CSc 466/566

Computer Security

16 : Number Theory — Modular Arithmetic

Version: 2019/10/28 13:14:29

Department of Computer Science
University of Arizona

collberg@gmail.com

Christian Collberg

Outline

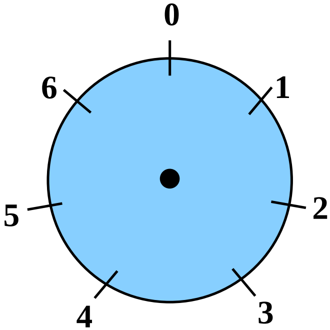
Modular Arithmetic

- Public-key ciphers operate on large numbers (1000s of bits).
- We can't deal with overflow: the output has to fit in the same size block as the input.
- We therefore perform arithmetic modulo n.
- After each arithmetic operation return the remainder after dividing by n.
- We're performing arithmetic in Z_n:

$$Z_n = \{0, 1, 2, \ldots, n-1\}$$

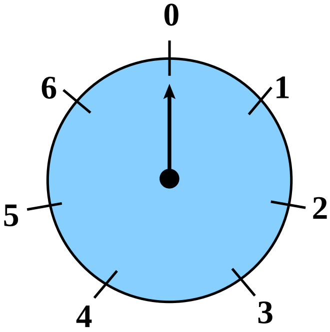
Clock Arithmetic

- We sometimes call arithmetic in Z_n clock arithmetic.
- Just like when a clock wrapps around when we pass 12, arithmetic in Z_n wrapps around when we reach n:



Clock Arithmetic. . .

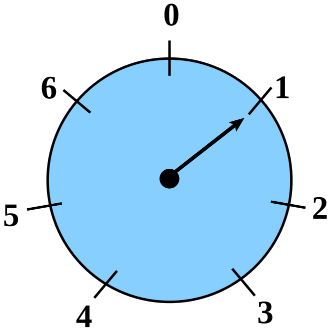
- Here we increment, starting at 0, but all arithmetic is done mod 7:



0 mod 7

Clock Arithmetic...

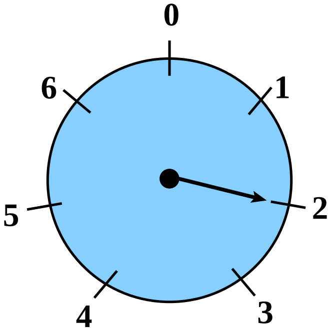
- Here we increment, starting at 0, but all arithmetic is done mod 7:



1 mod 7

Clock Arithmetic. . .

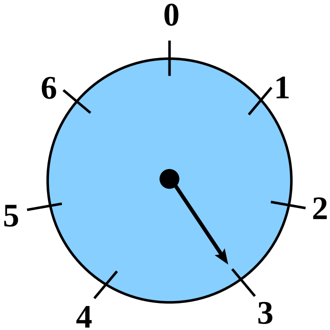
- Here we increment, starting at 0, but all arithmetic is done mod 7:



2 mod 7

Clock Arithmetic. . .

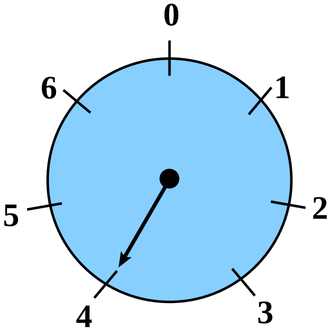
- Here we increment, starting at 0, but all arithmetic is done mod 7:



3 mod 7

Clock Arithmetic. . .

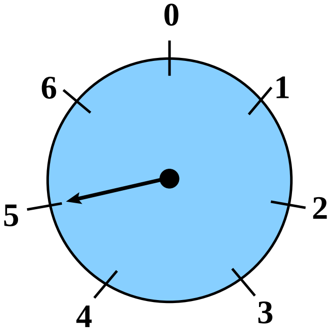
- Here we increment, starting at 0, but all arithmetic is done mod 7:



4 mod 7

Clock Arithmetic...

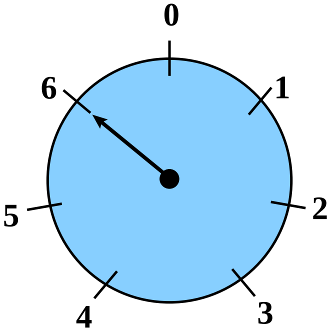
- Here we increment, starting at 0, but all arithmetic is done mod 7:



5 mod 7

Clock Arithmetic...

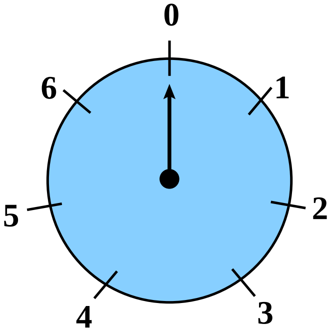
- Here we increment, starting at 0, but all arithmetic is done mod 7:



6 mod 7

Clock Arithmetic. . .

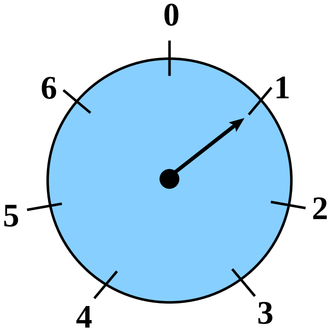
- Here we increment, starting at 0, but all arithmetic is done mod 7:



7 mod 7

Clock Arithmetic. . .

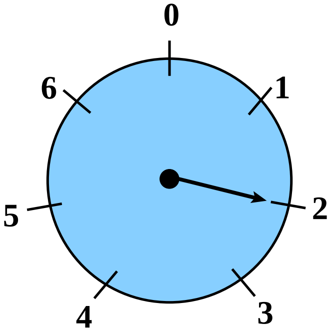
- Here we increment, starting at 0, but all arithmetic is done mod 7:



8 mod 7

Clock Arithmetic...

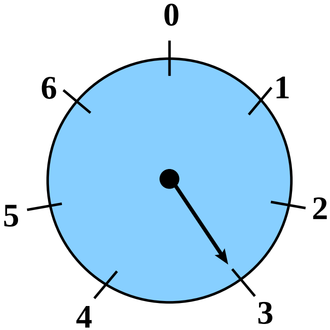
- Here we increment, starting at 0, but all arithmetic is done mod 7:



9 mod 7

Clock Arithmetic. . .

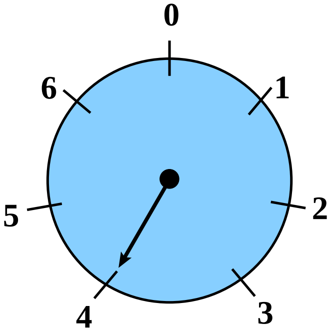
- Here we increment, starting at 0, but all arithmetic is done mod 7:



10 mod 7

Clock Arithmetic. . .

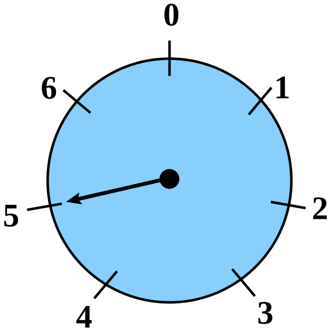
- Here we increment, starting at 0, but all arithmetic is done mod 7:



11 mod 7

Clock Arithmetic. . .

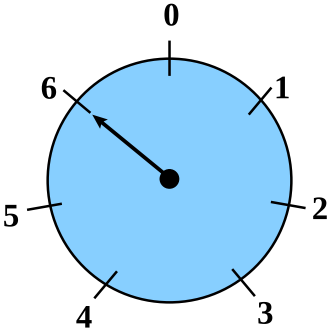
- Here we increment, starting at 0, but all arithmetic is done mod 7:



12 mod 7

Clock Arithmetic. . .

- Here we increment, starting at 0, but all arithmetic is done mod 7:



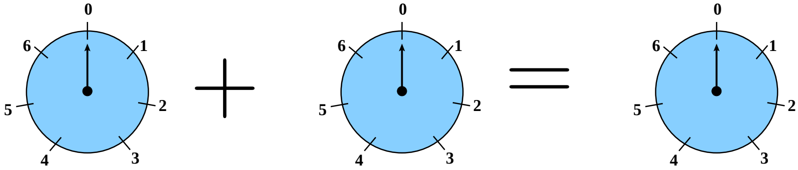
13 mod 7

Modular Addition

- Addition is done by reducing the result to values in Z_n:

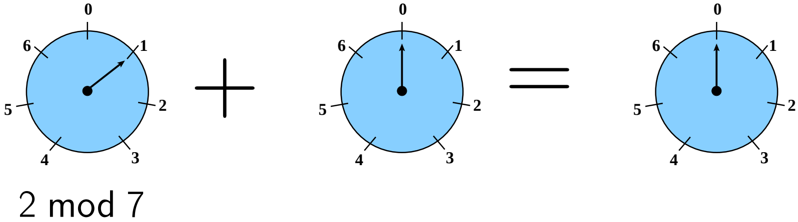
$$(a+b) \bmod n \;=\; ((a \bmod n)+(b \bmod n)) \bmod n$$

