OneNote for Windows 10 — Blathnaid Sheridan

Quotients & Remainders

Write in the form $a = q(b) + r$

① Let $a = 27$ and $b = 3$

$$27 = 9(3) + 0$$

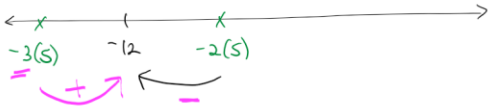
② Let $a = 19$ and $b = 4$

$$19 = 4(4) + 3$$

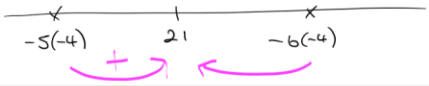
$q = 4$, $r = 3$

③ Let $a = -12$ and $b = 5$

$$-12 = -3(5) + 3$$



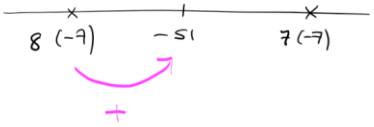
④ Let $a = 21$ and $b = -4$



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

⑤ Let $a = -51$ and $b = -7$

$$-51 = 8(-7) + 5$$



⑥

a	b	q	r
8	6	1	2
-8	6	-2	4
8	-6	-1	2
-8	-6	2	4

Euclidean Algorithm

① gcd(2406, 654)

R.W

Type here to search — 14°C — 08:47 09/10/2023

OneNote for Windows 10 — Blathnaid Sheridan

① gcd(2406, 654)

