Modular Arithmetic

Dr. Chuck Rocca
roccac@wcsu.edu
http://sites.wcsu.edu/roccac

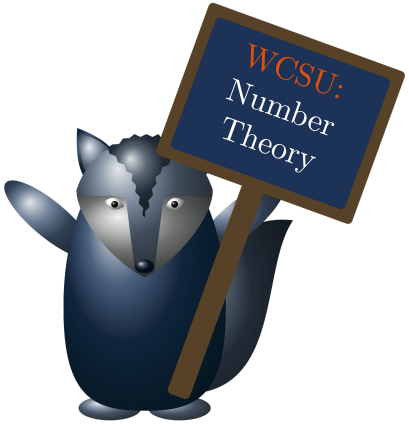
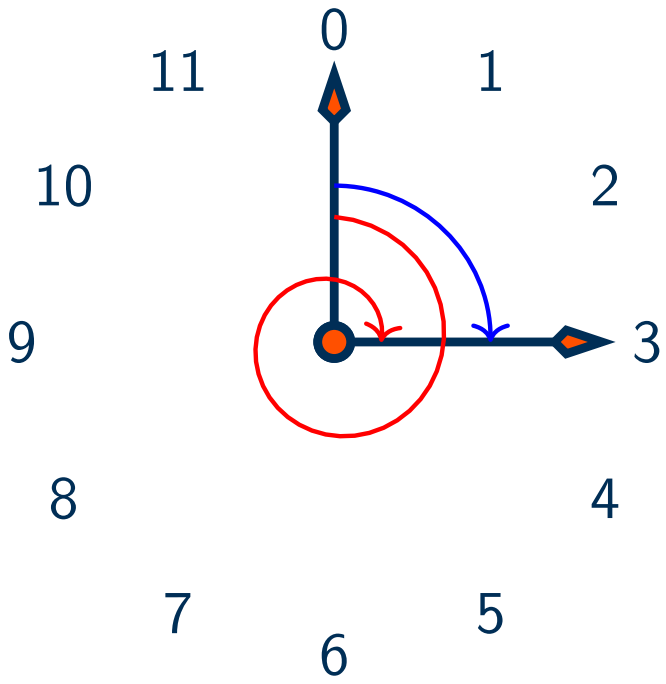


Table of Contents

Modular Equivalence

Definition 1

Two numbers a and b are equivalent modulo n if $|b - a|$ is a multiple of n.



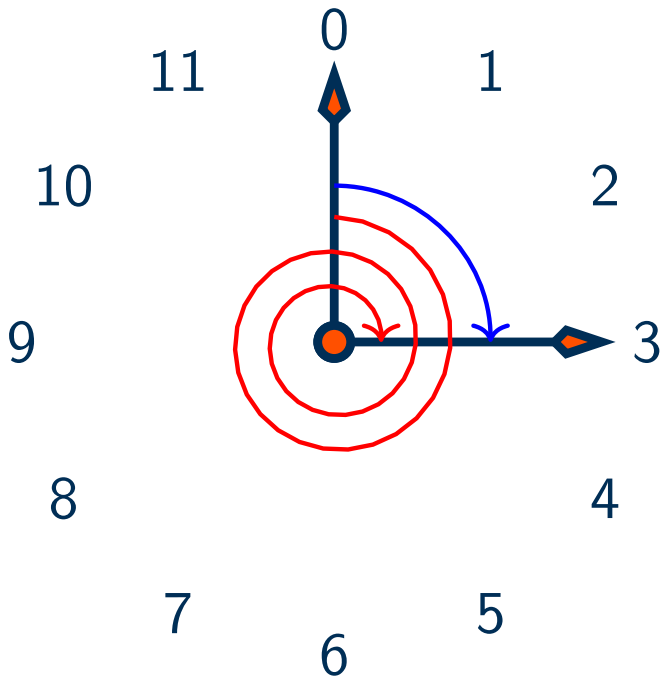
Consider the 12 hour clock on the left:

- $3 \equiv 15 \pmod{12}$ because $15 - 3 = 12$

Modular Equivalence

Definition 1

Two numbers a and b are equivalent modulo n if $|b - a|$ is a multiple of n.



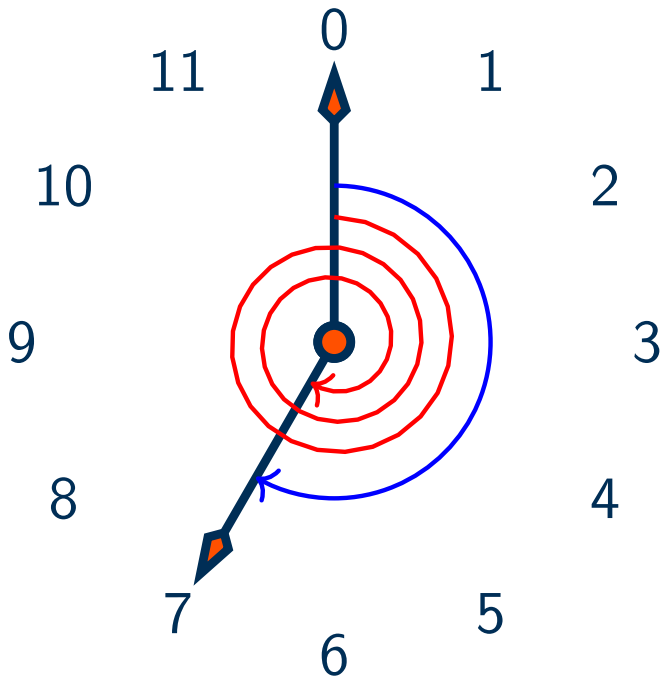
Consider the 12 hour clock on the left:

- $3 \equiv 15 \pmod{12}$ because $15 - 3 = 12$
- $3 \equiv 27 \pmod{12}$ because $27 - 3 = 2 \cdot 12$

Modular Equivalence

Definition 1

Two numbers a and b are equivalent modulo n if $|b - a|$ is a multiple of n.



