Number Theory

Blathnaid Sheridan

September 20, 2023

Number Theory

You will recall that we covered *Number Theory* in Year 1 and were primarily concerned with the **Euclidean Algorithm** and the **Extended Euclidean Algorithm** for finding the gcd between two integers and the (multiplicative) inverse of a number in a modular number system.

In this topic of mathematics for computer science we are interested in the integers

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$$

$\mathbb{Z}$ is closed under addition, subtraction, multiplication but not under division. This means that if you divide one integer by another you get a *fraction* (which is not an integer!).

Quotients

We dont talk about dividing integers and instead talk about *quotients* and *remainders*.
Recall; if a and b are any two integers where $a > b$ we can write

$$a = q(b) + r$$

where q is the **quotient**/how many times b divides into a, and r is the **remainder**.

Remainders

Given two integers a and b and $a > b$ such that

$$a = q(b) + r$$

then the remainder is always an integer less than b i.e. r lies in the set

$$\{0, 1, 2, 3, \ldots b - 1\}$$

Examples

Write the following integers in the form $a = q(b) + r$.
Recall that r is always a positive integer!

1. Let $a = 27$ and $b = 3$ then
$$27 = 9(3) + 0$$
so $q = 9$ and $r = 0$.
2. Let $a = 19$ and $b = 4$ then
$$19 = 4(4) + 3$$
so $q = 4$ and $r = 3$.
3. Let $a = -12$ and $b = 5$ then
$$-12 = -3(5) + 3$$
so $q = -3$ and $r = 3$. The remainder must always be **added**.

The following table gives q and r for different combinations of signs.

		Quotient	Remainder
a	b	q	r
-a	b	-(q+1)	b-r
a	-b	-q	r
-a	-b	q+1	b-r

Note: a and b are positive so $-a$ and $-b$ are negative.

Example

a	b	Quotient	Remainder
8	6	1	2
-8	6	-2	4
8	-6	-1	2
-8	-6	2	4

Euclidean Algorithm

Recall that we used the Euclidean Algorithm to find the **greatest common divisor** or **gcd** of any two integers.
Let a and $b \in \mathbb{Z}$ and $a > b$, then

$$a = q(b) + r$$

where $r < b$. Repeat the process of dividing the smaller number into the larger number and finding a remainder. The last non-zero remainder is the gcd.
*Always start with the largest number on the LHS and the smaller number in the brackets on the RHS.

Example - Euclidean Algorithm

Find the $gcd(2406, 654)$

$$2406 = 3(654) + 444$$
$$654 = 1(444) + 210$$
$$444 = 2(210) + 24$$
$$210 = 9(24) + 6$$
$$24 = 4(6) + 0$$

The $gcd(2406, 654) = 6$

Extended Euclidean Algorithm

Let $a, b \in \mathbb{Z}$, $a \neq 0, b \neq 0$ and $d = gcd(a, b)$. Then $\exists m, n \in \mathbb{Z}$ such that

$$am + bn = d = gcd(a, b)$$

To use the Extended Euclidean Algorithm, we must write Part 1 (Euclidean Algorithm) in reverse and then sub this into Part 2 (Extended Euclidean Algorithm)

Example - Extended Euclidean Algorithm

From above, given $gcd(2406, 654) = 6$ find integers m and n such that

$$2406m + 654n = 6.$$

1. Rewrite Part 1

$$2406 - 3(654) = 444$$

$$654 - 1(444) = 210$$

$$444 - 2(210) = 24$$

$$210 - 9(24) = 6$$

2. Start on the last line and sub in each remainder:

$$1(210) - 9(24) = 6$$

$$1(210) - 9\{444 - 2(210)\} = 6$$

$$19(210) - 9(444) = 6$$

$$19\{654 - 1(444)\} - 9(444) = 6$$

$$19(654) - 28(444) = 6$$

$$19(654) - 28\{2406 - 3(654)\} = 6$$

$$103(654) - 28(4206) = 6$$

3. Hence $m = -28$ and $n = 103$.

Exercise

1. Use the Euclidean Algorithm to find $d = gcd(16810, 424)$.
2. Use the Extended Euclidean Algorithm to find integers m and n such that

$$16810m + 424n = d = gcd(16810, 424).$$

Diophantine Equations

More generally, an equation of the form

$$ax + by = c$$

where a, b, c and d are integers, is called a **Diophantine Equation**.