$2406 = 3(654) + 444$

$654 = 1(444) + 210$

$444 = 2(210) + 24$

$210 = 8(24) + 18$

$24 = 1(18) + 6$ → gcd

~~$18 = 3(6) + 0$~~

$\Rightarrow \boxed{\gcd(2406, 654) = 6}$

R.W

$2406 - 3(654) = 444$

$654 - 1(444) = 210$

$444 - 2(210) = 24$

$210 - 8(24) = 18$

$24 - 1(18) = 6$

Extended Euclidean Algorithm $2406m + 654n = 6$

* Put bracket around 24 and 1 outside bracket

② $1(24) - 1(18) = 6$

$1(24) - 1[210 - 8(24)] = 6$

$1(24) - 1(210) + 8(24) = 6$

Type here to search — 14°C — 08:47 09/10/2023

OneNote for Windows 10 — Blathnaid Sheridan

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

$9[444 - 2(210)] - 1(210) = 6$

$9(444) - 18(210) - 1(210) = 6$

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

$9(444) - 19[654 - 1(444)] = 6$

$9(444) - 19(654) + 19(444) = 6$

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

$28[2406 - 3(654)] - 19(654) = 6$

$28(2406) - 84(654) - 19(654) = 6$

$\boxed{28(2406) - 103(654) = 6}$

$m = 28$ $\quad n = -103$ $\quad d = \gcd$

Exercise

R.W