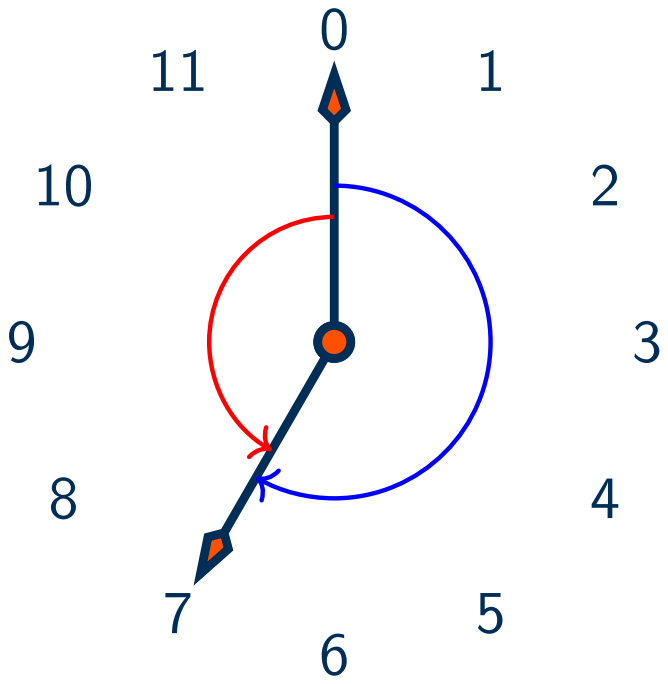
Consider the 12 hour clock on the left:

- $3 \equiv 15 \pmod{12}$ because $15 - 3 = 12$
- $3 \equiv 27 \pmod{12}$ because $27 - 3 = 2 \cdot 12$
- $7 \equiv 31 \pmod{12}$ because $31 - 7 = 2 \cdot 12$

Modular Equivalence

Definition 1

Two numbers a and b are equivalent modulo n if $|b - a|$ is a multiple of n.



Consider the 12 hour clock on the left:

- $3 \equiv 15 \pmod{12}$ because $15 - 3 = 12$
- $3 \equiv 27 \pmod{12}$ because $27 - 3 = 2 \cdot 12$
- $7 \equiv 31 \pmod{12}$ because $31 - 7 = 2 \cdot 12$
- $7 \equiv -5 \pmod{12}$ because $7 - (-5) = 12$

Modular Arithmetic

Theorem 2

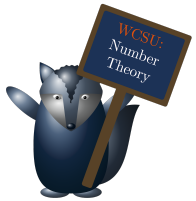
Given $n \in \mathbb{N}$ and $a, b, c, d \in \mathbb{Z}$, if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{N}$, then

$$\begin{aligned} a + c &\equiv b + d \pmod{n} \\ a - c &\equiv b - d \pmod{n} \\ ac &\equiv bd \pmod{n} \end{aligned}$$

Arithmetic Modulo 7

$+_7$	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

$\times_7$	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



Arithmetic Modulo 10

$+_{10}$	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

$\times_{10}$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Proof Modular Arithmetic is Well-Defined

Proof of Theorem 2.

Let $n \in \mathbb{N}$ and $a, b, c, d \in \mathbb{Z}$, let $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. By definition, $a - b = q_1 n$ and $c - d = q_2 n$ so that

$$(a + c) - (b + d) = (q_1 + q_2)n;$$

thus

$$a + c \equiv b + d \pmod{n}.$$

$\square$

Proof Modular Arithmetic is Well-Defined

Proof of Theorem 2.

Let $n \in \mathbb{N}$ and $a, b, c, d \in \mathbb{Z}$, let $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. By definition, $a - b = q_1 n$ and $c - d = q_2 n$ so that

$$(ac) - (bd) = (a - b)c + (c - d)b = (q_1 c + q_2 b)n;$$

thus

$$ac \equiv bd \pmod{n}.$$

$\square$

Table of Contents

Identities, Inverses, and Zero Divisors

Definition 3

The additive identity is 0 because $a + 0 = 0 + a = a$ for any a. And, we say that a and b are additive inverses if $a + b = 0$.

Identities, Inverses, and Zero Divisors

Definition 3

The additive identity is 0 because $a + 0 = 0 + a = a$ for any a. And, we say that a and b are additive inverses if $a + b = 0$.

Definition 4

The multiplicative identity is 1 because $a \cdot 1 = 1 \cdot a = a$ for any a. And, we say that a and b are multiplicative inverses if $a \cdot b = 1$.

Identities, Inverses, and Zero Divisors

Definition 3

The additive identity is 0 because $a + 0 = 0 + a = a$ for any a. And, we say that a and b are additive inverses if $a + b = 0$.

Definition 4

The multiplicative identity is 1 because $a \cdot 1 = 1 \cdot a = a$ for any a. And, we say that a and b are multiplicative inverses if $a \cdot b = 1$.

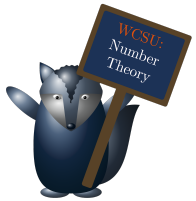
Definition 5

We say that $a \neq 0$ is a zero divisor if there exists $b \neq 0$ with $a \cdot b = 0$.

Arithmetic Modulo 7

$+_7$	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

$\times_7$	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



Arithmetic Modulo 7

$+_7$	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

$\times_7$	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

Arithmetic Modulo 10

$+_{10}$	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

$\times_{10}$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Arithmetic Modulo 10

$+_{10}$	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

$\times_{10}$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Bezout and Inverses

Theorem 6 (Bezout's Theorem)

Given $a, b \in \mathbb{Z}$, $d = (a, b)$ if and only if $d = ax + by$ is the least positive linear combination of a and b.

Bezout and Inverses

Theorem 6 (Bezout's Theorem)

Given $a, b \in \mathbb{Z}$, $d = (a, b)$ if and only if $d = ax + by$ is the least positive linear combination of a and b.

Theorem 7 (Modular Inverses)

Given $n \in \mathbb{N}$, $a \in \mathbb{Z}$, and $d = (a, n)$, a has a multiplicative inverse modulo n if $d = 1$, otherwise a is a zero divisor.

Proof of 7

Proof.