Clock Addition: $2 + 3 \bmod 7$

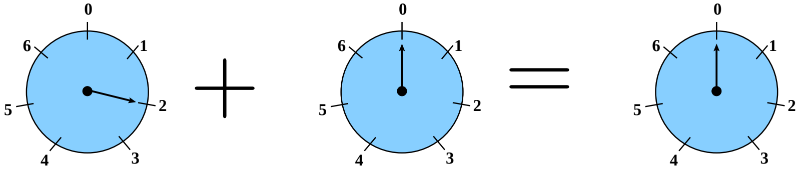


$2 \bmod 7$

Clock Addition: $2 + 3 \bmod 7$

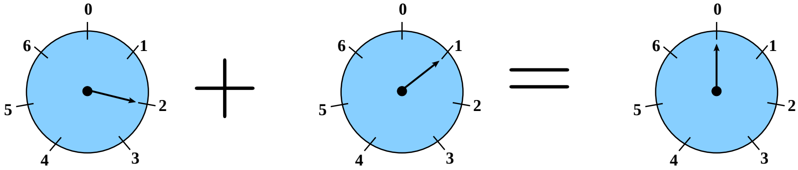


Clock Addition: $2 + 3 \text{ mod } 7$



2 mod 7

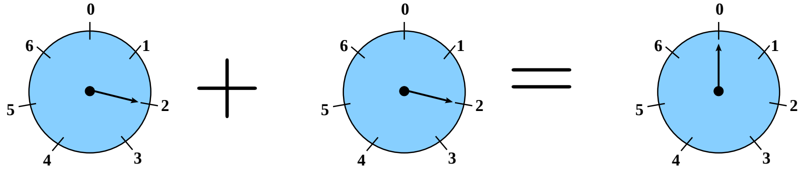
Clock Addition: $2 + 3 \bmod 7$



2 mod 7

3 mod 7

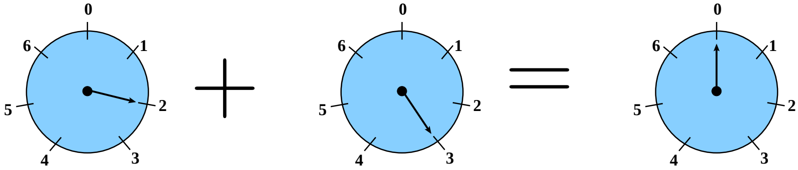
Clock Addition: $2 + 3 \textbf{ mod } 7$



2 mod 7

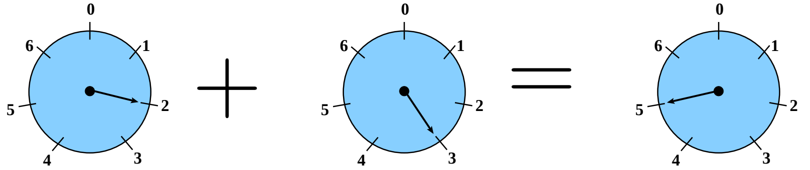
3 mod 7

Clock Addition: $2 + 3 \bmod 7$



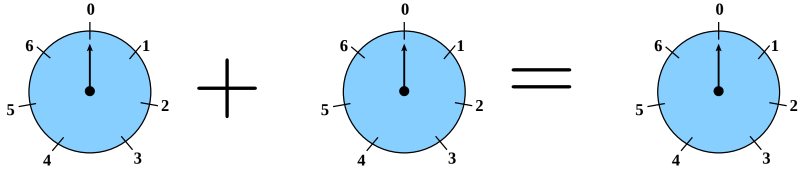
2 mod 7 3 mod 7

Clock Addition: $2 + 3 \bmod 7$



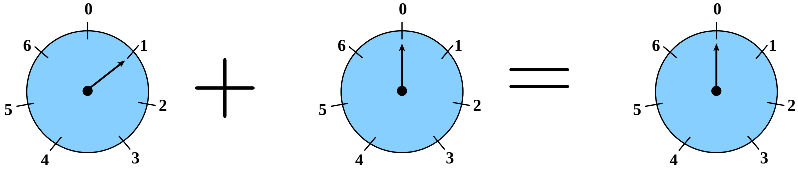
$2 \bmod 7$ $\quad + \quad$ $3 \bmod 7$ $\quad = \quad$ $2 + 3 \bmod 7$