Type here to search — 14°C — 08:47 09/10/2023

OneNote for Windows 10 — Blathnaid Sheridan

Home Insert Draw View Help Share

Calibri Light 20 B I U Heading 1

Exercise

I $\gcd(16810, 424)$

$16810 = 39(424) + 274$

$424 = 1(274) + 150$

$274 = 1(150) + 124$

$150 = 1(124) + 26$

$124 = 4(26) + 20$

$26 = 1(20) + 6$

$20 = 3(6) + \boxed{2}$ → $\gcd = 2$

RW

$16810 - 39(424) = 274$ ✓

$424 - 1(274) = 150$ ✓

$274 - 1(150) = 124$ ✓

$150 - 1(124) = 26$ ✓

$124 - 4(26) = 20$ ✓

$26 - 1(20) = 6$ ✓

$20 - 3(6) = 2$ ✓

II $(16810)m + (424)n = 2$

$1(20) - 3(6) = 2$

$1(20) - 3[26 - 1(20)] = 4(20) - 3(26) = 2$

$4[124 - 4(26)] - 3(26) = 4(124) - 19(26) = 2$

Type here to search 14°C 08:47 09/10/2023

OneNote for Windows 10 — Blathnaid Sheridan

Home Insert Draw View Help Share

Calibri Light 20 B I U Heading 1

$4[124 - 4(26)] - 3(26) = 4(124) - 19(26) = 2$

$4(124) - 19[150 - 1(124)] = 23(124) - 19(150) = 2$

$23[274 - 1(150)] - 19(150) = 23(274) - 42(150) = 2$

$23(274) - 42[424 - 1(274)] = 65(274) - 42(424) = 2$