If $(a, n) = 1$, then by theorem 6, $ax + ny = 1$ and $ax \equiv 1 \pmod{n}$, i.e. $x \equiv a^{-1} \pmod{n}$.

$\square$

Proof of 7

Proof.

If $(a, n) = 1$, then by theorem 6, $ax + ny = 1$ and $ax \equiv 1 \pmod{n}$, i.e. $x \equiv a^{-1} \pmod{n}$.

Suppose $(a, n) = d \neq 1$, then by theorem 6, $ax + ny = d$. Let $q = n/d < n$, so that

$$aqx \equiv qd \equiv 0 \pmod{n},$$

i.e. a is a zero divisor. □

Comments on Some Equivalencies

Theorem 8

If $r_1, r_2, \ldots, r_n$ is a complete set of residues modulo n, $(a, n) = 1$, and $b \in \mathbb{Z}$ then

$$ar_1 + b, ar_2 + b, \ldots, ar_n + b$$

is also a complete set of residues.

Comments on Some Equivalencies

Theorem 9

If $a, b, k, m \in \mathbb{Z}$ with $k, m > 0$ and $a \equiv b \pmod{m}$, then

$$a^k \equiv b^k \pmod{m}.$$

Comments on Some Equivalencies

Theorem 9

If $a, b, k, m \in \mathbb{Z}$ with $k, m > 0$ and $a \equiv b \pmod{m}$, then

$$a^k \equiv b^k \pmod{m}.$$

Theorem 10

If $a, b, m_1, m_2, \ldots, m_k \in \mathbb{Z}$ with $m_i > 0$ and $a \equiv b \pmod{m_i}$ for all i, then

$$a \equiv b \pmod{[m_1, m_2, \ldots, m_k]}.$$

Table of Contents

Solving Linear Congruences

Theorem 11 (Solving Single Linear Congruences)

Let $n \in \mathbb{N}$, and $a, b, c \in \mathbb{Z}$, then

$$ax + b \equiv c \pmod{n},$$

has solution $x \equiv a^{-1}(c - b) \pmod{n}$ provided $a^{-1} \pmod{n}$ exists.

Congruences Modulo 7

Example 12

Find x such that $5x + 2 \equiv 1 \pmod 7$.

Congruences Modulo 7

Example 12

Find x such that $5x + 2 \equiv 1 \pmod 7$.
Modulo 7, $5^{-1} \equiv 3$, so we get

$$x \equiv 3(1 - 2) \equiv 4 \pmod 7.$$

Congruences Modulo 7

Example 12

Find x such that $5x + 2 \equiv 1 \pmod 7$.
Modulo 7, $5^{-1} \equiv 3$, so we get

$$x \equiv 3(1-2) \equiv 4 \pmod 7.$$

Check:

$$\begin{aligned} 5 \cdot 4 + 2 &= 22 \\ &\equiv 1 \pmod 7. \end{aligned}$$

Congruences Modulo 10

Example 13

Find x such that $3x + 2 \equiv 5 \pmod{10}$.

Congruences Modulo 10

Example 13

Find x such that $3x + 2 \equiv 5 \pmod{10}$.
Modulo 10, $3^{-1} \equiv 7$, so we get

$$x \equiv 7(5 - 2) \equiv 1 \pmod{10}.$$

Congruences Modulo 10

Example 13

Find x such that $3x + 2 \equiv 5 \pmod{10}$.
Modulo 10, $3^{-1} \equiv 7$, so we get

$$x \equiv 7(5-2) \equiv 1 \pmod{10}.$$

Check:

$$3 \cdot 1 + 2 \equiv 5 \pmod{10}.$$

Congruences Modulo 10

Example 14

Find x such that $2x + 3 \equiv 5 \pmod{10}$.

Congruences Modulo 10

Example 14

Find x such that $2x + 3 \equiv 5 \pmod{10}$.
Modulo 10, 2 doesn't have a multiplicative inverse, but we can easily see that $x = 1$ still works.

Congruences Modulo 10

Example 14

Find x such that $2x + 3 \equiv 5 \pmod{10}$.
Modulo 10, 2 doesn't have a multiplicative inverse, but we can easily see that $x = 1$ still works.

Example 15

Find x such that $2x \equiv 5 \pmod{10}$.

Congruences Modulo 10

Example 14

Find x such that $2x + 3 \equiv 5 \pmod{10}$.
Modulo 10, 2 doesn't have a multiplicative inverse, but we can easily see that $x = 1$ still works.

Example 15

Find x such that $2x \equiv 5 \pmod{10}$.
Modulo 10, 2 doesn't have a multiplicative inverse and in this case there is no solution.

Table of Contents

Affine Cipher: $\mathtt{C} \equiv m(M) + s \pmod{26}$

Algorithm

1. Key: m ,s # a multiplier and a shift
2. Message Character: M
3. Replace M with $\mathtt{C} \equiv m \cdot M + s \pmod{26}$
4. Repeat step 3 for each character