Clock Addition: $8 + 5 \bmod 7$



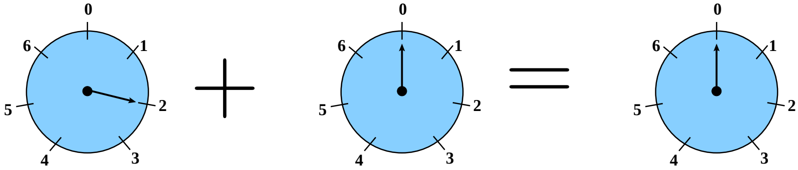
8 mod 7

Clock Addition: $8 + 5 \bmod 7$



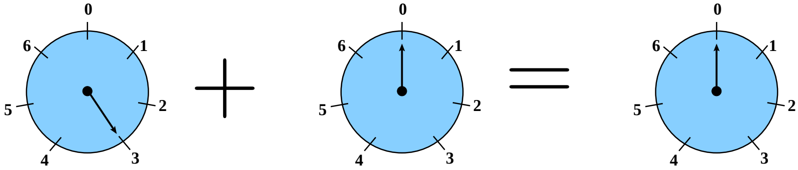
8 mod 7

Clock Addition: $8 + 5 \bmod 7$



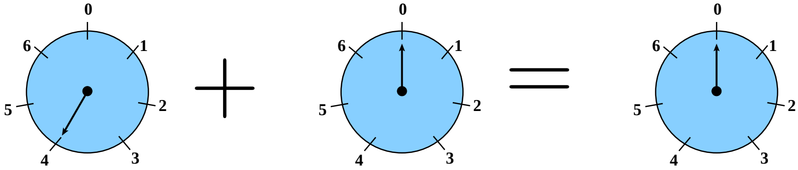
$8 \bmod 7$

Clock Addition: $8 + 5 \bmod 7$



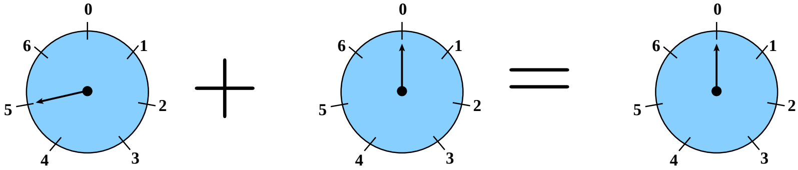
8 mod 7

Clock Addition: $8 + 5 \bmod 7$



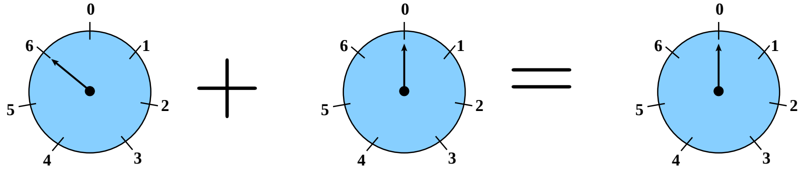
8 mod 7

Clock Addition: $8 + 5 \bmod 7$



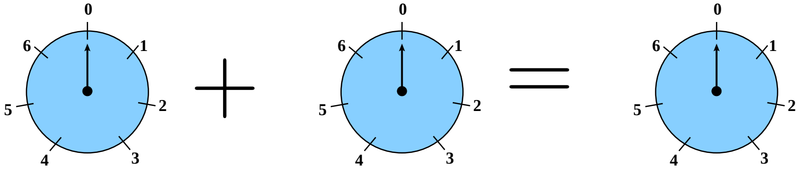
8 mod 7

Clock Addition: $8 + 5 \bmod 7$



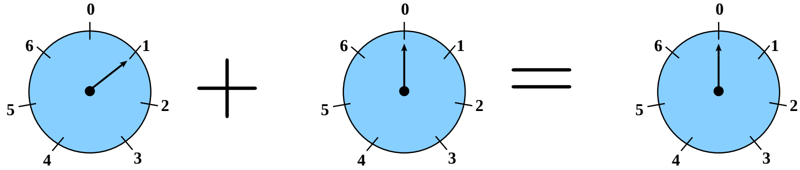
$8 \bmod 7$

Clock Addition: $8 + 5 \bmod 7$



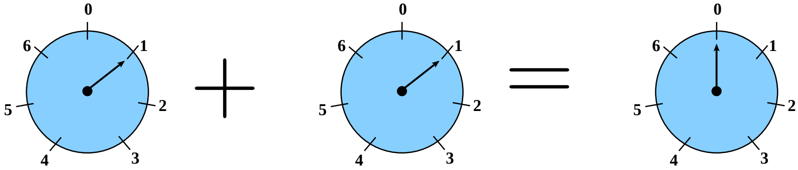
8 mod 7

Clock Addition: $8 + 5 \bmod 7$



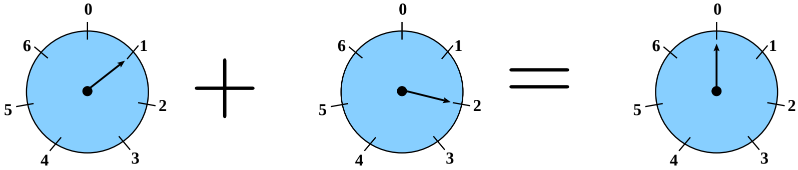
8 mod 7

Clock Addition: $8 + 5 \bmod 7$



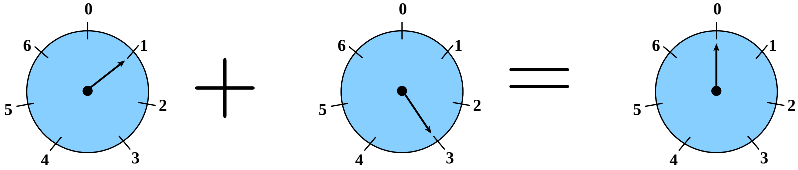
$8 \bmod 7$ $5 \bmod 7$

Clock Addition: $8 + 5 \bmod 7$



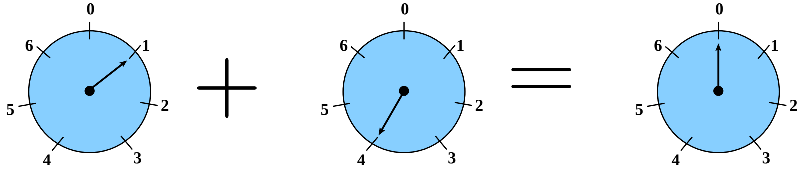
8 mod 7   5 mod 7

Clock Addition: $8 + 5 \textbf{ mod } 7$



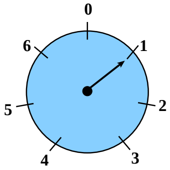
8 mod 7　　　　5 mod 7

Clock Addition: $8 + 5 \bmod 7$

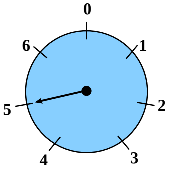


$8 \bmod 7$ $\qquad$ $5 \bmod 7$

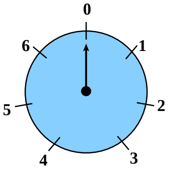
Clock Addition: $8 + 5 \bmod 7$



$+$



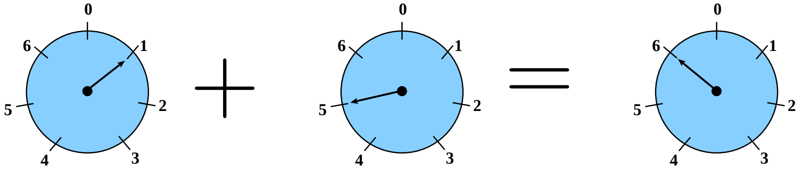
$=$



8 mod 7

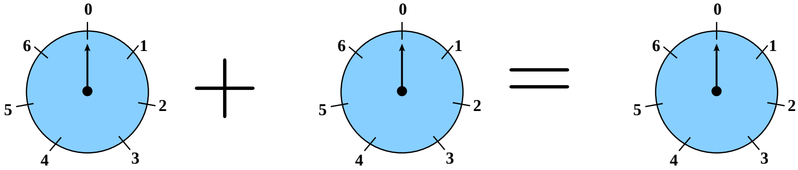
5 mod 7

Clock Addition: $8 + 5 \bmod 7$



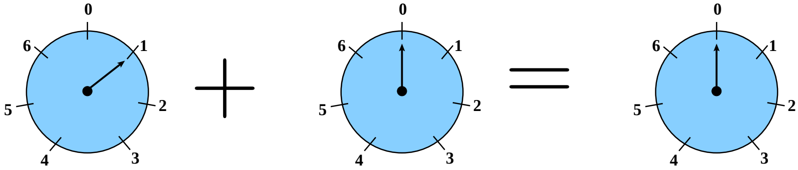
$8 \bmod 7$ $\qquad$ $5 \bmod 7$ $\qquad$ $8 + 5 \bmod 7$

Clock Addition: $8 + 7 \bmod 7$



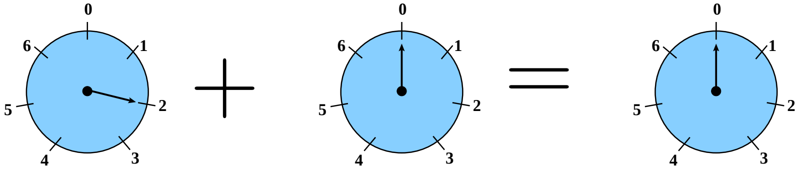
8 mod 7

Clock Addition: $8 + 7 \bmod 7$



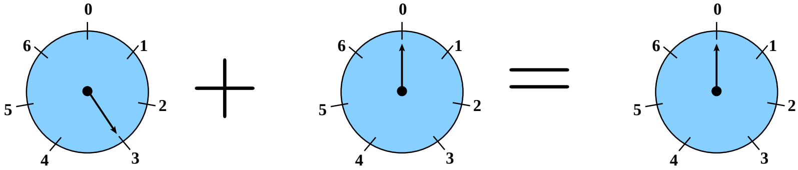
8 mod 7

Clock Addition: $8 + 7 \textbf{ mod } 7$



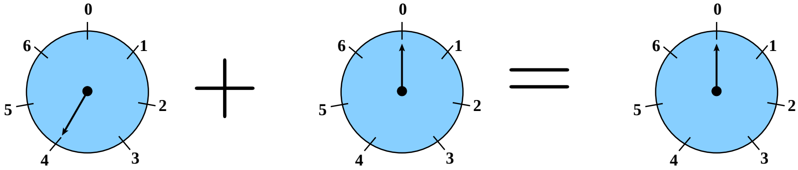
8 mod 7

Clock Addition: $8 + 7 \bmod 7$



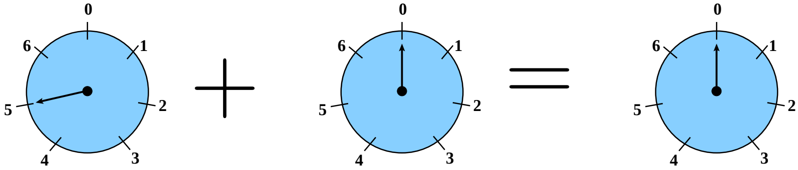
$8 \bmod 7$

Clock Addition: $8 + 7 \ \mathbf{mod}\ 7$



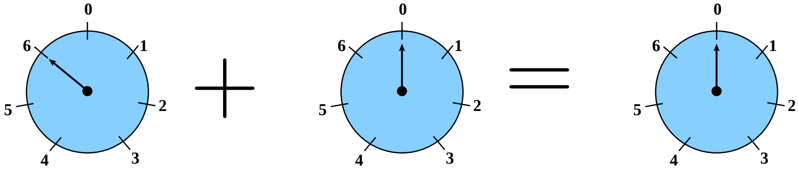
8 mod 7

Clock Addition: $8 + 7 \textbf{ mod } 7$



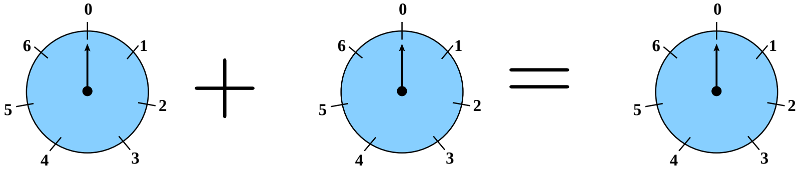
8 mod 7

Clock Addition: $8 + 7 \bmod 7$



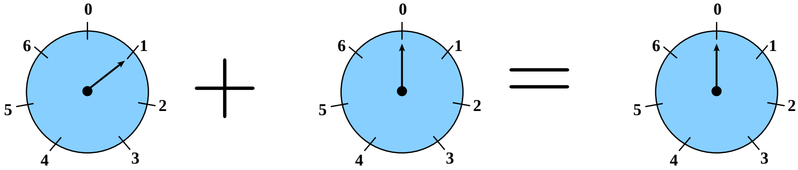
8 mod 7

Clock Addition: $8 + 7 \bmod 7$



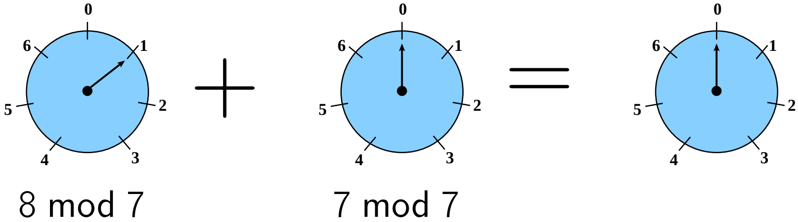
8 mod 7

Clock Addition: $8 + 7 \textbf{ mod } 7$

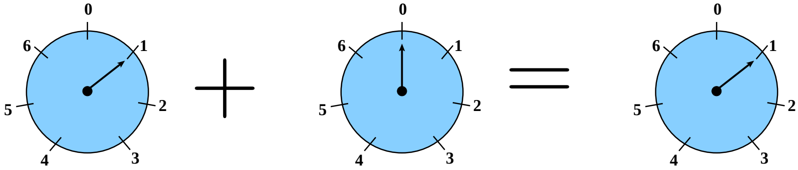


8 mod 7

Clock Addition: $8 + 7 \bmod 7$

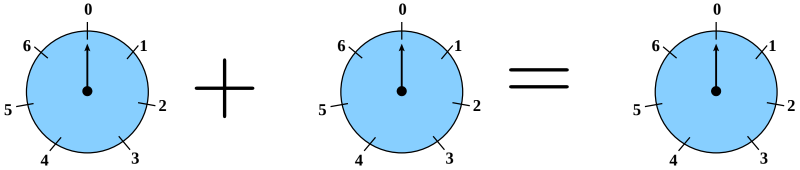


Clock Addition: $8 + 7 \text{ mod } 7$



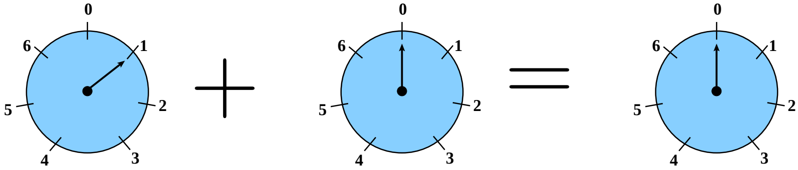
$8 \text{ mod } 7 \qquad + \qquad 7 \text{ mod } 7 \qquad = \qquad 1 + 0 \text{ mod } 7$