$65[16810 - 39(424)] - 42(424) = 65(16810) - 2577(424) = 2$

$m = 65$ $n = -2577$

Diophantine Equations

Solve the Diophantine Equation

$(243)x + (198)y = 9$

① find gcd

I $243 = 1(198) + 45$

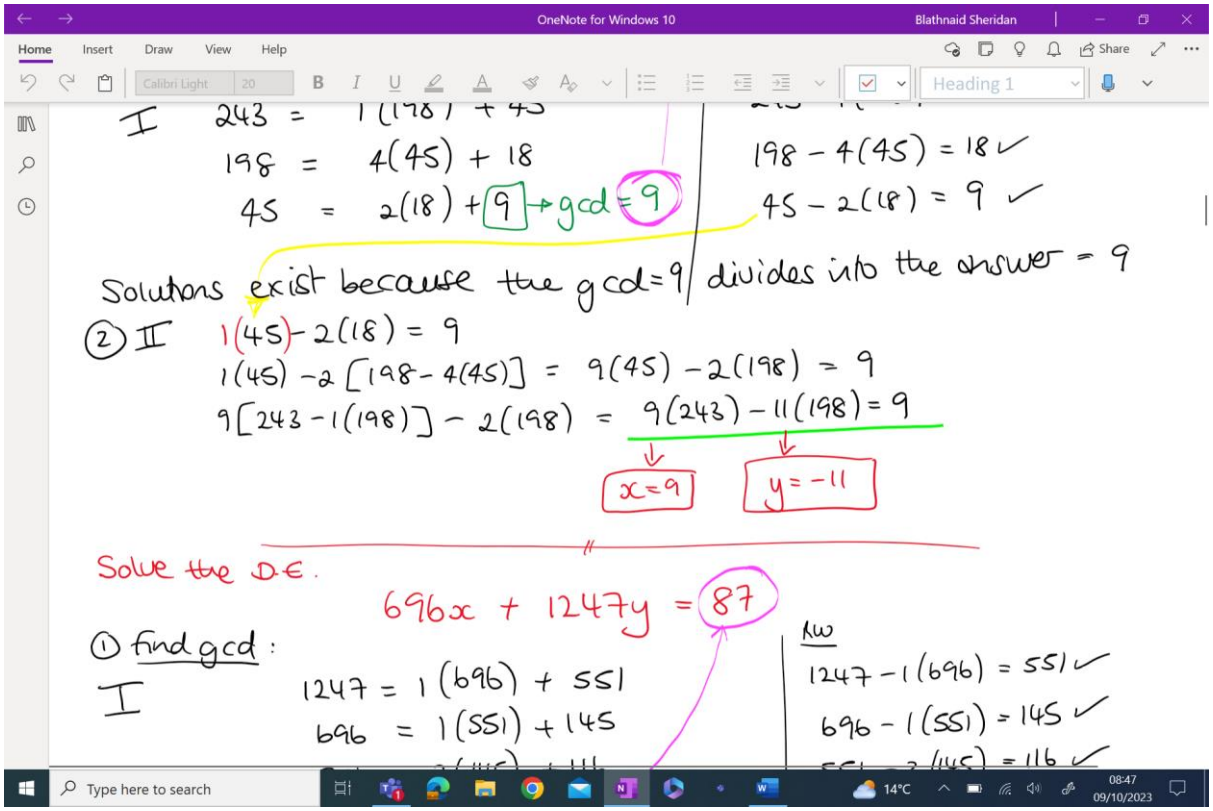
$198 = 4(45) + 18$

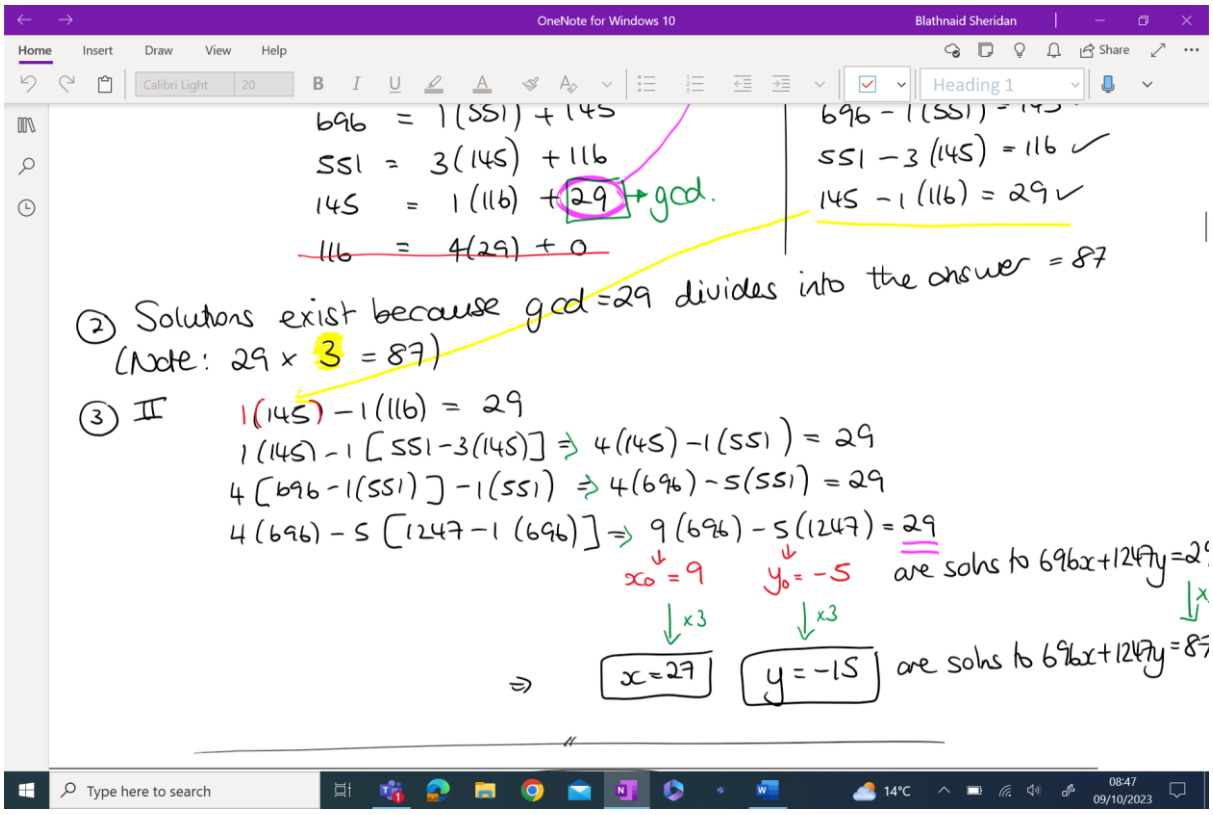
RW

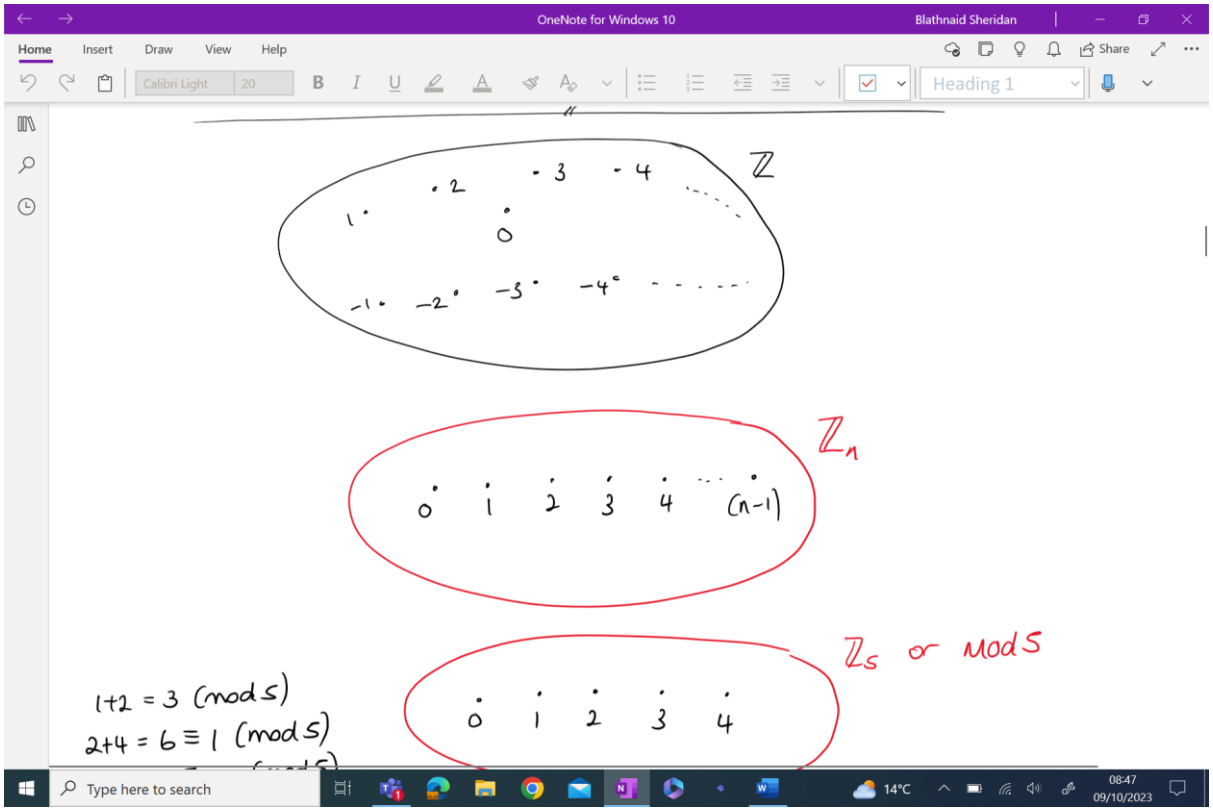
$243 - 1(198) = 45$ ✓

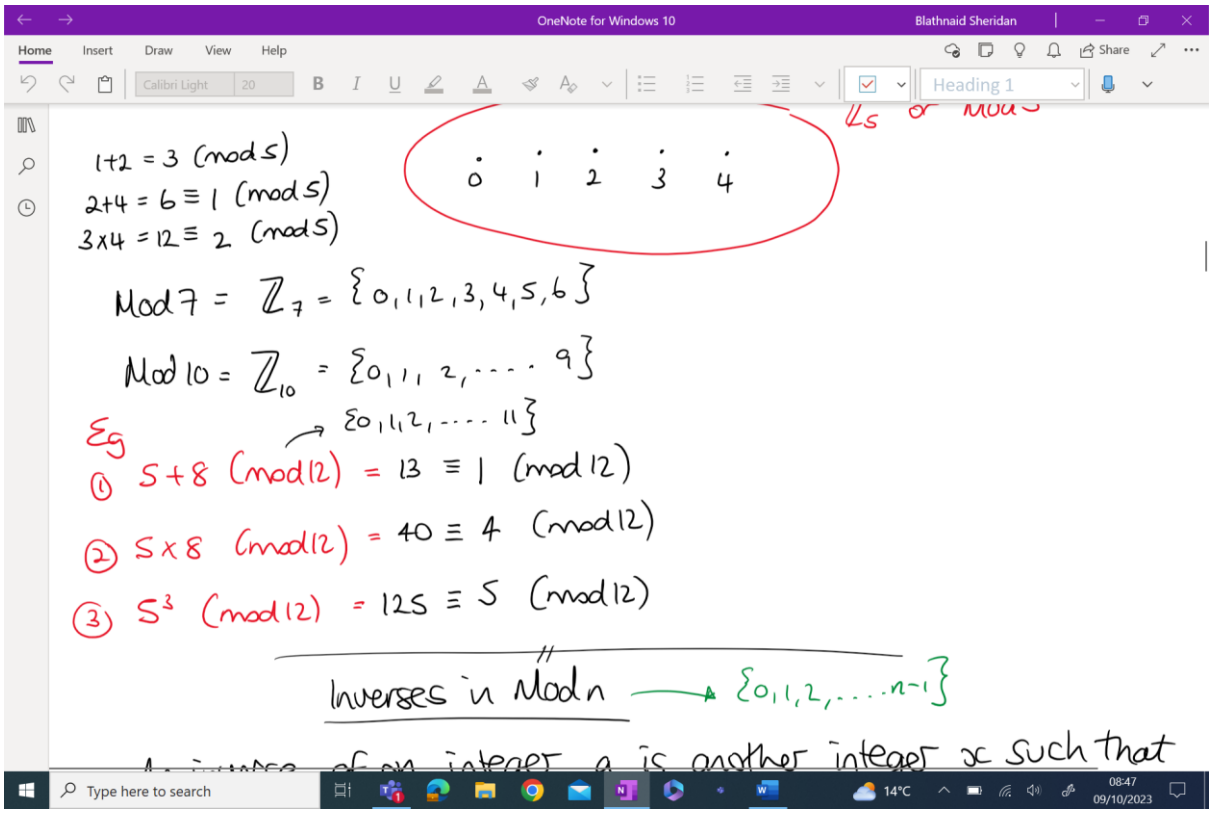
$198 - 4(45) = 18$ ✓

Type here to search 14°C 08:47 09/10/2023


OneNote for Windows 10
Blathnaid Sheridan
Home Insert Draw View Help
Heading 1
I
198 = 4(45) + 18
45 = 2(18) + 9 → gcd = 9
198 − 4(45) = 18 ✓
45 − 2(18) = 9 ✓
Solutions exist because the gcd = 9 divides into the answer = 9
② II 1(45) − 2(18) = 9
1(45) − 2[198 − 4(45)] = 9(45) − 2(198) = 9
9[243 − 1(198)] − 2(198) = 9(243) − 11(198) = 9
x = 9
y = −11
Solve the DE.
696x + 1247y = 87
① find gcd:
I
1247 = 1(696) + 551
696 = 1(551) + 145
Aw
1247 − 1(696) = 551 ✓
696 − 1(551) = 145 ✓
Type here to search
14°C
08:47
09/10/2023


