0 + t(aq - bp) \\ &= c + t(dpq - dpq) = c \end{aligned}$$

is a solution

Proof of Theorem

Proof (continued)

- Consider 2 solutions: (x_1, y_1) and (x_2, y_2)

Proof of Theorem

Proof (continued)

- Consider 2 solutions: (x_1, y_1) and (x_2, y_2)
- $a(x_1 - x_2) + b(y_1 - y_2) = c - c = 0$

Proof of Theorem

Proof (continued)

- Consider 2 solutions: (x_1, y_1) and (x_2, y_2)
- $a(x_1 - x_2) + b(y_1 - y_2) = c - c = 0$
- $p(x_1 - x_2) + q(y_1 - y_2) = 0$

Proof of Theorem

Proof (continued)

- Consider 2 solutions: (x_1, y_1) and (x_2, y_2)
- $a(x_1 - x_2) + b(y_1 - y_2) = c - c = 0$
- $p(x_1 - x_2) + q(y_1 - y_2) = 0$
- $\gcd(p, q) = 1$

Proof of Theorem

Proof (continued)

- Consider 2 solutions: (x_1, y_1) and (x_2, y_2)
- $a(x_1 - x_2) + b(y_1 - y_2) = c - c = 0$
- $p(x_1 - x_2) + q(y_1 - y_2) = 0$
- $\gcd(p, q) = 1$
- By Euclid's lemma: $x_1 - x_2 = tq$

Proof of Theorem

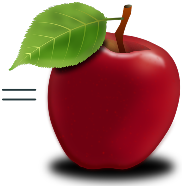
Proof (continued)

- Consider 2 solutions: (x_1, y_1) and (x_2, y_2)
- $a(x_1 - x_2) + b(y_1 - y_2) = c - c = 0$
- $p(x_1 - x_2) + q(y_1 - y_2) = 0$
- $\gcd(p, q) = 1$
- By Euclid's lemma: $x_1 - x_2 = tq$
- Then $y_1 - y_2 = -tp$ $\square$

Example

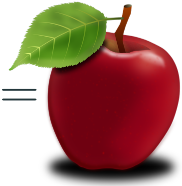
$\times 9 +$

$\times 1 =$



Example

$\times 9 +$

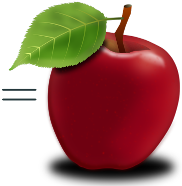

$\times 1 =$


- $3x + 5y = 22$

Example

$\times 9 +$

$\times 1 =$

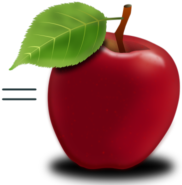


- $3x + 5y = 22$
- $x_0 = 9, y_0 = -1$

Example

$\times 9 +$

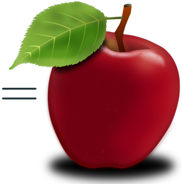
$\times 1 =$



- $3x + 5y = 22$
- $x_0 = 9, y_0 = -1$
- $a = 3, b = 5, d = 1$

Example

$\times 9 +$

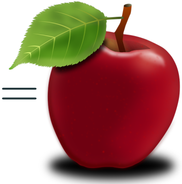

$\times 1 =$


- $3x + 5y = 22$
- $x_0 = 9, y_0 = -1$
- $a = 3, b = 5, d = 1$
- $a = dp, b = dq, p = 3, q = 5$

Example

$\times 9 +$

$\times 1 =$



- $3x + 5y = 22$
- $x_0 = 9, y_0 = -1$
- $a = 3, b = 5, d = 1$
- $a = dp, b = dq, p = 3, q = 5$
- All solutions:

$$x = x_0 + tq = 9 + 5t$$

$$y = y_0 - tp = -1 - 3t$$

Example

- All solutions:

$$\begin{aligned} x &= x_0 + tq = 9 + 5t \\ y &= y_0 - tp = -1 - 3t \end{aligned}$$

Example

- All solutions:

$$x = x_0 + tq = 9 + 5t$$
$$y = y_0 - tp = -1 - 3t$$

- If we want $x \geq 0$ and $y \leq 0$, then take

$$9 + 5t \geq 0$$
$$-1 - 3t \leq 0$$

Example

- All solutions:

$$x = x_0 + tq = 9 + 5t$$
$$y = y_0 - tp = -1 - 3t$$

- If we want $x \geq 0$ and $y \leq 0$, then take

$$9 + 5t \geq 0$$
$$-1 - 3t \leq 0$$

- That is, $t \geq -1/3$, or $t \geq 0$

Outline

Least Common Multiple

Diophantine Equations: Examples

Diophantine Equations: Theorem

Modular Division

Division mod 7

$\times$	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

Division mod 7

$\times$	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

- Given $a \neq 0$ and b, there exists x such that $a \times x \equiv b \pmod 7$

Division mod 7

$\times$	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

- Given $a \neq 0$ and b, there exists x such that $a \times x \equiv b \pmod 7$
- x plays the role of modular division $x = b/a \pmod 7$

Division mod 6

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Division mod 6

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

- $2/5 \equiv 4 \pmod 6$.
  Indeed, $4 \times 5 \equiv 2 \pmod 6$

Division mod 6

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

- $2/5 \equiv 4 \pmod 6$.
  Indeed, $4 \times 5 \equiv 2 \pmod 6$
- But there is no x s.t. $3 \times x \equiv 1 \pmod 6$

Division mod 6

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

- $2/5 \equiv 4 \pmod{6}$.
  Indeed, $4 \times 5 \equiv 2 \pmod{6}$
- But there is no x s.t. $3 \times x \equiv 1 \pmod{6}$
- We can't divide 1 by 3 modulo 6!