- We assume that a, b, c, d are non-zero.
- We are only interested in integer solutions.
- Solutions exist if and only if $gcd(a, b)$ divides into c.

Example - Diophantine Equations

Solve the Diophantine equation

$$243x + 198y = 9$$

1. First find $gcd(243, 198)$

$$243 = 1(198) + 45$$

$$198 = 4(45) + 18$$

$$45 = 2(18) + 9$$

Hence $gcd(243, 198) = 9$.

2. Are there solutions? **Yes!**
   There are solutions because $gcd(243, 198) = 9$ and 9 divides into the answer of the original equation 9 i.e. $9 \div 9 = 1$.
3. To find x and y we now use the Extended Euclidean Algorithm (by first reversing Part 1).

$$243 - 1(198) = 45$$

$$198 - 4(45) = 18$$

$$45 - 2(18) = 9$$

3. Starting on the last line, we rewrite

$$1(45) - 2(18) = 9$$

$$1(45) - 2\{198 - 4(45)\} = 9$$
$$9(45) - 2(198) = 9$$
$$9\{243 - 1(198)\} - 2(198) = 9$$
$$9(243) - 11(198) = 9$$

4. So $x = 9$ and $y = -11$ are solutions to the equation

$$243x + 198y = 9.$$

Diophantine Equations

Before solving a Diophantine equation you should divide out any common factors. For example,

$$670x + 322y = 42$$

instead divide across by 2 and solve

$$335x + 161y = 21.$$

Diophantine Equations

Sometimes the right-hand side of

$$ax + by = c$$

wont be exactly equal to the $gcd(a, b)$. There are two possibilities:

- If $gcd(a, b)$ does **not** divide c,then **no solutions exist**.
- If $gcd(a, b)$ is a factor of c, then you multiply the answers for x and y by this factor.

Example - Diophantine Equation

Solve the Diophantine equation

$$696x + 1247y = 87$$

1. First find $gcd(696, 1247)$.

$$1247 = 1(696) + 551$$

$$696 = 1(551) + 145$$

$$551 = 3(145) + 116$$

$$145 = 1(116) + 29$$

   So $gcd(696, 1247) = 29$

2. Check if this gcd divides into the answer (87). Yes!
   $87 \div 29 = 3$. Hence we will **multiply** our answers by 3 at the end.

3. Rewrite Part 1

$$1247 - 1(696) = 551$$

$$696 - 1(551) = 145$$

$$551 - 3(145) = 116$$

$$145 - 1(116) = 29$$

4. Find x and y

$$1(145) = 1(116) = 29$$

$$4(145) - 1(551) = 29$$

$$4(696) - 5(551) = 29$$

$$9(696) - 5(1247) = 29$$

5. So $x_0 = 9$ and $y_0 = -5$ are solutions to

$$1247x + 696y = 29.$$

6. Since $3 \times 29 = 87$ then $3x_0$ and $3y_0$ are solutions to

$$1247x + 696y = 87.$$

7. Hence $3x_0 = 27$ and $3y_0 = -15$ are solutions to

$$1247x + 696y = 87.$$

Modular Arithmetic

Let a and $b \in \mathbb{Z}$. We say that *a is congruent to b modulo n* written

$$a \equiv b(mod\ n)$$

if n divides into $(a - b)$.
So $\mathbb{Z}_n$ is the set of integers $= \{0, 1, 2, 3, 4, 5 \dots (n-1)\}$.

$$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$$

$$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$$

$$\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

Examples

1. $5 + 8 \equiv 1 \ (mod 12)$
2. $5 \times 8 = 40 \equiv 4 \ (mod 12)$
3. $5^3 = 25 \times 5 \equiv 1 \times 5 = 5 \ (mod 12)$

Inverses in $\mathbb{Z}_n$

We have seen how to add and multiply mod n. We will now look investigate the existence of **inverses** mod n.

- The inverse of an integer is *another* integer that you can multiply it by to get 1 mod n. i.e.
  The inverse of a is x because

$$ax \equiv 1 \ (mod n)$$

  In this case, we call x the **inverse** of a and denote it by a^{-1}.