OneNote for Windows 10
Blathnaid Sheridan
Home Insert Draw View Help
Heading 1
696 = 1(551) + 145
551 = 3(145) + 116
145 = 1(116) + 29 → gcd.
116 = 4(29) + 0
551 − 3(145) = 116 ✓
145 − 1(116) = 29 ✓
② Solutions exist because gcd = 29 divides into the answer = 87
(Note: 29 × 3 = 87)
③ II 1(145) − 1(116) = 29
1(145) − 1[551 − 3(145)] ⇒ 4(145) − 1(551) = 29
4[696 − 1(551)] − 1(551) ⇒ 4(696) − 5(551) = 29
4(696) − 5[1247 − 1(696)] ⇒ 9(696) − 5(1247) = 29
x₀ = 9
y₀ = −5
are solns to 696x + 1247y = 29
×3
×3
x = 27
y = −15
are solns to 696x + 1247y = 87
⇒
Type here to search
14°C
08:47
09/10/2023


OneNote for Windows 10
Blathnaid Sheridan
Home Insert Draw View Help
Heading 1
ℤ
1 2 3 4
0
-1 -2 -3 -4
$\mathbb{Z}_n$
0 1 2 3 4 (n-1)
$\mathbb{Z}_5$ or Mod 5
0 1 2 3 4
1+2 = 3 (mod 5)
2+4 = 6 ≡ 1 (mod 5)
Type here to search
14°C
08:47
09/10/2023


OneNote for Windows 10
Blathnaid Sheridan
Home Insert Draw View Help
Heading 1
$\mathbb{Z}_5$ or Mod 5
0 1 2 3 4
1+2 = 3 (mod 5)
2+4 = 6 ≡ 1 (mod 5)
3×4 = 12 ≡ 2 (mod 5)
Mod 7 = $\mathbb{Z}_7$ = {0,1,2,3,4,5,6}
Mod 10 = $\mathbb{Z}_{10}$ = {0,1,2,.... 9}
Eg → {0,1,2,.... 11}
① 5+8 (mod 12) = 13 ≡ 1 (mod 12)
② 5×8 (mod 12) = 40 ≡ 4 (mod 12)
③ 5^3 (mod 12) = 125 ≡ 5 (mod 12)
Inverses in Mod n → {0,1,2,....n-1}
Type here to search
14°C
08:47
09/10/2023

OneNote for Windows 10 — Blathnaid Sheridan

Home Insert Draw View Help — Share

Inverses in Mod n → $\{0,1,2,\ldots,n-1\}$

An inverse of an integer a is another integer x such that

$$ax \equiv 1 \pmod{n}$$

ie The 2 integers multiply to give 1 (mod n).
To find the inverse of any integer we use the Euclidean Algorithm.
We usually denote the inverse of a as a^{-1}.

- Let $a, b \in \mathbb{Z}$

elements of the integers.

The we write a is congruent to b modulo n if n divides into the difference $(a-b)$. If so, we write

$$a \equiv b \pmod{n}$$

Eg.

① $12 \equiv 7 \pmod{5}$ because $(12-7)=5$ which is divisible by 5.

② $17 \equiv 5 \pmod{4}$ because $(17-5)=12$ which is divisible by 4.

③ $12 \not\equiv 1 \pmod{10}$ because $(12-1)=11$ which is nor divisible by 10.

we can think of congruence equations in another way.

Type here to search — 14°C — 08:48 09/10/2023

We can think of congruence equations

If $a \equiv b \pmod{n}$

then $(a-b) = nm$

Eg. find the inverse of $41 \pmod{78}$

ie we want a number x such that

$$41x \equiv 1 \pmod{78}$$

we can write this congruence equation as a Diophantine Equation

$$41x - 78y = 1$$

we know we can use the Euclidean Algorithm to solve this

I $\gcd(41, 78)$

$78 = 1(41) + 37$ | RW $78 - 1(41) = 37$

$41 = 1(37) + 4$ | $41 - 1(37) = 4$

$41 = 1(37) + 4$ | $41 - 1(37) = 4$

$37 = 9(4) + 1 \rightarrow \gcd = 1$ | $37 - 9(4) = 1$

Solutions do exist because gcd = 1 divides into the answer = 1 ✓

II $1(37) - 9(4) = 1$

$1(37) - 9[41 - 1(37)] = 1$

$10(37) - 9(41) = 1$

$10[78 - 1(41)] - 9(41) = 1$

$10(78) - 19(41) = 1$ $\pmod{78}$ ... any multiple of $78 = 0 \pmod{78}$

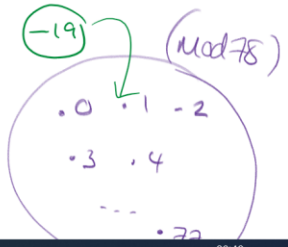
0

$(-19)(41) = 1 \pmod{78}$

$\Rightarrow$ The inverse of 41 is $-19 \pmod{78}$

$\Rightarrow$ $(41)^{-1} = -19 + 78 \pmod{78}$

$$(41)^{-1} = 59 \pmod{78}$$



OneNote for Windows 10 — Blathnaid Sheridan

Home Insert Draw View Help — Share

Calibri Light 20 — Heading 1

* check :

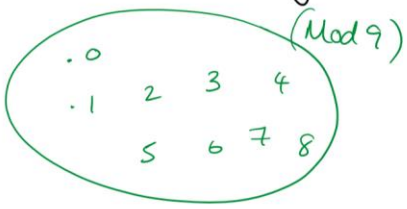
$(41)(59) = 2419 \pmod{78}$

$\equiv 1 \pmod{78}$ ✓

Modular Exponentiation

Means finding powers of integers in a modular number system.

e.g find $7^{40} \pmod 9$



$7^0 = 1 \pmod 9$

$7^1 = 7 \pmod 9$

$7^2 = 49 \equiv 4 \pmod 9$ (×7)

$7^3 = 343 \equiv 1 \pmod 9$ (×7)

$(7^2)(7) = 7^3$

$(7^3)(7) = 7^4$

4×7 = 28

$7^4 = 7 \pmod 9$

Type here to search — 14°C — 08:48 09/10/2023

OneNote for Windows 10 — Blathnaid Sheridan

Home Insert Draw View Help — Share

Calibri Light 20 — Heading 1

$7^5 = 49 \equiv 4 \pmod 9$

$7^6 = 28 \equiv 1 \pmod 9$ (×7)

There is a pattern here: $7^0\ 7^1\ 7^2\ 7^3\ 7^4\ 7^5\ 7^6\ 7^7$

1, 7, 4, 1, 7, 4, 1, 7, 4, ...