Clock Addition: $12 + 10 \bmod 7$



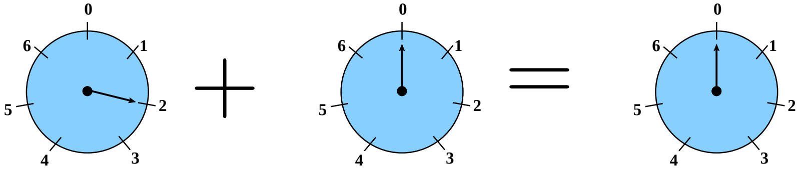
12 mod 7

Clock Addition: $12 + 10 \bmod 7$



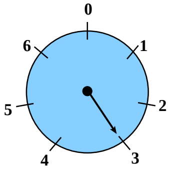
12 mod 7

Clock Addition: $12 + 10 \textbf{ mod } 7$

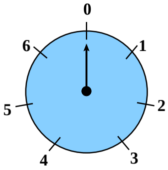


12 mod 7

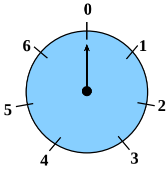
Clock Addition: $12 + 10 \bmod 7$



$+$

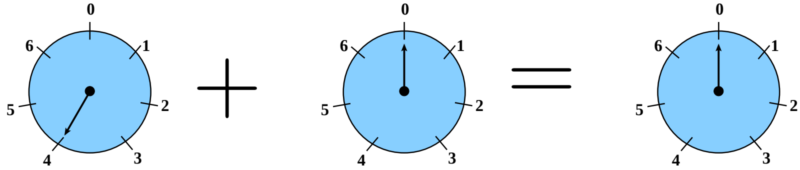


$=$



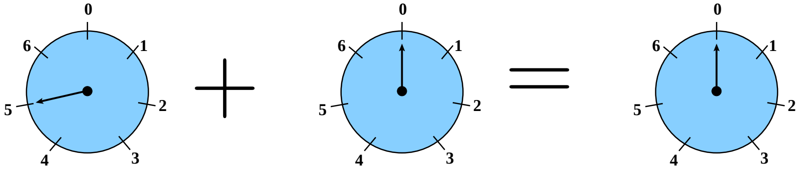
12 mod 7

Clock Addition: $12 + 10 \textbf{ mod } 7$



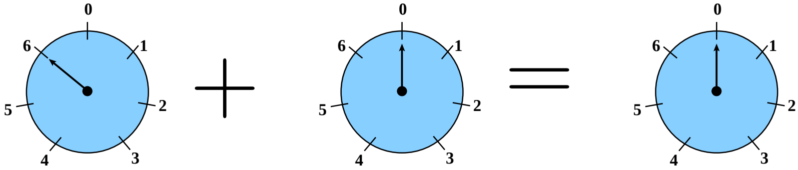
12 mod 7

Clock Addition: $12 + 10 \textbf{ mod } 7$



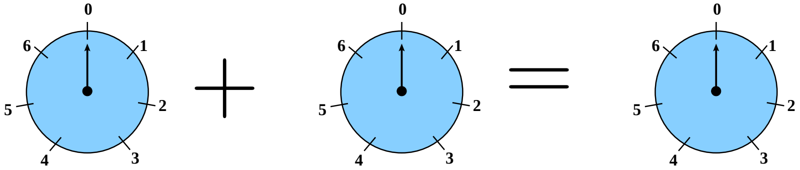
12 mod 7

Clock Addition: $12 + 10 \bmod 7$



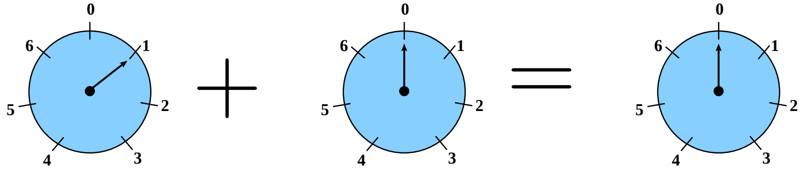
12 mod 7

Clock Addition: $12 + 10 \bmod 7$



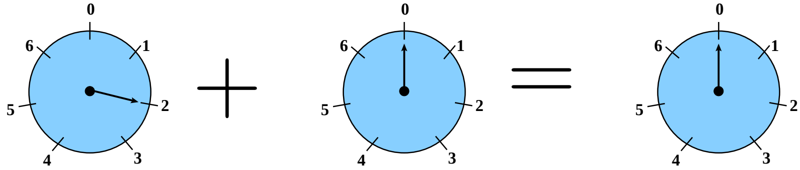
12 mod 7

Clock Addition: $12 + 10 \bmod 7$



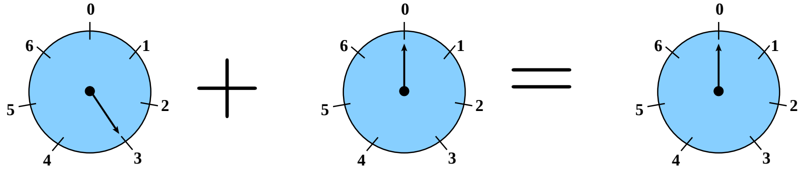
12 mod 7

Clock Addition: $12 + 10 \textbf{ mod } 7$



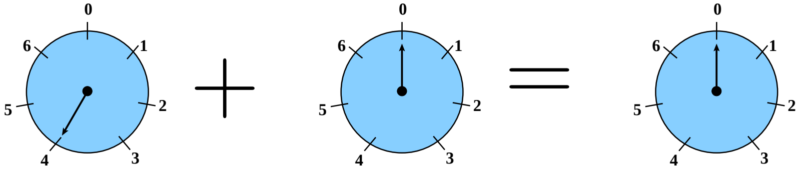
12 mod 7

Clock Addition: $12 + 10 \bmod 7$



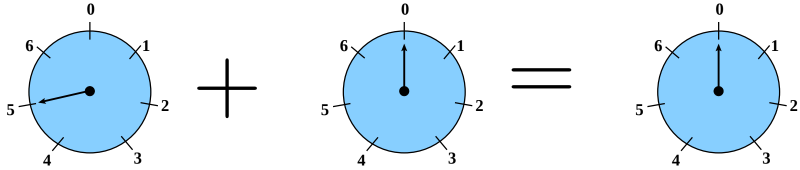
12 mod 7

Clock Addition: $12 + 10 \bmod 7$



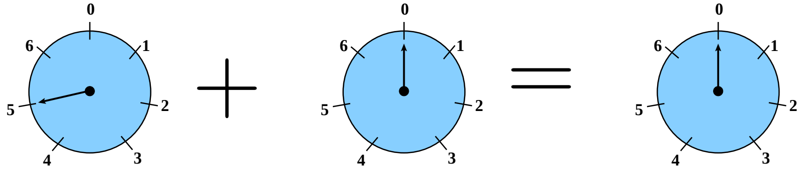
12 mod 7

Clock Addition: $12 + 10 \bmod 7$



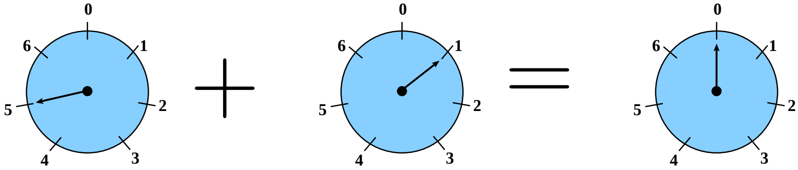
12 mod 7

Clock Addition: $12 + 10 \textbf{ mod } 7$



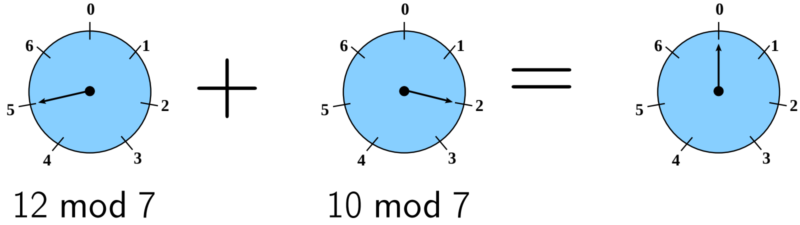
12 mod 7 10 mod 7

Clock Addition: $12 + 10 \bmod 7$

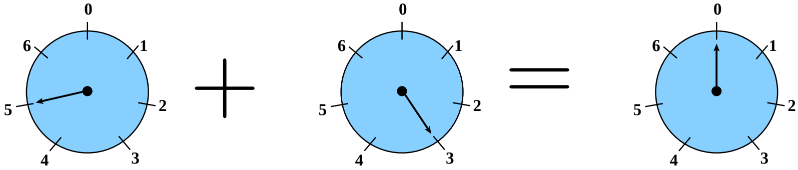


12 mod 7 10 mod 7

Clock Addition: $12 + 10 \ \mathbf{mod}\ 7$



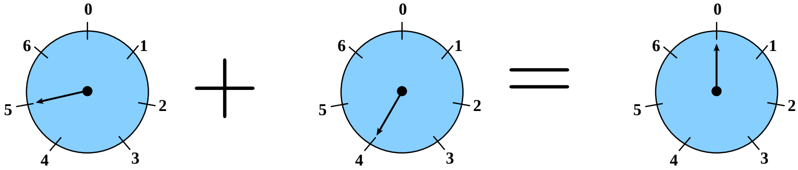
Clock Addition: $12 + 10 \bmod 7$



12 mod 7

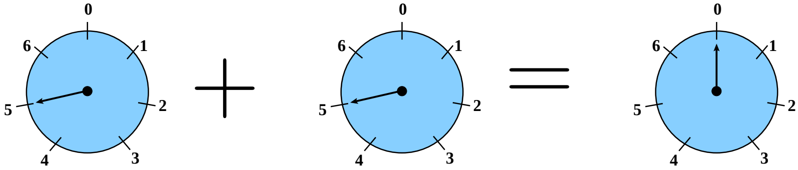
10 mod 7

Clock Addition: $12 + 10 \bmod 7$



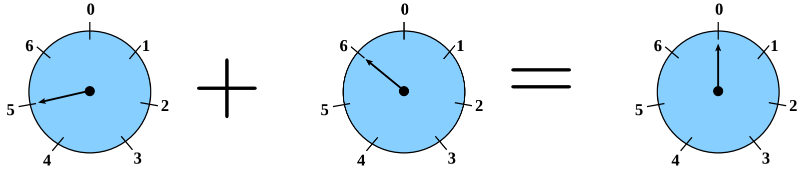
$12 \bmod 7$ $\qquad$ $10 \bmod 7$

Clock Addition: $12 + 10 \bmod 7$



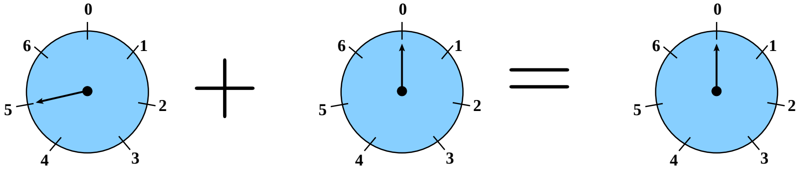
$12 \bmod 7$ $10 \bmod 7$

Clock Addition: $12 + 10 \textbf{ mod } 7$



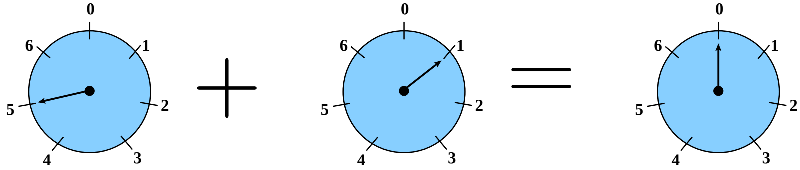
12 mod 7 10 mod 7

Clock Addition: $12 + 10 \bmod 7$



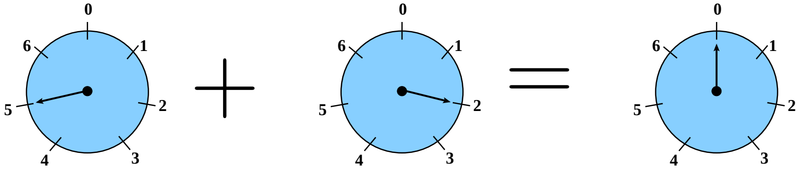
12 mod 7 10 mod 7

Clock Addition: $12 + 10 \ \mathbf{mod}\ 7$



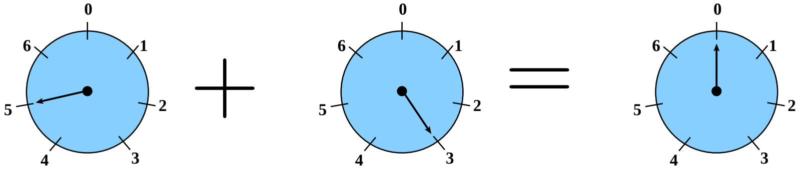
12 mod 7 10 mod 7

Clock Addition: $12 + 10 \textbf{ mod } 7$



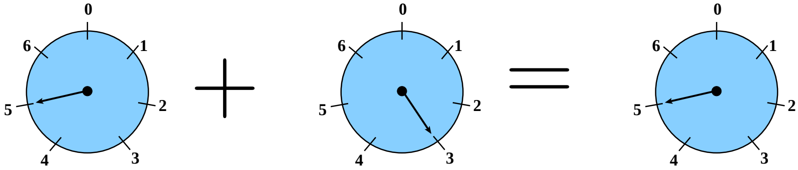
12 mod 7 10 mod 7

Clock Addition: $12 + 10 \bmod 7$



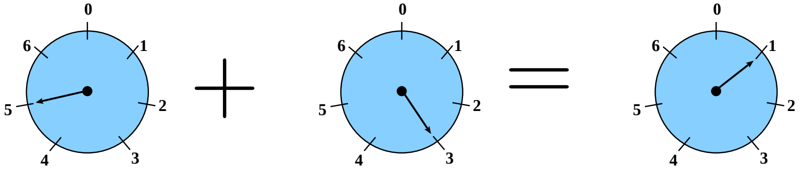
12 mod 7 10 mod 7

Clock Addition: $12 + 10 \bmod 7$



$12 \bmod 7$ $\quad$ $10 \bmod 7$ $\quad$ $5 + 3 \bmod 7$

Clock Addition: $12 + 10$ **mod** 7



12 mod 7 | 10 mod 7 | $5 + 3$ mod 7

Modular Arithmetic — Examples

$$\begin{aligned} 23 &\equiv \quad \mod 12 \\ 23 &\equiv \quad \mod 7 \\ (10+13) \bmod 7 &= \\ &= \\ &= \end{aligned}$$

Modular Arithmetic — Examples

$$
\begin{aligned}
23 &\equiv 11 \bmod 12 \\
23 &\equiv \quad \bmod 7 \\
(10 + 13) \bmod 7 &= \\
&= \\
&=
\end{aligned}
$$

Modular Arithmetic — Examples

$$
\begin{aligned}
23 &\equiv 11 \bmod 12 \\
23 &\equiv 2 \bmod 7 \\
(10 + 13) \bmod 7 &= \\