Modular Arithmetic

Let $a, b, n \in \mathbb{Z}$ then we say that **a is congruent to b modulo n** if n divides into the difference $(a - b)$. If so, we write

$$a \equiv b(mod\ \ n).$$

Otherwise

$$a \not\equiv b(mod\ \ n).$$

We usually shorten modulo to *mod*.
Example:

$$17 \equiv 5(mod\ \ 4)$$

because $17 - 5 = 12$ and 12 is divisible by 4.

We can interpret congruence in another way. If $a \equiv b(mod\ \ n)$ then $\exists m \in \mathbb{Z}$ such that

$$a - b = nm.$$

Since $a, b \in \mathbb{Z}$, the division theorem says

$$a = nq_1 + r_1,\ 0 \leq r_1 < n$$

$$b = nq_2 + r_2,\ 0 \leq r_2 < n$$

Then

$$a - b = n(q_1 - q_2) + (r_1 - r_2).$$

This tells us that the quotient and remainder are unique mod n.

Modular Exponentiation

We often need to calculate congruences of powers of numbers which may be impossible to calculate on a calculator. Other approaches are needed. For example

$$7^{40}(mod\ 9)$$

The first thing to note is that $a^b(mod\ c)$ has a value between 0 and $c-1$.Lets calculate some values and see what is going on. We will use the example above $7^{40(mod\ 9)}$.

$$7^0 \equiv 1(mod\ 9)$$

$$7^1 \equiv 7(mod\ 9)$$

$$7^2 = 49 \equiv 4(mod\ 9)$$

$$7^3 = 343 \equiv 1(mod\ 9)$$

$$7^4 = 2401 \equiv 7(mod\ 9)$$

$$7^5 = 16807 \equiv 4(mod\ 9)$$

Notice the repeating pattern. We will see that this always happens. If we arrive at a power p where $a^p \equiv 1(mod)$, then the values will repeat from then on.

- $$\begin{aligned}(3+7)mod\ 3 &\equiv (3mod\ 3 + 7mod\ 3)\\ &\equiv (0+1)mod\ 3\\ &\equiv 1(mod\ 3)\\ &= 1\end{aligned}$$

- $$\begin{aligned}(3\times 7)mod\ 4 &\equiv (3mod\ 4 \times 7mod\ 4)\\ &\equiv (3\times 3)mod\ 4\\ &\equiv 9(mod\ 4)\\ &= 1\end{aligned}$$

Example

Calculate

$$7^{41} (mod\ 9).$$

$$7^1 \equiv 7 (mod\ 9)$$
$$7^2 = 49 \equiv 4 (mod\ 9)$$
$$7^3 = 343 \equiv 1 (mod\ 9)$$

We use rules of powers to see that

$$7^{41} = 7^2 \cdot 7^{39}$$

Further

$$7^{41} = 7^2 \cdot (7^3)^{13}$$

Hence

$$7^{41} (mod\ 9) \equiv 49 \cdot (1)^{13} (mod\ 9)$$
$$7^{41} = 4 \cdot 1 (mod\ 9)$$
$$7^{41} \equiv 4 (mod\ 9).$$

Thus, one way to calculate $a^b(mod\ n)$ is to calculate small powers of a until you arrive at some power k for which

$$a^k \equiv 1(mod\ n)$$

and use the remainder theorem to write

$$b = q(k) + r$$

when

$$\begin{aligned} a^b(mod\ n) &\equiv a^{qk+r}(mod\ n) \\ &\equiv ((a^k mod)^q(a^r mod\ n)) \\ &\equiv a^r(mod\ n) \end{aligned}$$

The only problem with this approach is that we have no idea which value will ever give us an answer of 1. Suppose we want

$$(1397)^{634}(mod\ 317)$$

We don't have any idea what value k satisfies

$$1397^k \equiv (mod\ 317)$$

Fast Exponentiation

This technique is a quicker way to find powers of an integer ($mod\ n$).

1. Express the power you want to find in binary i.e. Successive division by 2.
2. This will inform exactly which powers you need to calculate to find the answer.

Example - Fast Exponentiation

Calculate $3^{10}(mod\ 11)$.