7^{40}

⇒ By counting up to the power of 40

⇒ $7^{40} = 7 \pmod 9$

* If you can find the power that gives an answer of 1, we can solve the question much quicker

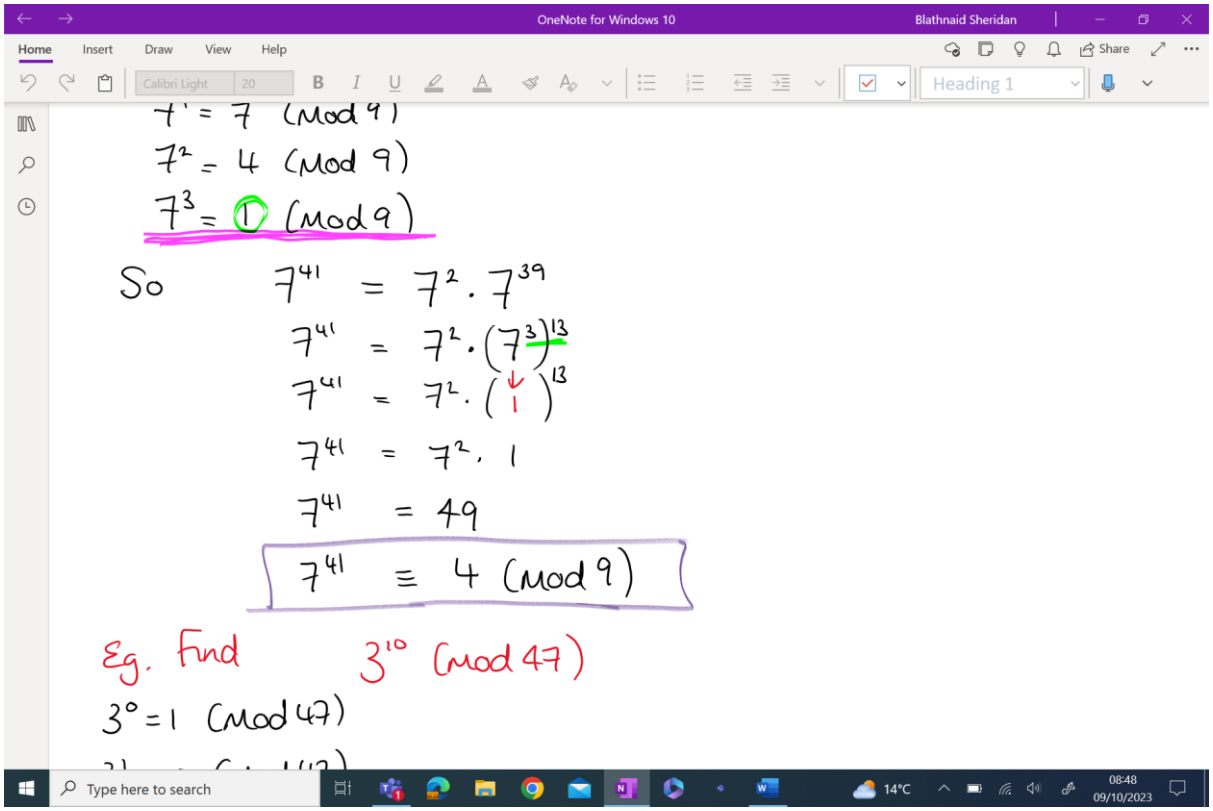
E.g find $7^{41} \pmod 9$