&= \\
&=
\end{aligned}
$$

Modular Arithmetic — Examples

$$
\begin{aligned}
23 &\equiv 11 \bmod 12 \\
23 &\equiv 2 \bmod 7 \\
(10 + 13) \bmod 7 &= ((10 \bmod 7) + (13 \bmod 7)) \bmod 7 \\
&= \\
&=
\end{aligned}
$$

Modular Arithmetic — Examples

$$
\begin{aligned}
23 &\equiv 11 \bmod 12 \\
23 &\equiv 2 \bmod 7 \\
(10 + 13) \bmod 7 &= ((10 \bmod 7) + (13 \bmod 7)) \bmod 7 \\
&= (3 + 6) \bmod 7 \\
&=
\end{aligned}
$$

Modular Arithmetic — Examples

$$
\begin{aligned}
23 &\equiv 11 \bmod 12 \\
23 &\equiv 2 \bmod 7 \\
(10 + 13) \bmod 7 &= ((10 \bmod 7) + (13 \bmod 7)) \bmod 7 \\
&= (3 + 6) \bmod 7 \\
&= 2
\end{aligned}
$$

Exercise: Modular Addition

1. $0 \equiv ? \mod 7$:

Exercise: Modular Addition

1. $0 \equiv ? \mod 7$: 0
2. $1 \equiv ? \mod 7$:

Exercise: Modular Addition

1. $0 \equiv ? \bmod 7$: 0
2. $1 \equiv ? \bmod 7$: 1
3. $2 \equiv ? \bmod 7$:

Exercise: Modular Addition

1. $0 \equiv ? \mod 7$: 0
2. $1 \equiv ? \mod 7$: 1
3. $2 \equiv ? \mod 7$: 2
4. $11 \equiv ? \mod 7$:

Exercise: Modular Addition

1. $0 \equiv ? \mod 7$: 0
2. $1 \equiv ? \mod 7$: 1
3. $2 \equiv ? \mod 7$: 2
4. $11 \equiv ? \mod 7$: 3
5. $22 \equiv ? \mod 7$:

Exercise: Modular Addition

1. $0 \equiv ? \bmod 7$: 0
2. $1 \equiv ? \bmod 7$: 1
3. $2 \equiv ? \bmod 7$: 2
4. $11 \equiv ? \bmod 7$: 3
5. $22 \equiv ? \bmod 7$: 1
6. $(22 + 11) \bmod 7 =$

Exercise: Modular Addition

1. $0 \equiv ? \bmod 7$: 0
2. $1 \equiv ? \bmod 7$: 1
3. $2 \equiv ? \bmod 7$: 2
4. $11 \equiv ? \bmod 7$: 3
5. $22 \equiv ? \bmod 7$: 1
6. $(22 + 11) \bmod 7 = 5$
7. $(771 + 71) \bmod 7 =$

Exercise: Modular Addition

1. $0 \equiv ? \bmod 7$: 0
2. $1 \equiv ? \bmod 7$: 1
3. $2 \equiv ? \bmod 7$: 2
4. $11 \equiv ? \bmod 7$: 3
5. $22 \equiv ? \bmod 7$: 1
6. $(22 + 11) \bmod 7 =$ 5
7. $(771 + 71) \bmod 7 =$2

Modular Arithmetic

- Subtraction and multiplication are done the same way:

$$
\begin{aligned}
(a - b) \bmod n &= ((a \bmod n) - (b \bmod n)) \bmod n \\
(a * b) \bmod n &= ((a \bmod n) * (b \bmod n)) \bmod n
\end{aligned}
$$

Exercises

1. $(22 * 11) \bmod 7 \equiv ? \bmod 7$:

Exercises

1. $(22 * 11) \bmod 7 \equiv ? \bmod 7$: 4
2. $(771 - 71) \bmod 7 \equiv ? \bmod 7$:

Exercises

1. $(22 * 11) \bmod 7 \equiv ? \bmod 7$: 4
2. $(771 - 71) \bmod 7 \equiv ? \bmod 7$: 0
3. $(771 * 71) \bmod 7 \equiv ? \bmod 7$:

Exercises

1. $(22 * 11) \bmod 7 \equiv ? \bmod 7$: 4
2. $(771 - 71) \bmod 7 \equiv ? \bmod 7$: 0
3. $(771 * 71) \bmod 7 \equiv ? \bmod 7$: 1
4. $((22 + 11) - (25 * 8)) \bmod 7 \equiv ? \bmod 7$:

Exercises

1. $(22 * 11) \bmod 7 \equiv ? \bmod 7$: 4
2. $(771 - 71) \bmod 7 \equiv ? \bmod 7$: 0
3. $(771 * 71) \bmod 7 \equiv ? \bmod 7$: 1
4. $((22 + 11) - (25 * 8)) \bmod 7 \equiv ? \bmod 7$: 1

Negative Numbers

- To find $-b \bmod N$ keep adding N to $-b$ until the number is between 0 and $N-1$.
- Example, $N = 13$, $b = -27$:
  1. Add 13, you get $-27 + 13 = -14$
  2. Add 13, you get $-14 + 13 = -1$
  3. Add 13, you get $-1 + 13 = 12$.
  4. I.e. $-27 \bmod 13 = 12$.