Arithmetic Modulo 26

$\times_{26}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	0	2	4	6	8	10	12	14	16	18	20	22	24	0	2	4	6	8	10	12	14	16	18	20	22	24
3	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23
4	0	4	8	12	16	20	24	2	6	10	14	18	22	0	4	8	12	16	20	24	2	6	10	14	18	22
5	0	5	10	15	20	25	4	9	14	19	24	3	8	13	18	23	2	7	12	17	22	1	6	11	16	21
6	0	6	12	18	24	4	10	16	22	2	8	14	20	0	6	12	18	24	4	10	16	22	2	8	14	20
7	0	7	14	21	2	9	16	23	4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19
8	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18
9	0	9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25	8	17
10	0	10	20	4	14	24	8	18	2	12	22	6	16	0	10	20	4	14	24	8	18	2	12	22	6	16
11	0	11	22	7	18	3	14	25	10	21	6	17	2	13	24	9	20	5	16	1	12	23	8	19	4	15
12	0	12	24	10	22	8	20	6	18	4	16	2	14	0	12	24	10	22	8	20	6	18	4	16	2	14
13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13
14	0	14	2	16	4	18	6	20	8	22	10	24	12	0	14	2	16	4	18	6	20	8	22	10	24	12
15	0	15	4	19	8	23	12	1	16	5	20	9	24	13	2	17	6	21	10	25	14	3	18	7	22	11
16	0	16	6	22	12	2	18	8	24	14	4	20	10	0	16	6	22	12	2	18	8	24	14	4	20	10
17	0	17	8	25	16	7	24	15	6	23	14	5	22	13	4	21	12	3	20	11	2	19	10	1	18	9
18	0	18	10	2	20	12	4	22	14	6	24	16	8	0	18	10	2	20	12	4	22	14	6	24	16	8
19	0	19	12	5	24	17	10	3	22	15	8	1	20	13	6	25	18	11	4	23	16	9	2	21	14	7
20	0	20	14	8	2	22	16	10	4	24	18	12	6	0	20	14	8	2	22	16	10	4	24	18	12	6
21	0	21	16	11	6	1	22	17	12	7	2	23	18	13	8	3	24	19	14	9	4	25	20	15	10	5
22	0	22	18	14	10	6	2	24	20	16	12	8	4	0	22	18	14	10	6	2	24	20	16	12	8	4
23	0	23	20	17	14	11	8	5	2	25	22	19	16	13	10	7	4	1	24	21	18	15	12	9	6	3
24	0	24	22	20	18	16	14	12	10	8	6	4	2	0	24	22	20	18	16	14	12	10	8	6	4	2
25	0	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Arithmetic Modulo 26

$\times_{26}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	0	2	4	6	8	10	12	14	16	18	20	22	24	0	2	4	6	8	10	12	14	16	18	20	22	24
3	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23
4	0	4	8	12	16	20	24	2	6	10	14	18	22	0	4	8	12	16	20	24	2	6	10	14	18	22
5	0	5	10	15	20	25	4	9	14	19	24	3	8	13	18	23	2	7	12	17	22	1	6	11	16	21
6	0	6	12	18	24	4	10	16	22	2	8	14	20	0	6	12	18	24	4	10	16	22	2	8	14	20
7	0	7	14	21	2	9	16	23	4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19
8	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18
9	0	9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25	8	17
10	0	10	20	4	14	24	8	18	2	12	22	6	16	0	10	20	4	14	24	8	18	2	12	22	6	16
11	0	11	22	7	18	3	14	25	10	21	6	17	2	13	24	9	20	5	16	1	12	23	8	19	4	15
12	0	12	24	10	22	8	20	6	18	4	16	2	14	0	12	24	10	22	8	20	6	18	4	16	2	14
13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13
14	0	14	2	16	4	18	6	20	8	22	10	24	12	0	14	2	16	4	18	6	20	8	22	10	24	12
15	0	15	4	19	8	23	12	1	16	5	20	9	24	13	2	17	6	21	10	25	14	3	18	7	22	11
16	0	16	6	22	12	2	18	8	24	14	4	20	10	0	16	6	22	12	2	18	8	24	14	4	20	10
17	0	17	8	25	16	7	24	15	6	23	14	5	22	13	4	21	12	3	20	11	2	19	10	1	18	9
18	0	18	10	2	20	12	4	22	14	6	24	16	8	0	18	10	2	20	12	4	22	14	6	24	16	8
19	0	19	12	5	24	17	10	3	22	15	8	1	20	13	6	25	18	11	4	23	16	9	2	21	14	7
20	0	20	14	8	2	22	16	10	4	24	18	12	6	0	20	14	8	2	22	16	10	4	24	18	12	6
21	0	21	16	11	6	1	22	17	12	7	2	23	18	13	8	3	24	19	14	9	4	25	20	15	10	5
22	0	22	18	14	10	6	2	24	20	16	12	8	4	0	22	18	14	10	6	2	24	20	16	12	8	4
23	0	23	20	17	14	11	8	5	2	25	22	19	16	13	10	7	4	1	24	21	18	15	12	9	6	3
24	0	24	22	20	18	16	14	12	10	8	6	4	2	0	24	22	20	18	16	14	12	10	8	6	4	2
25	0	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Arithmetic Modulo 26

$\times_{26}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	0	2	4	6	8	10	12	14	16	18	20	22	24	0	2	4	6	8	10	12	14	16	18	20	22	24
3	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23
4	0	4	8	12	16	20	24	2	6	10	14	18	22	0	4	8	12	16	20	24	2	6	10	14	18	22
5	0	5	10	15	20	25	4	9	14	19	24	3	8	13	18	23	2	7	12	17	22	1	6	11	16	21
6	0	6	12	18	24	4	10	16	22	2	8	14	20	0	6	12	18	24	4	10	16	22	2	8	14	20
7	0	7	14	21	2	9	16	23	4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19
8	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18
9	0	9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25	8	17
10	0	10	20	4	14	24	8	18	2	12	22	6	16	0	10	20	4	14	24	8	18	2	12	22	6	16
11	0	11	22	7	18	3	14	25	10	21	6	17	2	13	24	9	20	5	16	1	12	23	8	19	4	15
12	0	12	24	10	22	8	20	6	18	4	16	2	14	0	12	24	10	22	8	20	6	18	4	16	2	14
13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13
14	0	14	2	16	4	18	6	20	8	22	10	24	12	0	14	2	16	4	18	6	20	8	22	10	24	12
15	0	15	4	19	8	23	12	1	16	5	20	9	24	13	2	17	6	21	10	25	14	3	18	7	22	11
16	0	16	6	22	12	2	18	8	24	14	4	20	10	0	16	6	22	12	2	18	8	24	14	4	20	10
17	0	17	8	25	16	7	24	15	6	23	14	5	22	13	4	21	12	3	20	11	2	19	10	1	18	9
18	0	18	10	2	20	12	4	22	14	6	24	16	8	0	18	10	2	20	12	4	22	14	6	24	16	8
19	0	19	12	5	24	17	10	3	22	15	8	1	20	13	6	25	18	11	4	23	16	9	2	21	14	7
20	0	20	14	8	2	22	16	10	4	24	18	12	6	0	20	14	8	2	22	16	10	4	24	18	12	6
21	0	21	16	11	6	1	22	17	12	7	2	23	18	13	8	3	24	19	14	9	4	25	20	15	10	5
22	0	22	18	14	10	6	2	24	20	16	12	8	4	0	22	18	14	10	6	2	24	20	16	12	8	4
23	0	23	20	17	14	11	8	5	2	25	22	19	16	13	10	7	4	1	24	21	18	15	12	9	6	3
24	0	24	22	20	18	16	14	12	10	8	6	4	2	0	24	22	20	18	16	14	12	10	8	6	4	2
25	0	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Affine Cipher: $\mathtt{C} \equiv m(M) + s \pmod{26}$