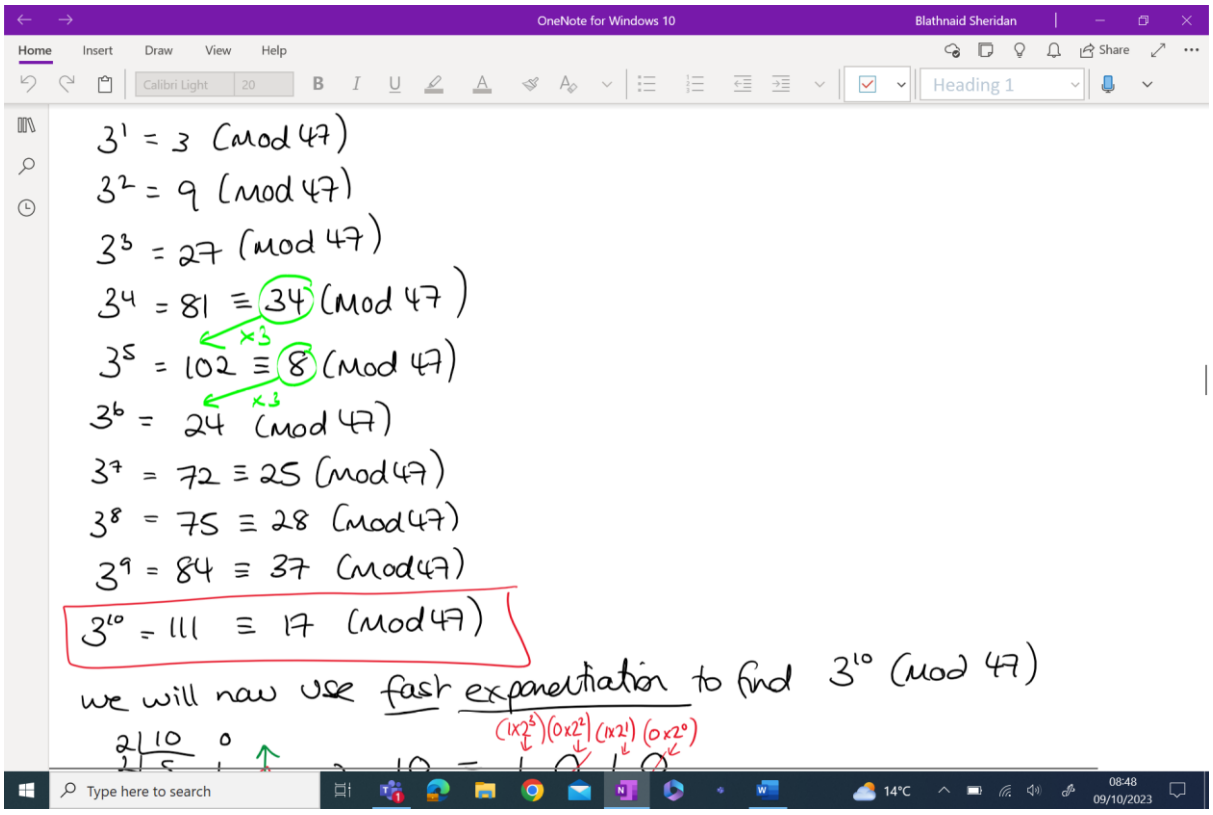
from above

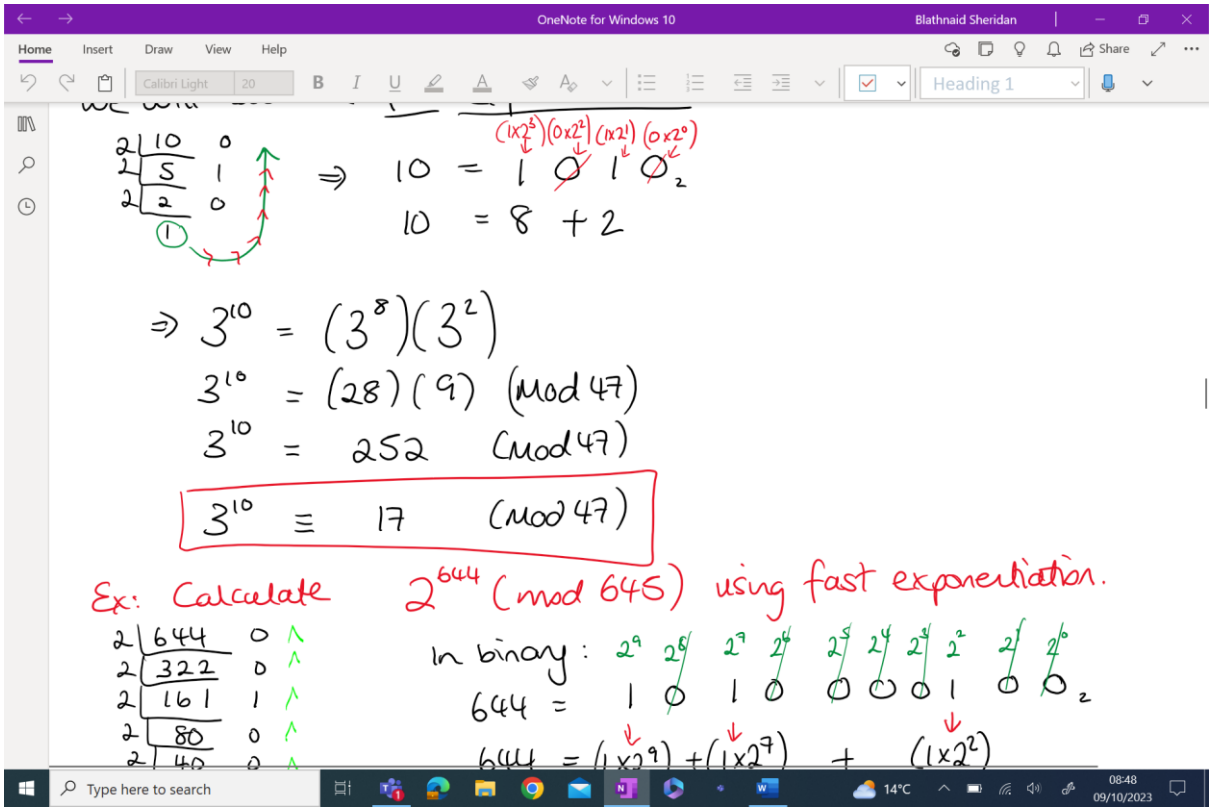
$7^0 = 1 \pmod 9$

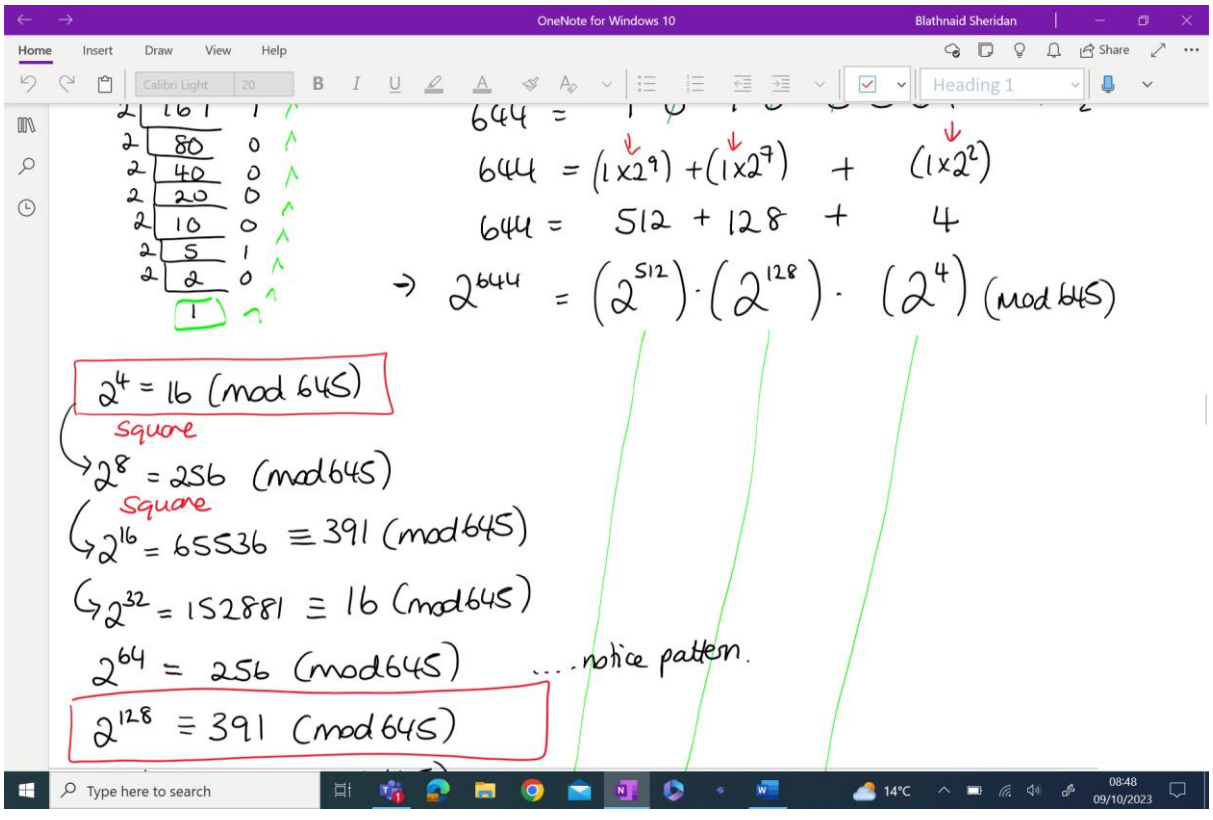
$7^1 = 7 \pmod 9$

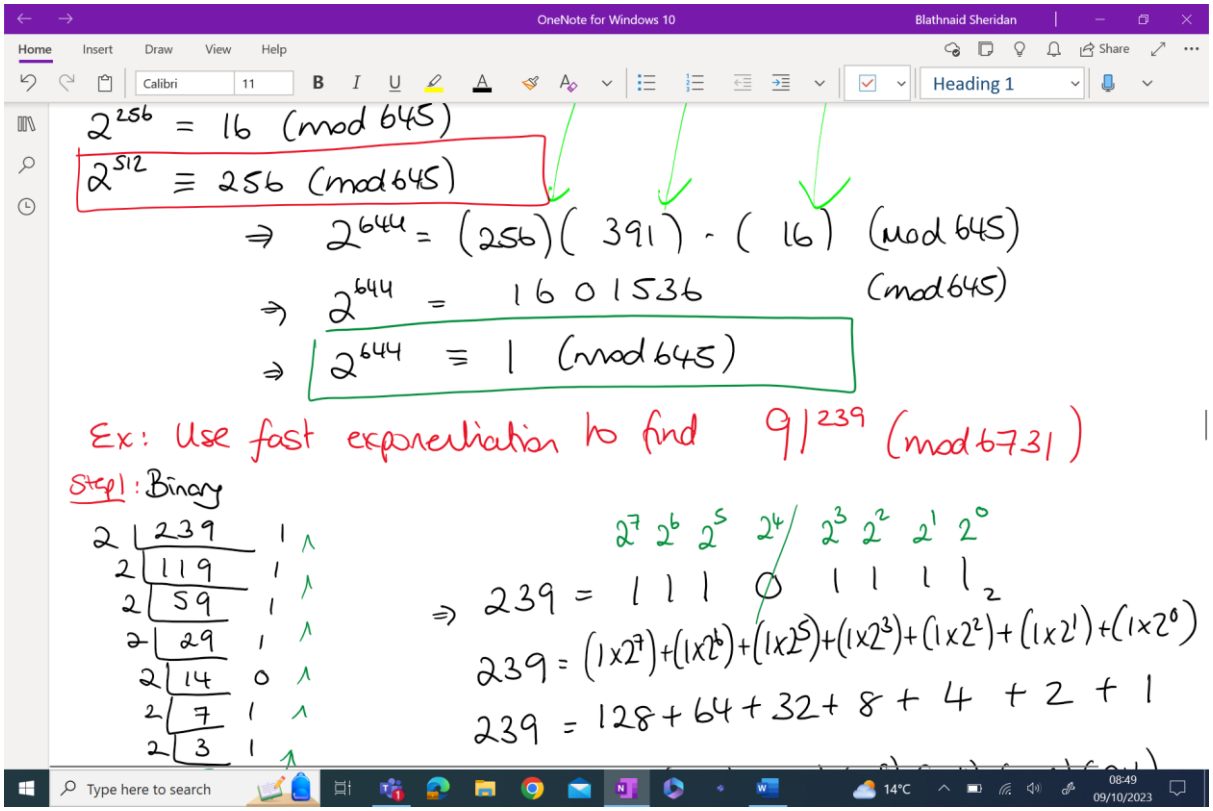
Type here to search — 14°C — 08:48 09/10/2023