1. Divide the power (10) by 2 to convert it to binary, to get
$$1010 = (1 \times 2^3) + (0 \times 2^2) + (1 \times 2^1) + (0 \times 2^0) = 8 + 2$$
2. Hence we will use the powers
$$10 = 8 \times 2$$
3. $$3^{10}(mod\ 11) \equiv 3^8 3^2 (mod\ 11)$$
4. $$3^1 \equiv 3(mod\ 11)$$
$$3^2 \equiv 9(mod\ 11)$$
Square this answer to get
$$3^4 = (9)^2 = 81 \equiv 4(mod\ 11)$$
Square this answer to get
$$3^8 = (4)^2 = 16 \equiv 5(mod\ 11)$$

Cont'

5. Put these two powers of 3 together to get

$$3^{10}(mod\ 11) \equiv 3^8 3^2 (mod\ 11)$$

$$3^{10}(mod\ 11) \equiv (9) \cdot (5) = 45(mod\ 11)$$
$$\equiv 1(mod\ 11)$$

Exercise - Fast Exponentiation

Calculate

$$2^{644} (mod\ 645).$$

using fast exponentiation.

1. In binary $644 = 1010000100 = 512 + 128 + 4$. These are the powers we need to find i.e.

$$2^{644} = 2^{512} \cdot 2^{128} \cdot 2^{4}$$

2. Calculate all powers $2^1 \equiv 2(mod 645), 2^2 \equiv 4(mod 645), \ldots 2^{256} \equiv 16(mod 645), 2^{512} \equiv 256(mod 645)$.
3. $$2^{644} = 2^{512} \cdot 2^{128} \cdot 2^{4}$$

$$2^{644} = 256 \cdot 39 \cdot 16 (mod\ 645)$$

$$2^{644} \equiv 1 (mod\ 645).$$

Exercise

Calculate

$$91^{239} (mod\ 6731)$$

1. $239 = 11101111_2$
2. $239 = 128 + 64 + 32 + 8 + 4 + 2 + 1$
3. Calculate these powers
4. $$91^{239} \equiv 1970 (mod\ 6731)$$

Fermat's Little Theorem (FLT)

You may recall from last year that Fermat's Little Theorem can be used to find the *inverse* of an integer in a modular number system.

Fermat's Little Theorem (FLT)

If p is prime and a is an integer (with a not divisible by p) then

$$a^{(p-1)} \equiv 1(mod\ p)$$

FLT - Example

Show that $2^{(340)} \equiv 1(mod\ 11)$.
Note that in this question the prime $p = 11$.

$$340 = 10 \cdot (34)$$

$$2^{340} = \left(2^{(10)}\right)^{(34)}$$

FLT tells that $2^{10} \equiv 1(mod 11)$

$$2^{340} = (1)^{34} = 1(mod\ 11)$$

FLT - Example

Calculate $31^{5323905}(mod\ 1039)$ given that 1039 is prime.
Since 1039 is a prime number, we can use FLT.
Note that $1039 - 1 = 1038$ and so we divide our power 5323905 by 1038 to get

$$5323905 = (1038)(5129) + 3$$

$$31^{5323905} = \left(31^{(1038)}\right)^{5129} \cdot 31^3$$

FLT gives $31^{1038} \equiv 1(mod\ 1039)$ since 31 does not divide into 1039.

$$31^{5323905} \equiv (1)^{5129} \cdot 31^3(mod\ 1039)$$

$$31^{5323905} \equiv 29791(mod\ 1039)$$

$$31^{5323905} \equiv 699$$

Inverses

An integer x is the inverse, mod n, of an integer a if

$$ax \equiv 1(mod\ \ n)$$

We usually denote the inverse of a by a^{-1}.
Example: Find the inverse of $3(mod\ 5)$.
Since the mod is small, we can use trial and error.
Mod 5= $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ so we try each of these possibilities:

$$3(0) \not\equiv 1(mod\ 5)$$

$$3(1) = 3 \not\equiv 1(mod\ 5)$$

$$3(2) = 6 \equiv 1(mod\ 5)$$

This means that

$$3^{-1} = 2(mod\ 5)$$

Exercises

1. $3^{-1}(mod\ 7)$ (You can use FLT here because the mod is prime.)
2. $5^{-1}(mod\ 7)$ (You can use FLT here because the mod is prime.)

Finding Inverses in Mods which are **not** prime

How do we find the inverse of an integer a in $(mod\ \ n)$ when n is **not** a prime number?
We use Euclid's Algorithm!
Recall that if we have

$$ax \equiv b(mod\ \ n)$$

we can rewrite this as a Diophantine Equation

$$ax - ny = b$$

for some integer y, using Euclid's Algorithm and the Extended Euclidean Algorithm.