Algorithm

1. Key: m ,s # a multiplier and a shift
2. Message Character: M
3. Replace M with $\mathtt{C} \equiv m \cdot M + s \pmod{26}$
4. Repeat step 3 for each character

Key Alphabet with Multiplier of m=7 and s=4

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
plain	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
CIPHER	E	L	S	Z	G	N	U	B	I	P	W	D	K	R	Y	F	M	T	A	H	O	V	C	J	Q	X

Affine Cipher: $\mathtt{C} \equiv m(M) + s \pmod{26}$

Algorithm

1. Key: m ,s # a multiplier and a shift
2. Message Character: M
3. Replace M with $\mathtt{C} \equiv m \cdot M + s \pmod{26}$
4. Repeat step 3 for each character

Key Alphabet with Multiplier of m=7 and s=4

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
plain	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
CIPHER	E	L	S	Z	G	N	U	B	I	P	W	D	K	R	Y	F	M	T	A	H	O	V	C	J	Q	X

$$7 \cdot \text{“d”} + 4 = 7 \cdot 3 + 4 = 25 \equiv 25 \pmod{26} \text{ (or C=“Z”)}$$

Affine Cipher: $\mathtt{C} \equiv m(M) + s \pmod{26}$

Algorithm

1. Key: m ,s # a multiplier and a shift
2. Message Character: M
3. Replace M with $\mathtt{C} \equiv m \cdot M + s \pmod{26}$
4. Repeat step 3 for each character

Key Alphabet with Multiplier of m=7 and s=4

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
plain	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
CIPHER	E	L	S	Z	G	N	U	B	I	P	W	D	K	R	Y	F	M	T	A	H	O	V	C	J	Q	X

$$7 \cdot \text{“m”} + 4 = 7 \cdot 12 + 4 = 88 \equiv 10 \pmod{26} \text{ (or } \mathtt{C}\text{=“K”)}$$

Affine Cipher: $\mathtt{C} \equiv m(M) + s \pmod{26}$

Algorithm

1. Key: m ,s # a multiplier and a shift
2. Message Character: M
3. Replace M with $\mathtt{C} \equiv m \cdot M + s \pmod{26}$
4. Repeat step 3 for each character

Key Alphabet with Multiplier of m=7 and s=4

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
plain	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
CIPHER	E	L	S	Z	G	N	U	B	I	P	W	D	K	R	Y	F	M	T	A	H	O	V	C	J	Q	X

$$7 \cdot \text{“p”} + 4 = 7 \cdot 15 + 4 = 109 \equiv 5 \pmod{26} \text{ (or } \mathtt{C}\text{=“F”)}$$

Inverting an Affine Cipher

Invert the Cipher

Given

$$C = m \cdot M + s$$

Inverting an Affine Cipher

Invert the Cipher

Given

$$\mathtt{C} = m \cdot M + s$$

we can solve for $\mathtt{C}$:

$$m \cdot M + s = \mathtt{C} \Rightarrow m \cdot M = \mathtt{C} - s$$

Inverting an Affine Cipher

Invert the Cipher

Given

$$C = m \cdot M + s$$

we can solve for C:

$$\begin{aligned} m \cdot M + s = C &\Rightarrow m \cdot M = C - s \\ &\Rightarrow M = m^{-1}(C - s) \end{aligned}$$

Inverting an Affine Cipher

Invert the Cipher

Given

$$C = m \cdot M + s$$

we can solve for C:

$$\begin{aligned} m \cdot M + s = C &\Rightarrow m \cdot M = C - s \\ &\Rightarrow M = m^{-1}(C - s) \\ &\Rightarrow M = m^{-1}C - m^{-1}s \end{aligned}$$

Inverting an Affine Cipher

Invert the Cipher

Given

$$C = m \cdot M + s$$

we can solve for C:

$$\begin{aligned} m \cdot M + s = C &\Rightarrow m \cdot M = C - s \\ &\Rightarrow M = m^{-1}(C - s) \\ &\Rightarrow M = m^{-1}C - m^{-1}s \end{aligned}$$

so we have two expressions we can use to find M.

Deciphering: $M \equiv m^{-1}C - m^{-1}s \pmod{26}$

Algorithm using $M \equiv m^{-1}C - m^{-1}s \pmod{26}$

1. Key $= m$,s # a multiplier and a shift
2. Inverse Key $= m^{-1}$, $-s$ # mult. and add. inverses
3. Simplify Key: m^{-1}, $-m^{-1}s$
4. Cipher Character $= C$
5. Replace C with $M \equiv m^{-1}C + (-m^{-1}s) \pmod{26}$
6. Repeat step 5 for each cipher character

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "I"=8
5. $M \equiv 15 \cdot 8 + 18 \equiv 8 \pmod{26}$, M="i"
6. plain message = "i"
7. Next C="D"=3

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "I"=8
5. $M \equiv 15 \cdot 8 + 18 \equiv 8 \pmod{26}$, M="i"
6. plain message = "i"
7. Next C="D"=3

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "I"=8
5. $M \equiv 15 \cdot 8 + 18 \equiv 8 \pmod{26}$, M="i"
6. plain message = "i"
7. Next C="D"=3

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "I"=8
5. $M \equiv 15 \cdot 8 + 18 \equiv 8 \pmod{26}$, M="i"
6. plain message = "i"
7. Next C="D"=3

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "I"=8
5. $M \equiv 15 \cdot 8 + 18 \equiv 8 \pmod{26}$, M="i"
6. plain message = "i"
7. Next C="D"=3