Exercises

1. $(-1) \bmod 7 \equiv ? \bmod 7$:

Exercises

1. $(-1) \bmod 7 \equiv ? \bmod 7$: 6
2. $(-8) \bmod 7 \equiv ? \bmod 7$:

Exercises

1. $(-1) \bmod 7 \equiv ? \bmod 7$: 6
2. $(-8) \bmod 7 \equiv ? \bmod 7$: 6
3. $(-21) \bmod 5 \equiv ? \bmod 7$:

Exercises

1. $(-1) \bmod 7 \equiv ? \bmod 7$: 6
2. $(-8) \bmod 7 \equiv ? \bmod 7$: 6
3. $(-21) \bmod 5 \equiv ? \bmod 7$: 4
4. $(11 - 22) \bmod 7 \equiv ? \bmod 7$:

Exercises

1. $(-1) \bmod 7 \equiv ? \bmod 7$: 6
2. $(-8) \bmod 7 \equiv ? \bmod 7$: 6
3. $(-21) \bmod 5 \equiv ? \bmod 7$: 4
4. $(11 - 22) \bmod 7 \equiv ? \bmod 7$: 3
5. $(22 - 11) \bmod 7 \equiv ? \bmod 7$:

Exercises

1. $(-1) \bmod 7 \equiv ? \bmod 7$: 6
2. $(-8) \bmod 7 \equiv ? \bmod 7$: 6
3. $(-21) \bmod 5 \equiv ? \bmod 7$: 4
4. $(11 - 22) \bmod 7 \equiv ? \bmod 7$: 3
5. $(22 - 11) \bmod 7 \equiv ? \bmod 7$: 3
6. $(25 - 9) \bmod 5 \equiv ? \bmod 7$:

Exercises

1. $(-1) \bmod 7 \equiv ? \bmod 7$: 6
2. $(-8) \bmod 7 \equiv ? \bmod 7$: 6
3. $(-21) \bmod 5 \equiv ? \bmod 7$: 4
4. $(11 - 22) \bmod 7 \equiv ? \bmod 7$: 3
5. $(22 - 11) \bmod 7 \equiv ? \bmod 7$: 3
6. $(25 - 9) \bmod 5 \equiv ? \bmod 7$: 1
7. $(10 - 13) \bmod 9 \equiv ? \bmod 7$:

Exercises

1. $(-1) \bmod 7 \equiv ? \bmod 7$: 6
2. $(-8) \bmod 7 \equiv ? \bmod 7$: 6
3. $(-21) \bmod 5 \equiv ? \bmod 7$: 4
4. $(11 - 22) \bmod 7 \equiv ? \bmod 7$: 3
5. $(22 - 11) \bmod 7 \equiv ? \bmod 7$: 3
6. $(25 - 9) \bmod 5 \equiv ? \bmod 7$: 1
7. $(10 - 13) \bmod 9 \equiv ? \bmod 7$: 6

Modular Addition Tables

- Addition table for Z_{10}, $(x + y) \bmod 10$.

$+$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Exercise: Modular Subtraction Tables

- Generate the subtraction table for Z_5, $(x - y) \bmod 5$.

$-$	0	1	2	3	4
0					
1					
2					
3					
4					

Outline

Greatest Common Divisor

- $\mathrm{GCD}(a, b)$ is the largest number d that divides a and b evenly.

Greatest Common Divisor

- $\mathrm{GCD}(a, b)$ is the largest number d that divides a and b evenly.
- Example:

Greatest Common Divisor

- $\mathrm{GCD}(a, b)$ is the largest number d that divides a and b evenly.
- Example:
  - The divisors of 54 are: $1, 2, 3, 6, 9, 18, 27, 54$

Greatest Common Divisor

- $\mathrm{GCD}(a, b)$ is the largest number d that divides a and b evenly.
- Example:
  - The divisors of 54 are: $1, 2, 3, 6, 9, 18, 27, 54$
  - The divisors of 24 are: $1, 2, 3, 4, 6, 8, 12, 24$

Greatest Common Divisor

- $\mathrm{GCD}(a, b)$ is the largest number d that divides a and b evenly.
- Example:
  - The divisors of 54 are: $1, 2, 3, 6, 9, 18, 27, 54$
  - The divisors of 24 are: $1, 2, 3, 4, 6, 8, 12, 24$
  - The common divisors of 54 and 24 are: $1, 2, 3, 6$

Greatest Common Divisor

- $\mathrm{GCD}(a, b)$ is the largest number d that divides a and b evenly.
- Example:
  - The divisors of 54 are: $1, 2, 3, 6, 9, 18, 27, 54$
  - The divisors of 24 are: $1, 2, 3, 4, 6, 8, 12, 24$
  - The common divisors of 54 and 24 are: $1, 2, 3, 6$
  - $\mathrm{GCD}(54, 24) = 6$

Exercise: Greatest Common Divisor

1. The divisors of 21 are:

Exercise: Greatest Common Divisor

1. The divisors of 21 are: 1,3,7
2. The divisors of 23 are:

Exercise: Greatest Common Divisor

1. The divisors of 21 are: 1,3,7
2. The divisors of 23 are: 1,23
3. The divisors of 99 are:

Exercise: Greatest Common Divisor

1. The divisors of 21 are: 1,3,7
2. The divisors of 23 are: 1,23
3. The divisors of 99 are: 1,3,11
4. The common divisors of 21 and 23 are:

Exercise: Greatest Common Divisor

1. The divisors of 21 are: 1,3,7
2. The divisors of 23 are: 1,23
3. The divisors of 99 are: 1,3,11
4. The common divisors of 21 and 23 are: 1
5. The common divisors of 66 and 110 are:

Exercise: Greatest Common Divisor

1. The divisors of 21 are: 1,3,7
2. The divisors of 23 are: 1,23
3. The divisors of 99 are: 1,3,11
4. The common divisors of 21 and 23 are: 1
5. The common divisors of 66 and 110 are: 1,2,11
6. $\mathrm{GCD}(66, 110) =$

Exercise: Greatest Common Divisor

1. The divisors of 21 are: 1,3,7
2. The divisors of 23 are: 1,23
3. The divisors of 99 are: 1,3,11
4. The common divisors of 21 and 23 are: 1
5. The common divisors of 66 and 110 are: 1,2,11
6. $\mathrm{GCD}(66, 110) =$ 11
7. $\mathrm{GCD}(52, 78) =$

Exercise: Greatest Common Divisor

1. The divisors of 21 are: 1,3,7
2. The divisors of 23 are: 1,23
3. The divisors of 99 are: 1,3,11
4. The common divisors of 21 and 23 are: 1
5. The common divisors of 66 and 110 are: 1,2,11
6. $\mathrm{GCD}(66, 110) =$ 11
7. $\mathrm{GCD}(52, 78) =$ 13

Euclid's GCD Algorithm

- Based on the observation that if x divides a and b, it also divides $a - b$. We need to find the largest such x.