Example

Solve $81x \equiv 1 (mod\ 256)$
This is equivalent to

$$81x - 256y = 1 \text{ (Diophantine)}$$

1. $$256 = 3(81) + 13$$
$$81 = 6(13) + 3$$
$$13 = 4(3) + 1$$

So $gcd(256, 81) = 1$

Cont'

2. Reverse Part 1 and start on the bottom line

$$256 - 3(81) = 13$$

$$81 - 6(13) = 3$$

$$13 - 4(3) = 1$$

3.

$$1(13) - 4(3) = 1$$

$$1(13) - 4\{81 - 6(13)\} = 25(13) - 4(81) = 1$$

$$25\{256 - 3(81)\} - 4(81) = 25(256) - 79(81) = 1$$

4. Since we are working (mod 256), the solution is $x = -79$ and this gives $x = -79 \equiv 177(mod\ 256)$.
   So
   $$x = 177$$

Hill Digraph Cipher

This cipher splits the plaintext into blocks consisting of **pairs** of characters. Each block is then encrypted using a (2×2) matrix to produce the ciphertext. If the plaintext has an odd length, then a random character is added to the end.

We will restrict ourselves to encrypting plaintext consisting of just the letters $A, B, \ldots Z$ (all uppercase). Recall that $A = 0, B = 1, C = 2, \ldots Z = 25$.

You may need to revise how to:

1. Multiply two matrices,
2. Find the inverse of a (2×2) matrix.

Hill Digraph Cipher - Encrypting

Suppose we want to encrypt the plaintext message **"TUD"** using the encryption matrix

$$\begin{pmatrix} 5 & 3 \\ 2 & 1 \end{pmatrix}$$

We break the plaintext into blocks of 2 letters i.e. $T \quad U$ and $D \quad \mathbf{X}$
We add on the characted **X** at the end to balance up the matrix sizes (you can add any character you wish!) so we can multiply the matrices.
We construct a **column** matrix for each pair and multiply by the encrypting matrix reducing the results *mod* 26 (or whatever the number of characters in the set is).

Cont'

We get

$$\begin{pmatrix} 5 & 3 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 19 \\ 20 \end{pmatrix} = \begin{pmatrix} 155 \\ 58 \end{pmatrix} \equiv \begin{pmatrix} 26(mod\ 26) \\ 6(mod\ 26) \end{pmatrix} = \begin{pmatrix} Z \\ G \end{pmatrix}$$

$$\begin{pmatrix} 5 & 3 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 3 \\ 23 \end{pmatrix} = \begin{pmatrix} 84 \\ 29 \end{pmatrix} \equiv \begin{pmatrix} 6(mod\ 26) \\ 3(mod\ 26) \end{pmatrix} = \begin{pmatrix} G \\ D \end{pmatrix}$$

So

- Plaintext "TUDX"
- Ciphertext "ZGGD"

Hill Digraph Cipher - Decryption

In order to use the Hill Digraph cipher to decrypt ciphertext, we need to know how to find the **modular** inverse of a (2×2) matrix. For example, if A is a matrix then the modular inverse of A is the matrix A^{-1} satisfying

$$A \cdot A^{-1} = I(mod\ \ n)$$

To find the modular inverse of a matrix A i.e. To find $A^{-1}(mod\ \ n)$ simply find the usual inverse i.e. A^{-1} and reduce everything modulo n.

Modular Inverse of a (2×2) matrix

- Given a matrix

  $$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

  then

  $$A^{-1} = \frac{1}{(ad - bc)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

  Since fractions do not exist in modular number systems, we need to change the $\frac{1}{(ad-bc)}$ into an integer. To do this, we use that fact that if

  $$k \cdot \frac{1}{k} = 1 \text{ then } \frac{1}{k} = k^{-1} (mod\ n)$$

Modular Inverse of a (2×2) matrix

If

$$A = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}$$

then find $A^{-1}(mod\ 5)$ and show that $A \cdot A^{-1} = I(mod\ 5)$.