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "I"=8
5. $M \equiv 15 \cdot 8 + 18 \equiv 8 \pmod{26}$, M="i"
6. plain message = "i"
7. Next C="D"=3

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "I"=8
5. $M \equiv 15 \cdot 8 + 18 \equiv 8 \pmod{26}$, M="i"
6. plain message = "i"
7. Next C="D"=3

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "D"=3
5. $M \equiv 15 \cdot 3 + 18 \equiv 11 \pmod{26}$, M="I"
6. plain message = "il"
7. Next C="G"=6

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "D"=3
5. $M \equiv 15 \cdot 3 + 18 \equiv 11 \pmod{26}$, M="I"
6. plain message = "il"
7. Next C="G"=6

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "D"=3
5. $M \equiv 15 \cdot 3 + 18 \equiv 11 \pmod{26}$, M="I"
6. plain message = "il"
7. Next C="G"=6

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "D"=3
5. $M \equiv 15 \cdot 3 + 18 \equiv 11 \pmod{26}$, M="I"
6. plain message = "il"
7. Next C="G"=6

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "G"=6
5. $M \equiv 15 \cdot 6 + 18 \equiv 4 \pmod{26}$, M="e"
6. plain message = "ile"
7. Next C="E"=4

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "G"=6
5. $M \equiv 15 \cdot 6 + 18 \equiv 4 \pmod{26}$, M="e"
6. plain message = "ile"
7. Next C="E"=4

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "G"=6
5. $M \equiv 15 \cdot 6 + 18 \equiv 4 \pmod{26}$, M="e"
6. plain message = "ile"
7. Next C="E"=4

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "G"=6
5. $M \equiv 15 \cdot 6 + 18 \equiv 4 \pmod{26}$, M="e"
6. plain message = "ile"
7. Next C="E"=4

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "E"=4
5. $M \equiv 15 \cdot 4 + 18 \equiv 0 \pmod{26}$, M="a"
6. plain message = "ilea"
7. Next C="T"=19

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "E"=4
5. $M \equiv 15 \cdot 4 + 18 \equiv 0 \pmod{26}$, M="a"
6. plain message = "ilea"
7. Next C="T"=19

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "E"=4
5. $M \equiv 15 \cdot 4 + 18 \equiv 0 \pmod{26}$, M="a"
6. plain message = "ilea"
7. Next C="T"=19

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "E"=4
5. $M \equiv 15 \cdot 4 + 18 \equiv 0 \pmod{26}$, M="a"
6. plain message = "ilea"
7. Next C="T"=19

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "T"=19
5. $M \equiv 15 \cdot 19 + 18 \equiv 17 \pmod{26}$, M="r"
6. plain message = "ilear"
7. Next C="R"=17

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "T"=19
5. $M \equiv 15 \cdot 19 + 18 \equiv 17 \pmod{26}$, M="r"
6. plain message = "ilear"
7. Next C="R"=17

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "T"=19
5. $M \equiv 15 \cdot 19 + 18 \equiv 17 \pmod{26}$, M="r"
6. plain message = "ilear"
7. Next C="R"=17

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "T"=19
5. $M \equiv 15 \cdot 19 + 18 \equiv 17 \pmod{26}$, M="r"
6. plain message = "ilear"
7. Next C="R"=17

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "H"=7
5. $M \equiv 15 \cdot 7 + 18 \equiv 19 \pmod{26}$, M="t"
6. plain message = "ilearnedlongagonevertowrestlewithapigyouget-dirtyandbesidesthepiglikesit"
7. final message = "I learned long ago, never to wrestle with a pig. You get dirty, and besides, the pig likes it."

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "H"=7
5. $M \equiv 15 \cdot 7 + 18 \equiv 19 \pmod{26}$, M="t"
6. plain message = "ilearnedlongagonevertowrestlewithapigyouget-dirtyandbesidesthepiglikesit"
7. final message = "I learned long ago, never to wrestle with a pig. You get dirty, and besides, the pig likes it."

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "H"=7
5. $M \equiv 15 \cdot 7 + 18 \equiv 19 \pmod{26}$, M="t"
6. plain message = "ilearnedlongagonevertowrestlewithapigyouget-dirtyandbesidesthepiglikesit"
7. final message = "I learned long ago, never to wrestle with a pig. You get dirty, and besides, the pig likes it."

Sample Deciphering

Deciphering with an Algorithm

Cipher Text: "IDGET RGZDY RUEUY RGVGT HYCTG AHDGC IHBEF IUQYO UGHZI THQER ZLGAI ZGAHB GFIUD IWGAI H"

1. Key: m=7, s=4
2. Inverse Key: $m^{-1} = 15$, $-s = -4 \equiv 22$
3. Simplified Key: $m^{-1} = 15$, $-m^{-1}s = 15 \cdot 22 \equiv 18$
4. C = "H"=7
5. $M \equiv 15 \cdot 7 + 18 \equiv 19 \pmod{26}$, M="t"
6. plain message = "ilearnedlongagonevertowrestlewithapigyouget-dirtyandbesidesthepiglikesit"
7. final message = "I learned long ago, never to wrestle with a pig. You get dirty, and besides, the pig likes it."

Table of Contents

Chinese Remainder Theorem

Theorem 16 (Chinese Remainder Theorem)

Given the set of linear equations

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ x &\equiv a_3 \pmod{n_3} \\ &\vdots \\ x &\equiv a_r \pmod{n_r}, \end{aligned}$$

provided the n_i are relatively prime, there exists a unique solution modulo $M = n_1 n_2 n_3 \cdots n_r$.

C.R.T. Proof

Proof.

Let $M = n_1 n_2 n_3 \cdots n_r$ and $M_i = M/n_i$. Since the n_i are relatively prime, $(M_i, n_i) = 1$ and we can calculate $M_i^{-1} \pmod{n_i}$.

$\square$

C.R.T. Proof

Proof.

Let $M = n_1 n_2 n_3 \cdots n_r$ and $M_i = M/n_i$. Since the n_i are relatively prime, $(M_i, n_i) = 1$ and we can calculate $M_i^{-1} \pmod{n_i}$. Then

$$x \equiv \sum a_i M_i M_i^{-1} \pmod{M},$$

is the desired solution.