Euclid's GCD Algorithm

- Based on the observation that if x divides a and b, it also divides $a - b$. We need to find the largest such x.
- Key observation: If

$$d = \mathrm{GCD}(a, b) \text{ and } b > 0$$

then

$$d = \mathrm{GCD}(b, a \bmod b)$$

Euclid's GCD Algorithm — Recursive

```
function gcd(a, b)
    if b = 0
        return a;
    else
        return gcd(b, a mod b);
```

Euclid's GCD Algorithm — Iterative

```
function gcd(a, b)
    while b != 0
        t := b;
        b := a mod b;
        a := t;
    return a;
```

Euclid's GCD Algorithm: Example

$$\mathrm{GCD}(546, 198) = \mathrm{GCD}(198, 546 \bmod 198) = \mathrm{GCD}(198, 150)$$

Euclid's GCD Algorithm: Example

$$\begin{aligned}
\mathrm{GCD}(546, 198) &= \mathrm{GCD}(198, 546 \bmod 198) = \mathrm{GCD}(198, 150) \\
&= \mathrm{GCD}(150, 198 \bmod 150) = \mathrm{GCD}(150, 48)
\end{aligned}$$

Euclid's GCD Algorithm: Example

$$\begin{aligned}
\mathrm{GCD}(546, 198) &= \mathrm{GCD}(198, 546 \bmod 198) = \mathrm{GCD}(198, 150) \\
&= \mathrm{GCD}(150, 198 \bmod 150) = \mathrm{GCD}(150, 48) \\
&= \mathrm{GCD}(48, 150 \bmod 48) = \mathrm{GCD}(48, 6)
\end{aligned}$$

Euclid's GCD Algorithm: Example

$$
\begin{aligned}
\mathrm{GCD}(546, 198) &= \mathrm{GCD}(198, 546 \bmod 198) = \mathrm{GCD}(198, 150) \\
&= \mathrm{GCD}(150, 198 \bmod 150) = \mathrm{GCD}(150, 48) \\
&= \mathrm{GCD}(48, 150 \bmod 48) = \mathrm{GCD}(48, 6) \\
&= \mathrm{GCD}(6, 48 \bmod 6) = \mathrm{GCD}(6, 0)
\end{aligned}
$$

Euclid's GCD Algorithm: Example

$$\begin{aligned}
\mathrm{GCD}(546, 198) &= \mathrm{GCD}(198, 546 \bmod 198) = \mathrm{GCD}(198, 150) \\
&= \mathrm{GCD}(150, 198 \bmod 150) = \mathrm{GCD}(150, 48) \\
&= \mathrm{GCD}(48, 150 \bmod 48) = \mathrm{GCD}(48, 6) \\
&= \mathrm{GCD}(6, 48 \bmod 6) = \mathrm{GCD}(6, 0) \\
&= 6
\end{aligned}$$

Euclid's GCD Algorithm...

- Compute GCD by hand:
  1. divide the larger one by the smaller;
  2. write an equation of the form

$$\text{larger} = \text{smaller} \times \text{quotient} + \text{remainder};$$

  3. repeat using the two numbers smaller and remainder;
  4. when you get a 0 remainder, the previous line will be the gcd of the original two numbers.

Euclid's GCD Algorithm...

- Find $\mathrm{GCD}(421, 111)$.

$$421 = 111 \times 3 + 88$$

Euclid's GCD Algorithm...

- Find $\mathrm{GCD}(421, 111)$.

$$\begin{aligned} 421 &= 111 \times 3 + 88 \\ 111 &= 88 \times 1 + 23 \end{aligned}$$

Euclid's GCD Algorithm...

- Find $\mathrm{GCD}(421, 111)$.

$$\begin{aligned} 421 &= 111 \times 3 + 88 \\ 111 &= 88 \times 1 + 23 \\ 88 &= 23 \times 3 + 19 \end{aligned}$$

Euclid's GCD Algorithm...

- Find $\mathrm{GCD}(421, 111)$.

$$\begin{aligned}
421 &= 111 \times 3 + 88 \\
111 &= 88 \times 1 + 23 \\
88 &= 23 \times 3 + 19 \\
23 &= 19 \times 1 + 4
\end{aligned}$$

Euclid's GCD Algorithm...

- Find $\mathrm{GCD}(421, 111)$.

$$\begin{aligned}
421 &= 111 \times 3 + 88 \\
111 &= 88 \times 1 + 23 \\
88 &= 23 \times 3 + 19 \\
23 &= 19 \times 1 + 4 \\
19 &= 4 \times 4 + 3
\end{aligned}$$

Euclid's GCD Algorithm...

- Find $\mathrm{GCD}(421, 111)$.

$$\begin{aligned}
421 &= 111 \times 3 + 88 \\
111 &= 88 \times 1 + 23 \\
88 &= 23 \times 3 + 19 \\
23 &= 19 \times 1 + 4 \\
19 &= 4 \times 4 + 3 \\
4 &= 3 \times 1 + \boxed{1}
\end{aligned}$$

Euclid's GCD Algorithm. . .

- Find $\mathrm{GCD}(421, 111)$.

$$
\begin{aligned}
421 &= 111 \times 3 + 88 \\
111 &= 88 \times 1 + 23 \\
88 &= 23 \times 3 + 19 \\
23 &= 19 \times 1 + 4 \\
19 &= 4 \times 4 + 3 \\
4 &= 3 \times 1 + \boxed{1} \\
3 &= 1 \times 3 + 0
\end{aligned}
$$

- The last non-zero remainder is 1 $\Rightarrow \mathrm{GCD}(421, 111) = 1$.

Exercise

- Compute $\mathrm{GCD}(196, 42)$. Show your work.

Bezout's identity

Theorem (Bezout's identity)

Given any integers a and b, not both zero, there exist integers i and j such that $\mathrm{GCD}(a, b) = ia + jb$.

- Example:

$$\mathrm{GCD}(819, 462) = (-9) \times 819 + 16 \times 462 = 21.$$

Euclid's GCD Algorithm

- We use Extended GCD Algorithm to compute i and j.
- Euclid's extended algorithm $\mathrm{GCD}(a, b)$ returns a triple (d, i, j). d is the greatest common divisor of a and b.

Euclid's Extended GCD Algorithm

```
function gcd(int a, int b)
             : (int,int,int) =
   if b = 0 then
      return (a, 1, 0)
   q ← ⌊a/b⌋
   (d, k, l) ← gcd(b, a mod b)
   return (d, l, k − lq)
```

Exercise

- Compute i and j such that at

$$\mathrm{GCD}(196, 42) = i \times 196 + j \times 42.$$

Show your work.

Euclid's GCD Algorithm — Subtraction only!!!

```
while a != b {
    while a > b {
        c = a - b;
        a = c;
    }
    while b > a {
        c = b - a;
        b = c;
    }
}
```

Outline

1. Modular Arithmetic
2. Greatest Common Divisor
   - Bezout's identity
3. Modular Inverses
   - Computing Modular Inverses
4. Summary

Inverses

- The inverse of 4 is $\frac{1}{4}$.
- What does this mean?
- To find the inverse of x we want to compute:

$$x \cdot y = 1$$

- In the "normal" integer space, inverses always exist.
- We can write the inverse as: $x^{-1} = \frac{1}{x}$.

Modular Inverses

- y is the modular inverse of x, modulo n, if

$$xy \bmod n = 1$$

- Not every number in Z_n has an inverse:

$$\begin{aligned} 5 \cdot 3 &= 1 \bmod 14 \\ 2 \cdot ? &= 1 \bmod 14 \end{aligned}$$

Modular Inverses by Brute Force!

- What is the inverse of $3 \pmod{7}$?

Modular Inverses by Brute Force!

- What is the inverse of $3 \pmod 7$?
- Try all values in Z_7:

Modular Inverses by Brute Force!

- What is the inverse of $3 \pmod 7$?
- Try all values in Z_7:
  1. $3 * 0 = 0 \pmod 7$

Modular Inverses by Brute Force!

- What is the inverse of $3 \pmod 7$?
- Try all values in Z_7:
  1. $3 * 0 = 0 \pmod 7$
  2. $3 * 1 = 3 \pmod 7$

Modular Inverses by Brute Force!

- What is the inverse of $3 \pmod 7$?
- Try all values in Z_7:
  1. $3 * 0 = 0 \pmod 7$
  2. $3 * 1 = 3 \pmod 7$
  3. $3 * 2 = 6 \pmod 7$

Modular Inverses by Brute Force!

- What is the inverse of $3 \pmod 7$?
- Try all values in Z_7:
  1. $3 * 0 = 0 \pmod 7$
  2. $3 * 1 = 3 \pmod 7$
  3. $3 * 2 = 6 \pmod 7$
  4. $3 * 3 = 9 = 2 \pmod 7$

Modular Inverses by Brute Force!

- What is the inverse of $3 \pmod 7$?
- Try all values in Z_7:
  1. $3 * 0 = 0 \pmod 7$
  2. $3 * 1 = 3 \pmod 7$
  3. $3 * 2 = 6 \pmod 7$
  4. $3 * 3 = 9 = 2 \pmod 7$
  5. $3 * 4 = 12 = 5 \pmod 7$

Modular Inverses by Brute Force!

- What is the inverse of $3 \pmod{7}$?
- Try all values in Z_7:
  1. $3 * 0 = 0 \pmod{7}$
  2. $3 * 1 = 3 \pmod{7}$
  3. $3 * 2 = 6 \pmod{7}$
  4. $3 * 3 = 9 = 2 \pmod{7}$
  5. $3 * 4 = 12 = 5 \pmod{7}$
  6. $3 * 5 = 15 \pmod{7} = \boxed{1} \pmod{7}$

Modular Inverses by Brute Force!

- What is the inverse of $3 \pmod 7$?
- Try all values in Z_7:
  1. $3 * 0 = 0 \pmod 7$
  2. $3 * 1 = 3 \pmod 7$
  3. $3 * 2 = 6 \pmod 7$
  4. $3 * 3 = 9 = 2 \pmod 7$
  5. $3 * 4 = 12 = 5 \pmod 7$
  6. $3 * 5 = 15 \pmod 7 = \boxed{1} \pmod 7$
  7. $3 * 6 = 18 \pmod 7 = 4 \pmod 7$

Modular Inverses by Brute Force!

- What is the inverse of $3 \pmod 7$?
- Try all values in Z_7:
  1. $3 * 0 = 0 \pmod 7$
  2. $3 * 1 = 3 \pmod 7$
  3. $3 * 2 = 6 \pmod 7$
  4. $3 * 3 = 9 = 2 \pmod 7$
  5. $3 * 4 = 12 = 5 \pmod 7$
  6. $3 * 5 = 15 \pmod 7 = \boxed{1} \pmod 7$
  7. $3 * 6 = 18 \pmod 7 = 4 \pmod 7$
- $\Rightarrow 3^{-1} \pmod 7 = 5$

Exercise: Modular Inverses by Brute Force

- What is the modular inverse of $3 \pmod{9}$?