- $det(A) = (3)(1) - (2)(2) = -1$
- We need to find the inverse of $-1(mod\ 5)$ i.e. $-1x \equiv 1(mod\ 5)$. Reduce this down to $4x \equiv 1(mod\ 5)$. So $x = 4$ since $4 \times 4 = 16 \equiv 1(mod\ 5)$
- So
$$A^{-1} = 4\begin{pmatrix} 1 & -2 \\ -2 & 3 \end{pmatrix} = \begin{pmatrix} 4 & -8 \\ -8 & 12 \end{pmatrix}(mod\ 5) = \begin{pmatrix} 4 & 2 \\ 2 & 2 \end{pmatrix}(mod\ 5)$$
- Check:
$$AA^{-1} = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 4 & 2 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Example

If

$$A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$$

then find $A^{-1}(mod\ 26)$.
<u>Solution:</u>

- $$A^{-1} = \frac{1}{(16-21)} \begin{pmatrix} 8 & -3 \\ -7 & 2 \end{pmatrix}$$
- We need $(-5)^{-1}(mod\ 26) \equiv (21)^{-1}(mod\ 26)$ i.e.

$$21x \equiv 1(mod\ 26)$$

Cont'

- Euclid Part 1

$$26 = 1(21) + 5$$

$$21 = 4(5) + 1$$

So the $gcd(21, 26) = 1$ and this congruence equation has a solution.

- Euclid Part 2

$$1(21) - 4(5) = 1$$

$$1(21) - 4\{(26 - 1(21))\}$$

$$5(21) - 4(26) = 1$$

Hence $x = 5$ is the inverse of $21(mod\ 26)$.

- Hence

$$A^{-1} = 5\begin{pmatrix} 8 & -3 \\ -7 & 2 \end{pmatrix}(mod\ 26) = \begin{pmatrix} 40 & -15 \\ -35 & 10 \end{pmatrix}(mod\ 26) = \left(\begin{matrix} 14 & 1 \\ 17 & 1 \end{matrix}\right.$$

Con't

- Hence

$$A^{-1} = 5 \begin{pmatrix} 8 & -3 \\ -7 & 2 \end{pmatrix} (mod\ 26) = \begin{pmatrix} 40 & -15 \\ -35 & 10 \end{pmatrix} (mod\ 26)$$

$$= \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} (mod\ 26)$$

- Check

$$A \cdot A^{-1} = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (mod\ 26)$$

Hill Digraph Cipher - Decryption

Recover the plaintext given the ciphertext "$ZGGD$" which was encrypted using the matrix

$$\begin{pmatrix} 5 & 3 \\ 2 & 1 \end{pmatrix}.$$

- Find

$$A^{-1} = \frac{1}{(5)(1) - (3)(2)} \begin{pmatrix} 1 & -3 \\ -2 & 5 \end{pmatrix} = -1 \begin{pmatrix} 1 & -3 \\ -2 & 5 \end{pmatrix} \equiv \begin{pmatrix} 25 & 3 \\ 2 & 21 \end{pmatrix} ($$

$$= \begin{pmatrix} 25 & 3 \\ 2 & 21 \end{pmatrix} (mod\ 26)$$

Cont'

- Now decrypt $Z = 25, G = 6, G = 6, D = 3$.
- Form into matrices and multiply

$$\begin{pmatrix} 25 & 3 \\ 2 & 21 \end{pmatrix} \begin{pmatrix} 25 \\ 6 \end{pmatrix} = \begin{pmatrix} 643 \\ 176 \end{pmatrix} \equiv \begin{pmatrix} 19 \\ 20 \end{pmatrix} = \begin{pmatrix} T \\ U \end{pmatrix}$$

$$\begin{pmatrix} 25 & 3 \\ 2 & 21 \end{pmatrix} \begin{pmatrix} 6 \\ 3 \end{pmatrix} = \begin{pmatrix} 159 \\ 75 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 23 \end{pmatrix} = \begin{pmatrix} D \\ X \end{pmatrix}$$

- Hence the ciphertext "$ZGGD$" gives the plaintext "$TUDX$".

Exercise

The ciphertext "$WKFT$" was encrypted by means of a Hill Digraph Cipher using a matrix

$$\begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix}$$

modulo 26 where

$$A = 0, \; B = 1, \ldots Z = 25.$$

Find A^{-1} and hence retrieve the plaintext.