$\square$

C.R.T. Proof

Proof.

Let $M = n_1 n_2 n_3 \cdots n_r$ and $M_i = M/n_i$. Since the n_i are relatively prime, $(M_i, n_i) = 1$ and we can calculate $M_i^{-1} \pmod{n_i}$. Then

$$x \equiv \sum a_i M_i M_i^{-1} \pmod{M},$$

is the desired solution. Note that $M_j \equiv 0 \pmod{n_i}$ if $i \neq j$ and $M_i M_i^{-1} \equiv 1 \pmod{n_i}$ so that $x \equiv a_i \pmod{n_i}$.

$\square$

C.R.T. Proof

Proof.

Let $M = n_1 n_2 n_3 \cdots n_r$ and $M_i = M/n_i$. Since the n_i are relatively prime, $(M_i, n_i) = 1$ and we can calculate $M_i^{-1} \pmod{n_i}$. Then

$$x \equiv \sum a_i M_i M_i^{-1} \pmod{M},$$

is the desired solution. Note that $M_j \equiv 0 \pmod{n_i}$ if $i \neq j$ and $M_i M_i^{-1} \equiv 1 \pmod{n_i}$ so that $x \equiv a_i \pmod{n_i}$. Finally if there existed two solutions x_1 and x_2 then theorem 10 ensures they are equal modulo M. $\square$

C.R.T. Example 1

$$x \equiv 3 \pmod{5}$$
$$x \equiv 1 \pmod{6}$$
$$x \equiv 2 \pmod{7}$$

C.R.T. Example 1

$$x \equiv 3 \pmod{5}$$
$$x \equiv 1 \pmod{6}$$
$$x \equiv 2 \pmod{7}$$
$$M = 210$$

C.R.T. Example 1

$$x \equiv 3 \pmod{5}$$
$$x \equiv 1 \pmod{6}$$
$$x \equiv 2 \pmod{7}$$
$$M = 210$$
$$M_1 = 42$$

C.R.T. Example 1

$$x \equiv 3 \pmod 5$$
$$x \equiv 1 \pmod 6$$
$$x \equiv 2 \pmod 7$$
$$M = 210$$
$$M_1 = 42$$
$$M_2 = 35$$

C.R.T. Example 1

$$x \equiv 3 \pmod{5}$$
$$x \equiv 1 \pmod{6}$$
$$x \equiv 2 \pmod{7}$$
$$M = 210$$
$$M_1 = 42$$
$$M_2 = 35$$
$$M_3 = 30$$

C.R.T. Example 1

$$x \equiv 3 \pmod 5$$
$$x \equiv 1 \pmod 6$$
$$x \equiv 2 \pmod 7$$
$$M = 210$$
$$M_1 = 42$$
$$M_2 = 35$$
$$M_3 = 30$$
$$M_1^{-1} \equiv 3 \pmod 5$$

C.R.T. Example 1

$$x \equiv 3 \pmod 5$$
$$x \equiv 1 \pmod 6$$
$$x \equiv 2 \pmod 7$$
$$M = 210$$
$$M_1 = 42$$
$$M_2 = 35$$
$$M_3 = 30$$
$$M_1^{-1} \equiv 3 \pmod 5$$
$$M_2^{-1} \equiv 5 \pmod 6$$

C.R.T. Example 1

$$x \equiv 3 \pmod 5$$
$$x \equiv 1 \pmod 6$$
$$x \equiv 2 \pmod 7$$
$$M = 210$$
$$M_1 = 42$$
$$M_2 = 35$$
$$M_3 = 30$$
$$M_1^{-1} \equiv 3 \pmod 5$$
$$M_2^{-1} \equiv 5 \pmod 6$$
$$M_3^{-1} \equiv 4 \pmod 7$$

C.R.T. Example 1

$$x \equiv 3 \pmod{5}$$
$$x \equiv 1 \pmod{6}$$
$$x \equiv 2 \pmod{7}$$
$$M = 210$$
$$M_1 = 42$$
$$M_2 = 35$$
$$M_3 = 30$$
$$M_1^{-1} \equiv 3 \pmod{5}$$
$$M_2^{-1} \equiv 5 \pmod{6}$$
$$M_3^{-1} \equiv 4 \pmod{7}$$

$$x \equiv \sum a_i M_i M_i^{-1} \pmod{M}$$

C.R.T. Example 1

$$x \equiv 3 \pmod 5$$
$$x \equiv 1 \pmod 6$$
$$x \equiv 2 \pmod 7$$
$$M = 210$$
$$M_1 = 42$$
$$M_2 = 35$$
$$M_3 = 30$$
$$M_1^{-1} \equiv 3 \pmod 5$$
$$M_2^{-1} \equiv 5 \pmod 6$$
$$M_3^{-1} \equiv 4 \pmod 7$$

$$\begin{aligned} x &\equiv \sum a_i M_i M_i^{-1} \pmod M \\ &\equiv 3 \cdot 42 \cdot 3 + 1 \cdot 35 \cdot 5 + 2 \cdot 30 \cdot 4 \pmod M \end{aligned}$$

C.R.T. Example 1

$$x \equiv 3 \pmod 5$$
$$x \equiv 1 \pmod 6$$
$$x \equiv 2 \pmod 7$$
$$M = 210$$
$$M_1 = 42$$
$$M_2 = 35$$
$$M_3 = 30$$
$$M_1^{-1} \equiv 3 \pmod 5$$
$$M_2^{-1} \equiv 5 \pmod 6$$
$$M_3^{-1} \equiv 4 \pmod 7$$

$$\begin{aligned} x &\equiv \sum a_i M_i M_i^{-1} \pmod M \\ &\equiv 3 \cdot 42 \cdot 3 + 1 \cdot 35 \cdot 5 + 2 \cdot 30 \cdot 4 \pmod M \\ &\equiv 378 + 175 + 240 \pmod M \end{aligned}$$