Multiplicative Inverse

- A multiplicative inverse of a mod n is $\bar{a}$ s.t.

$$a \times \bar{a} \equiv 1 \pmod{n}$$

Multiplicative Inverse

- A multiplicative inverse of a mod n is $\bar{a}$ s.t.

$$a \times \bar{a} \equiv 1 \pmod{n}$$

- If a has a multiplicative inverse $\bar{a}$, then one can divide by a:

$$b/a \equiv b \times \bar{a} \pmod{n}$$

Multiplicative Inverse

- A multiplicative inverse of a mod n is $\bar{a}$ s.t.

$$a \times \bar{a} \equiv 1 \pmod{n}$$

- If a has a multiplicative inverse $\bar{a}$, then one can divide by a:

$$b/a \equiv b \times \bar{a} \pmod{n}$$

- Indeed, for every b,

$$b/a \times a \equiv b \times \bar{a} \times a \equiv b \pmod{n}$$

Uniqueness of Inverses

Lemma

If a has a multiplicative inverse, then it is unique

Uniqueness of Inverses

Lemma

If a has a multiplicative inverse, then it is unique

Proof

If x and y are multiplicative inverses of a, then

$$x = x \times (a \times y) = (x \times a) \times y = y$$

$\square$

Existence of Inverses

Theorem

a has a multiplicative inverse modulo n if and only if $\gcd(a, n) = 1$

Existence of Inverses

Theorem

a has a multiplicative inverse modulo n if and only if $\gcd(a, n) = 1$

Proof

- $ax \equiv 1 \pmod{n}$ iff $ax + kn = 1$

Existence of Inverses

Theorem

a has a multiplicative inverse modulo n if and only if $\gcd(a, n) = 1$

Proof

- $ax \equiv 1 \pmod{n}$ iff $ax + kn = 1$
- For fixed a and n, this Diophantine equation has a solution (x) iff $\gcd(a, n) \mid 1$ $\square$

Modular Division

- If $\gcd(a, n) = 1$ then one can divide by a modulo n

Modular Division

- If $\gcd(a, n) = 1$ then one can divide by a modulo n
- Given a, b, n, we want to find $x \equiv b/a \pmod{n}$:

Modular Division

- If $\gcd(a, n) = 1$ then one can divide by a modulo n
- Given a, b, n, we want to find $x \equiv b/a \pmod{n}$:
    - First, use Extended Euclid's algorithm to find s and $t: nt + as = 1$

Modular Division

- If $\gcd(a, n) = 1$ then one can divide by a modulo n
- Given a, b, n, we want to find $x \equiv b/a \pmod{n}$:
    - First, use Extended Euclid's algorithm to find s and t : $nt + as = 1$
    - s is the multiplicative inverse of a modulo n

Modular Division

- If $\gcd(a, n) = 1$ then one can divide by a modulo n
- Given a, b, n, we want to find $x \equiv b/a \pmod{n}$:
  - First, use Extended Euclid's algorithm to find s and t: $nt + as = 1$
  - s is the multiplicative inverse of a modulo n
  - Now $x \equiv b/a \equiv b \times s \pmod{n}$

Example

- $\gcd(9, 2) = 1$, so we can compute

$$7/2 \pmod 9$$

Example

- $\gcd(9, 2) = 1$, so we can compute

$$7/2 \pmod 9$$

- Extended Euclid's algorithm gives us

$$9 \times 1 + 2 \times (-4) = 1$$

Example

- $\gcd(9, 2) = 1$, so we can compute

$$7/2 \pmod 9$$

- Extended Euclid's algorithm gives us

$$9 \times 1 + 2 \times (-4) = 1$$

- $-4 \equiv 5 \pmod 9$ is the inverse of 2 mod 9

Example

- $\gcd(9, 2) = 1$, so we can compute

$$7/2 \pmod 9$$

- Extended Euclid's algorithm gives us

$$9 \times 1 + 2 \times (-4) = 1$$

- $-4 \equiv 5 \pmod 9$ is the inverse of 2 mod 9
- $7/2 \equiv 7 \times 5 \equiv 8 \pmod 9$

Example

- $\gcd(9, 2) = 1$, so we can compute

$$7/2 \pmod 9$$

- Extended Euclid's algorithm gives us

$$9 \times 1 + 2 \times (-4) = 1$$

- $-4 \equiv 5 \pmod 9$ is the inverse of 2 mod 9
- $7/2 \equiv 7 \times 5 \equiv 8 \pmod 9$
- Indeed, $8 \times 2 \equiv 7 \pmod 9$