Solution

- $$A^{-1} = \frac{1}{5}\begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix}$$
- Need to find $5^{-1}(mod\ 26)$
$$5x \equiv 1(mod\ 26)$$
- Part 1
$$26 = 5(5) + 1$$
- Part 2
$$1(26) - 5(5) = 1$$

  So $x = -5$ is a solution to $5x \equiv 1(mod\ 26)$. Hence $x = 21(mod\ 26)$ is the inverse of $5(mod\ 26)$.

Cont'

- Therefore

$$A^{-1} = 21 \begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix} (mod\ 26)$$

$$= \begin{pmatrix} 42 & -21 \\ -63 & 84 \end{pmatrix} (mod\ 26) = \begin{pmatrix} 16 & 5 \\ 15 & 6 \end{pmatrix}$$

- Decrypting $W = 22, K = 10, F = 5, T = 19$. (Remember these go in as **columns**.

$$\begin{pmatrix} 16 & 5 \\ 15 & 6 \end{pmatrix} \begin{pmatrix} 22 & 5 \\ 10 & 19 \end{pmatrix} = \begin{pmatrix} 402 & 175 \\ 390 & 189 \end{pmatrix} = \begin{pmatrix} 12 & 19 \\ 0 & 7 \end{pmatrix}$$

$$\begin{pmatrix} M & T \\ A & H \end{pmatrix}$$

- Ciphertext "$WKFT$" gives plaintext "$MATH$".

Chinese Remainder Theorem

The Chinese Remainder Theorem is a theorem that enables us to solve systems of simultaneous congruence equations.
For example

$$x \equiv 2 (mod\ 3)$$

$$x \equiv 3 (mod\ 5)$$

$$x \equiv 2 (mod\ 7)$$

Chinese Remainder Theorem (CRT)

If $n_1, n_2, \ldots, n_k$ are pairwise coprime, then the system

$$x \equiv r_1 (mod \;\; n_1)$$
$$x \equiv r_2 (mod \;\; n_2)$$
$$\vdots$$
$$x \equiv r_n (mod \;\; n_n)$$

has a unique solution modulo $M = n_1 \cdot n_2 \ldots n_k$, given by

$$x = M_1 r_1 s_1 + M_2 r_2 s_2 + \ldots + M_k r_k s_k$$

where

$$M_1 = \frac{M}{n_1}, \;\; M_2 = \frac{M}{n_2}, \;\; \ldots M_k = \frac{M}{n_k},$$

and

$$s_1, s_2, \ldots s_k$$

are solutions to the equations

$$M_1 s_1 \equiv 1 (mod \;\; n_1), M_2 s_2 \equiv 1 (mod \;\; n_2), \ldots M_k s_k \equiv 1 (mod \;\; n_k),$$

Example CRT

Use the CRT to solve

$$x \equiv 2(mod\ 3)$$
$$x \equiv 4(mod\ 5)$$
$$x \equiv 6(mod\ 7)$$

Here $r_1 = 2,\ n_1 = 3, r_2 = 4,\ n_2 = 5, r_3 = 6,\ n_3 = 7$

$$M = (3)(5)(7) = 105$$

$$M_1 = \frac{105}{3} = 35,\ M_2 = \frac{105}{5} = 21, M_3 = \frac{105}{7} = 15$$

- To find s_1 we need to solve $35s_1 \equiv 1(mod\ 3)$.
  Reducing this down and testing all possible answers $(0, 1, 2)$ we get

  $$2s_1 \equiv 1(mod\ 3)$$

  .

  $$s_1 = 2$$

Cont'

- To find s_2 we need to solve $21s_1 \equiv 1(mod\ 5)$. Reducing this down and testing all possible answers $(0, 1, 2, 3, 4)$ we get

$$1s_2 \equiv 1(mod\ 5)$$

.

$$s_2 = 1$$

- To find s_3 we need to solve $15s_1 \equiv 1(mod\ 7)$. Reducing this down and testing all possible answers $(0, 1, 2, 3, 4, 5, 6)$ we get

$$1s_3 \equiv 1(mod\ 7)$$

.

$$s_3 = 1$$

Cont'

Putting this together we get the solution

$$x = M_1 r_1 s_1 + M_2 r_2 s_2 + \ldots + M_k r_k s_k$$

$$x = (35)(2)(2) + (21)(1)(4) + (15)(1)(6)(mod\ 105)$$

$$x = 314(mod\ 105)$$

$$x \equiv 104(mod\ 105)$$

Test it out!