C.R.T. Example 1

$$x \equiv 3 \pmod 5$$
$$x \equiv 1 \pmod 6$$
$$x \equiv 2 \pmod 7$$
$$M = 210$$
$$M_1 = 42$$
$$M_2 = 35$$
$$M_3 = 30$$
$$M_1^{-1} \equiv 3 \pmod 5$$
$$M_2^{-1} \equiv 5 \pmod 6$$
$$M_3^{-1} \equiv 4 \pmod 7$$

$$\begin{aligned} x &\equiv \sum a_i M_i M_i^{-1} \pmod M \\ &\equiv 3 \cdot 42 \cdot 3 + 1 \cdot 35 \cdot 5 + 2 \cdot 30 \cdot 4 \pmod M \\ &\equiv 378 + 175 + 240 \pmod M \\ &\equiv 169 + -35 + 30 \pmod M \end{aligned}$$

C.R.T. Example 1

$$x \equiv 3 \pmod 5$$
$$x \equiv 1 \pmod 6$$
$$x \equiv 2 \pmod 7$$
$$M = 210$$
$$M_1 = 42$$
$$M_2 = 35$$
$$M_3 = 30$$
$$M_1^{-1} \equiv 3 \pmod 5$$
$$M_2^{-1} \equiv 5 \pmod 6$$
$$M_3^{-1} \equiv 4 \pmod 7$$

$$\begin{aligned} x &\equiv \sum a_i M_i M_i^{-1} \pmod M \\ &\equiv 3 \cdot 42 \cdot 3 + 1 \cdot 35 \cdot 5 + 2 \cdot 30 \cdot 4 \pmod M \\ &\equiv 378 + 175 + 240 \pmod M \\ &\equiv 169 + -35 + 30 \pmod M \\ &\equiv 163 \pmod M \end{aligned}$$

C.R.T. Example 1

$$x \equiv 3 \pmod 5$$
$$x \equiv 1 \pmod 6$$
$$x \equiv 2 \pmod 7$$
$$M = 210$$
$$M_1 = 42$$
$$M_2 = 35$$
$$M_3 = 30$$
$$M_1^{-1} \equiv 3 \pmod 5$$
$$M_2^{-1} \equiv 5 \pmod 6$$
$$M_3^{-1} \equiv 4 \pmod 7$$

$$\begin{aligned} x &\equiv \sum a_i M_i M_i^{-1} \pmod M \\ &\equiv 3 \cdot 42 \cdot 3 + 1 \cdot 35 \cdot 5 + 2 \cdot 30 \cdot 4 \pmod M \\ &\equiv 378 + 175 + 240 \pmod M \\ &\equiv 169 + -35 + 30 \pmod M \\ &\equiv 163 \pmod M \end{aligned}$$

Check:

$$163 \equiv 3 \pmod 5$$
$$163 \equiv 1 \pmod 6$$
$$163 \equiv 2 \pmod 7$$

C.R.T. Example 2

$$x \equiv 3 \pmod{6}$$
$$x \equiv 7 \pmod{10}$$

C.R.T. Example 2

$$x \equiv 3 \pmod{6}$$
$$x \equiv 7 \pmod{10}$$
$$x \equiv 1 \pmod{2}$$
$$x \equiv 0 \pmod{3}$$
$$x \equiv 1 \pmod{2}$$
$$x \equiv 2 \pmod{5}$$

C.R.T. Example 2

$$x \equiv 3 \pmod{6}$$
$$x \equiv 7 \pmod{10}$$
$$x \equiv 1 \pmod{2}$$
$$x \equiv 0 \pmod{3}$$
$$x \equiv 1 \pmod{2}$$
$$x \equiv 2 \pmod{5}$$
$$M = 30$$
$$M_1 = 15$$
$$M_2 = 10$$
$$M_3 = 6$$

C.R.T. Example 2

$$x \equiv 3 \pmod{6}$$
$$x \equiv 7 \pmod{10}$$
$$x \equiv 1 \pmod{2}$$
$$x \equiv 0 \pmod{3}$$
$$x \equiv 1 \pmod{2}$$
$$x \equiv 2 \pmod{5}$$

$$M = 30$$
$$M_1 = 15$$
$$M_2 = 10$$
$$M_3 = 6$$

$$M_1^{-1} \equiv 1 \pmod{2}$$
$$M_2^{-1} \equiv 1 \pmod{3}$$
$$M_3^{-1} \equiv 1 \pmod{5}$$

C.R.T. Example 2

$$x \equiv 3 \pmod{6}$$
$$x \equiv 7 \pmod{10}$$
$$x \equiv 1 \pmod{2}$$
$$x \equiv 0 \pmod{3}$$
$$x \equiv 1 \pmod{2}$$
$$x \equiv 2 \pmod{5}$$
$$M = 30$$
$$M_1 = 15$$
$$M_2 = 10$$
$$M_3 = 6$$

$$M_1^{-1} \equiv 1 \pmod{2}$$
$$M_2^{-1} \equiv 1 \pmod{3}$$
$$M_3^{-1} \equiv 1 \pmod{5}$$
$$\begin{aligned} x &\equiv \sum a_i M_i M_i^{-1} \pmod{M} \\ &= 1 \cdot 15 \cdot 1 + 0 \cdot 10 \cdot 1 + 2 \cdot 6 \cdot 1 \pmod{M} \\ &= 27 \pmod{M} \end{aligned}$$

C.R.T. Example 3

$$x \equiv 7 \pmod{15}$$
$$x \equiv 3 \pmod{21}$$
$$x \equiv 4 \pmod{35}$$

C.R.T. Example 3

$$x \equiv 7 \pmod{15}$$
$$x \equiv 3 \pmod{21}$$
$$x \equiv 4 \pmod{35}$$

$$x \equiv 1 \pmod{3}$$
$$x \equiv 2 \pmod{5}$$
$$x \equiv 0 \pmod{3}$$
$$x \equiv 3 \pmod{7}$$
$$x \equiv 4 \pmod{5}$$
$$x \equiv 4 \pmod{7}$$

Table of Contents

Modular Arithmetic

Dr. Chuck Rocca
roccac@wcsu.edu
http://sites.wcsu.edu/roccac