Modular Inverses...

- To find the the inverse of 4 modulo 7 we want to compute:

$$4 \cdot x = 1 \bmod 7$$

- This is the same as finding integers x and k such that:

$$4x = 7k + 1$$

- Example:
  - $4 \cdot 2 = 7 \cdot 1 + 1$, i.e. $4^{-1} = 2 \bmod 7$

Modular Inverses: Primes

- If n is prime then every number in Z_n has an inverse.
- Examples:
  1. $4 \cdot 3 \bmod 11 = 12 \bmod 11 = 1 \Rightarrow 4$ is the inverse of 3 in Z_{11}.

Multiplication tables

- Multiplication table for Z_{10}, $xy \bmod 10$.
- Elements that have a modular inverse have been highlighted.

$\times$	**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

Multiplication table for Z_{11}, xy mod 11

×	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

Exercise: Modular Multiplication Table

- Create the modular multiplication table for Z_5, $xy \bmod 5$.

$*$	0	1	2	3	4
0					
1					
2					
3					
4					

Computing Modular Multiplicative Inverses

- We can use the GCD routine to compute modular multiplicative inverses.

Computing Modular Multiplicative Inverses

- We can use the GCD routine to compute modular multiplicative inverses.
- Given $x < n$, we want to compute $y = x^{-1} \bmod n$, i.e.

$$yx \bmod n = 1$$

Computing Modular Multiplicative Inverses

- We can use the GCD routine to compute modular multiplicative inverses.
- Given $x < n$, we want to compute $y = x^{-1} \bmod n$, i.e.

$$yx \bmod n = 1$$

- The inverse of x in Z_n exists when $\mathrm{GCD}(n, x) = 1$.

Modular Multiplicative Inverses...

- Call $\mathrm{GCD}(n, x)$ which returns
$$(1, i, j)$$
such that
$$1 = ix + jn$$

Modular Multiplicative Inverses...

- Call $\mathrm{GCD}(n, x)$ which returns
$$(1, i, j)$$
such that
$$1 = ix + jn$$
- Then
$$(ix + jn) \bmod n = ix \bmod n = 1$$
and i is x's multiplicative inverse in Z_n.

Modular Multiplicative Inverses. . .

- Call $\mathrm{GCD}(n, x)$ which returns
$$(1, i, j)$$
such that
$$1 = ix + jn$$
- Then
$$(ix + jn) \bmod n = ix \bmod n = 1$$
and i is x's multiplicative inverse in Z_n.
- If $\mathrm{GCD}(n, x) \neq 1$ then we know that the inverse doesn't exist.

Example: Modular Multiplicative Inverses

- What is $7^{-1} \pmod{11}$?

Example: Modular Multiplicative Inverses

- What is $7^{-1} \pmod{11}$?
  - $GCD(7, 11) = (1, -3, 2)$

Example: Modular Multiplicative Inverses

- What is $7^{-1} \pmod{11}$?
    - $GCD(7, 11) = (1, -3, 2)$
    - $(-3) \cdot 7 + (2) \cdot 11 = 1$

Example: Modular Multiplicative Inverses

- What is $7^{-1} \pmod{11}$?
  - $GCD(7, 11) = (1, -3, 2)$
  - $(-3) \cdot 7 + (2) \cdot 11 = 1$
  - $7 * (-3) = 1 \mod 11$

Example: Modular Multiplicative Inverses

- What is $7^{-1} \pmod{11}$?
  - $GCD(7, 11) = (1, -3, 2)$
  - $(-3) \cdot 7 + (2) \cdot 11 = 1$
  - $7 * (-3) = 1 \mod 11$
  - $7 * 8 = 1 \mod 11$

Example: Modular Multiplicative Inverses

- What is $7^{-1} \pmod{11}$?
  - $GCD(7, 11) = (1, -3, 2)$
  - $(-3) \cdot 7 + (2) \cdot 11 = 1$
  - $7 * (-3) = 1 \mod 11$
  - $7 * 8 = 1 \mod 11$
  - $7^{-1} \pmod{11} = 8$

Example: Modular Multiplicative Inverses

- What is $7^{-1} \pmod{11}$?
  - $GCD(7, 11) = (1, -3, 2)$
  - $(-3) \cdot 7 + (2) \cdot 11 = 1$
  - $7 * (-3) = 1 \mod 11$
  - $7 * 8 = 1 \mod 11$
  - $7^{-1} \pmod{11} = 8$
- What is $11^{-1} \pmod{23}$?

Example: Modular Multiplicative Inverses

- What is $7^{-1} \pmod{11}$?
  - $GCD(7, 11) = (1, -3, 2)$
  - $(-3) \cdot 7 + (2) \cdot 11 = 1$
  - $7 * (-3) = 1 \mod 11$
  - $7 * 8 = 1 \mod 11$
  - $7^{-1} \pmod{11} = 8$
- What is $11^{-1} \pmod{23}$?
  - $GCD(11, 23) = (1, -2, 1)$

Example: Modular Multiplicative Inverses

- What is $7^{-1} \pmod{11}$?
  - $GCD(7, 11) = (1, -3, 2)$
  - $(-3) \cdot 7 + (2) \cdot 11 = 1$
  - $7 * (-3) = 1 \mod 11$
  - $7 * 8 = 1 \mod 11$
  - $7^{-1} \pmod{11} = 8$
- What is $11^{-1} \pmod{23}$?
  - $GCD(11, 23) = (1, -2, 1)$
  - $(-2) \cdot 11 + (1) \cdot 23 = 1$

Example: Modular Multiplicative Inverses

- What is $7^{-1} \pmod{11}$?
  - $GCD(7, 11) = (1, -3, 2)$
  - $(-3) \cdot 7 + (2) \cdot 11 = 1$
  - $7 * (-3) = 1 \mod 11$
  - $7 * 8 = 1 \mod 11$
  - $7^{-1} \pmod{11} = 8$
- What is $11^{-1} \pmod{23}$?
  - $GCD(11, 23) = (1, -2, 1)$
  - $(-2) \cdot 11 + (1) \cdot 23 = 1$
  - $11 * (-2) = 1 \mod 23$

Example: Modular Multiplicative Inverses

- What is $7^{-1} \pmod{11}$?
  - $GCD(7, 11) = (1, -3, 2)$
  - $(-3) \cdot 7 + (2) \cdot 11 = 1$
  - $7 * (-3) = 1 \mod 11$
  - $7 * 8 = 1 \mod 11$
  - $7^{-1} \pmod{11} = 8$
- What is $11^{-1} \pmod{23}$?
  - $GCD(11, 23) = (1, -2, 1)$
  - $(-2) \cdot 11 + (1) \cdot 23 = 1$
  - $11 * (-2) = 1 \mod 23$
  - $11 * 21 = 1 \mod 23$

Example: Modular Multiplicative Inverses

- What is $7^{-1} \pmod{11}$?
  - $GCD(7, 11) = (1, -3, 2)$
  - $(-3) \cdot 7 + (2) \cdot 11 = 1$
  - $7 * (-3) = 1 \mod 11$
  - $7 * 8 = 1 \mod 11$
  - $7^{-1} \pmod{11} = 8$
- What is $11^{-1} \pmod{23}$?
  - $GCD(11, 23) = (1, -2, 1)$
  - $(-2) \cdot 11 + (1) \cdot 23 = 1$
  - $11 * (-2) = 1 \mod 23$
  - $11 * 21 = 1 \mod 23$
  - $11^{-1} \pmod{23} = 21$

Exercises: Modular Multiplicative Inverses

- Online calculator: https://jnalanko.net/eea/index.html
- What is $5^{-1} \pmod{11}$?
  - $GCD(5, 11) = (1, -2, 1)$
  - $(-2) \cdot 5 + 1 \cdot 11 = 1$

Exercises: Modular Multiplicative Inverses

- Online calculator: https://jnalanko.net/eea/index.html
- What is $5^{-1} \pmod{11}$?
  - $GCD(5, 11) = (1, -2, 1)$
  - $(-2) \cdot 5 + 1 \cdot 11 = 1$
  - 9
- What is $11^{-1} \pmod{19}$?
  - $GCD(11, 19 = (1, 7, -4)$
  - $7 \cdot 11 + (-4) \cdot 19 = 1$

Exercises: Modular Multiplicative Inverses

- Online calculator: https://jnalanko.net/eea/index.html
- What is $5^{-1} \pmod{11}$?
  - $GCD(5, 11) = (1, -2, 1)$
  - $(-2) \cdot 5 + 1 \cdot 11 = 1$
  - 9
- What is $11^{-1} \pmod{19}$?
  - $GCD(11, 19 = (1, 7, -4)$
  - $7 \cdot 11 + (-4) \cdot 19 = 1$
  - 7

Outline

Readings and References

- Chapter 8.1.7, 8.2.1, 8.5.2 in *Introduction to Computer Security*, by Goodrich and Tamassia.

Acknowledgments

Additional material and exercises have also been collected from these sources:

1. Igor Crk and Scott Baker, *620—Fall 2003—Basic Cryptography*.
2. William Stallings, *Cryptography and Network Security*.
3. Bruce Schneier, *Applied Cryptography*.
4. Neal R. Wagner, *The Laws of Cryptography with Java Code*, http://amadousarr.free.fr/java/javacryptobook.pdf.
5. *Euler's Totient Function Values For n = 1 to 500, with Divisor Lists*, http://primefan.tripod.com/Phi500.html
6. Diffie-Hellman calculator: http://dkerr.home.mindspring.com/diffie_hellman_calc.html.