Exercise

Use the CRT to solve

$$x \equiv 2(mod\ 3)$$

$$x \equiv 3(mod\ 5)$$

$$x \equiv 4(mod\ 11)$$

Solution:

$$x = (55)(2)(1) + (33)(3)(2) + (15)(4)(3)(mod\ 165)$$

$$x \equiv 158(mod\ 165)$$

Incongruent Solutions

In modular arithmetic, you cant just **cancel**! For example,

$$3(1) \equiv 3(5)(mod\ 6)$$

but

$$1 \not\equiv 5(mod\ 6).$$

Theorem 1: If $ab \equiv ac(mod\ n)$ and $gcd(a, n) = 1$, then

$$b \equiv c(mod\ n)$$

Theorem 2: If $ab \equiv ac(mod\ n)$ and $gcd(a, n) = d$, then

$$b \equiv c(mod\ \frac{n}{d})$$

Example

Suppose we have

$$6 \equiv 36 (mod\ 10).$$

Notice that 3 divides into 6 and 36 but that $gcd(3, 10) = 1$. Then by Theorem 1 we can write

$$2 \equiv 12 (mod\ 10).$$

However, if we again have

$$6 \equiv 36 (mod\ 10).$$

Notice that we **cannot** divide by 6 in this case because although 6 divides into 6 and into 36, the $gcd(6, 10) \neq 1$.
Theorem 2 tells us that we can get

$$1 \equiv 6 (mod\ 5).$$

Incongruent Solutions

Theorem 3: Let $ax \equiv b(mod\ n)$ with $d = gcd(a, n)$. Then

1. If $d \nmid b$ then $ax \equiv b(mod\ n)$ has **no solutions**.
2. If $d \mid b$ then $ax \equiv b(mod\ n)$ has **d** solutions which are *incongruent* modulo N to the unique solution of

$$AX \equiv B(mod\ N)$$

   where $A = \frac{a}{d}, B = \frac{b}{d}, N = \frac{n}{d}$.
   The d solutions are incongruent modulo n.

Example

Find all incongruent solutions of

$$119x \equiv 133 (mod\ 217)$$

<u>Solution:</u>

$$217 = 1(119) + 98$$

$$119 = 1(98) + 21$$

$$98 = 4(21) + 14$$

$$21 = 1(14) + 7$$

$$14 = 2(7) + 0$$

So $gcd(119, 217) = 7$ and since $7 \mid 133 = 7$ this means there are **7** incongruent solutions to $119x \equiv 133(mod\ 217)$.

Cont'

Since $gcd(119, 217) = 7$ and $7 \mid 133$ we can divide across by 7 to get

$$17x \equiv 19(mod\ 31)$$

1. Solve $17x \equiv 1(mod\ 31)$ $i.e.17x - 31y = 1.$
   1.1
   $$31 = 1(17) + 14$$
   $$17 = 1(14) + 3$$
   $$14 = 4(3) + 2$$
   $$3 = 1(2) + 1$$
   So $gcd(17, 31) = 1$ so a solution exists.
   1.2 Rewriting the remainders from Part 1:
   $$31 - 1(17) = 14$$
   $$17 - 1(14) = 3$$
   $$14 - 4(3) = 2$$
   $$3 - 1(2) = 1$$

Cont'

2.
$$1(3) - 1(2) = 1$$
$$5(3) - 1(14) = 1$$
$$5(17) - 6(14) = 1$$
$$11(17) - 6(31) = 1$$

So $x = 11$ and $y = -6$ is a solution of $17x \equiv 1(mod\ 31)$.

3. Secondly we multiply this answer by **19** to get a solution to the equation $17x \equiv 19(mod\ 31)$. Hence $x = 19(11) = 209 \equiv 23(mod\ 31)$

Cont'

4. The theorem above says that this answer of $x = 23$ is *also* a solution of the equation

$$119x \equiv 133(mod\ 217).$$

5. Hence the **7** incongruent solutions to $119x \equiv 133(mod\ 217)$ are:

$$23, (23 + 31), (23 + 2(31)), (23 + 3(31)), (23 + 4(31)),$$

$$(23 + 5(31)), (23 + 6(31))$$

$$\boxed{23, 54, 85, 116, 147, 178, 209.}$$