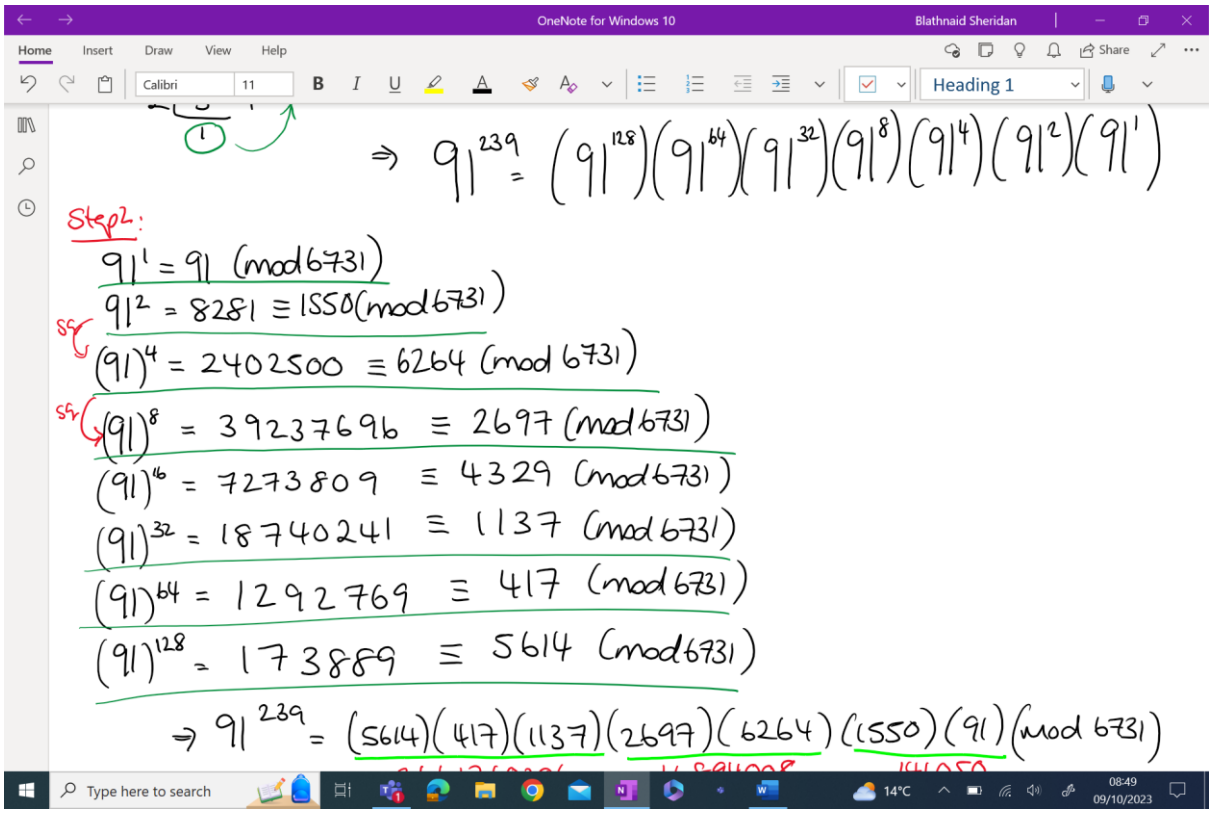

OneNote for Windows 10
Blathnaid Sheridan
Home Insert Draw View Help
Heading 1
$7^1 = 7 \pmod 9$
$7^2 = 4 \pmod 9$
$7^3 = 1 \pmod 9$
So $7^{41} = 7^2 \cdot 7^{39}$
$7^{41} = 7^2 \cdot (7^3)^{13}$
$7^{41} = 7^2 \cdot (1)^{13}$
$7^{41} = 7^2 \cdot 1$
$7^{41} = 49$
$7^{41} \equiv 4 \pmod 9$
Eg. Find $3^{10} \pmod{47}$
$3^0 = 1 \pmod{47}$
Type here to search
14°C
08:48
09/10/2023


OneNote for Windows 10
Blathnaid Sheridan
Home Insert Draw View Help
Heading 1
$3^1 = 3 \pmod{47}$
$3^2 = 9 \pmod{47}$
$3^3 = 27 \pmod{47}$
$3^4 = 81 \equiv 34 \pmod{47}$
$\times 3$
$3^5 = 102 \equiv 8 \pmod{47}$
$\times 3$
$3^6 = 24 \pmod{47}$
$3^7 = 72 \equiv 25 \pmod{47}$
$3^8 = 75 \equiv 28 \pmod{47}$
$3^9 = 84 \equiv 37 \pmod{47}$
$3^{10} = 111 \equiv 17 \pmod{47}$
we will now use fast exponentiation to find $3^{10} \pmod{47}$
$(1\times2^3)(0\times2^2)(1\times2^1)(0\times2^0)$
Type here to search
14°C
08:48
09/10/2023


OneNote for Windows 10
Blathnaid Sheridan
Home Insert Draw View Help
Heading 1
2|10 0
2|5 1
2|2 0
1
⇒ 10 = 1 0 1 0₂
(1x2³)(0x2²)(1x2¹)(0x2⁰)
10 = 8 + 2
⇒ 3^10 = (3^8)(3^2)
3^10 = (28)(9) (Mod 47)
3^10 = 252 (Mod 47)
3^10 ≡ 17 (Mod 47)
Ex: Calculate 2^644 (mod 645) using fast exponentiation.
2|644 0
2|322 0
2|161 1
2|80 0
In binary: 2^9 2^8 2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0
644 = 1 0 1 0 0 0 0 1 0 0₂
644 = (1x2^9) + (1x2^7) + (1x2^2)
Type here to search
14°C
08:48
09/10/2023


OneNote for Windows 10
Blathnaid Sheridan
Home Insert Draw View Help
Heading 1
2|161 1
2|80 0
2|40 0
2|20 0
2|10 0
2|5 1
2|2 0
1
644 = 1 0 1 0 0 0 0 1 0 0₂
644 = (1x2^9) + (1x2^7) + (1x2^2)
644 = 512 + 128 + 4
⇒ 2^644 = (2^512)·(2^128)·(2^4) (mod 645)
2^4 = 16 (mod 645)
square
2^8 = 256 (mod 645)
square
2^16 = 65536 ≡ 391 (mod 645)
2^32 = 152881 ≡ 16 (mod 645)
2^64 = 256 (mod 645) ....notice pattern.
2^128 ≡ 391 (mod 645)
Type here to search
14°C
08:48
09/10/2023


OneNote for Windows 10
Blathnaid Sheridan
Home Insert Draw View Help
Heading 1
$2^{256} = 16 \pmod{645}$
$2^{512} \equiv 256 \pmod{645}$
$\Rightarrow 2^{644} = (256)(391)\cdot(16) \pmod{645}$
$\Rightarrow 2^{644} = 1601536 \pmod{645}$
$\Rightarrow 2^{644} \equiv 1 \pmod{645}$
Ex: Use fast exponentiation to find $91^{239} \pmod{6731}$
Step1: Binary
2 | 239 1
2 | 119 1
2 | 59 1
2 | 29 1
2 | 14 0
2 | 7 1
2 | 3 1
1
$2^7\ 2^6\ 2^5\ 2^4\ 2^3\ 2^2\ 2^1\ 2^0$
$\Rightarrow 239 = 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1_2$
$239 = (1\times2^7)+(1\times2^6)+(1\times2^5)+(1\times2^3)+(1\times2^2)+(1\times2^1)+(1\times2^0)$
$239 = 128+64+32+8+4+2+1$
Type here to search
14°C
08:49
09/10/2023


OneNote for Windows 10
Blathnaid Sheridan
Home Insert Draw View Help
Heading 1
$\Rightarrow 91^{239} = (91^{128})(91^{64})(91^{32})(91^{8})(91^{4})(91^{2})(91^{1})$
Step2:
$91^1 = 91 \pmod{6731}$
$91^2 = 8281 \equiv 1550 \pmod{6731}$
SS
$(91)^4 = 2402500 \equiv 6264 \pmod{6731}$
SS
$(91)^8 = 39237696 \equiv 2697 \pmod{6731}$
$(91)^{16} = 7273809 \equiv 4329 \pmod{6731}$
$(91)^{32} = 18740241 \equiv 1137 \pmod{6731}$
$(91)^{64} = 1292769 \equiv 417 \pmod{6731}$
$(91)^{128} = 173889 \equiv 5614 \pmod{6731}$
$\Rightarrow 91^{239} = (5614)(417)(1137)(2697)(6264)(1550)(91) \pmod{6731}$
Type here to search
14°C
08:49
09/10/2023

OneNote for Windows 10 — Blathnaid Sheridan

$\Rightarrow 91^{239} = (5614)(417)(1137)(2697)(6264)(1550)(91) \pmod{6731}$

$2661760206 \qquad 16894008 \qquad 141050$

$91^{239} = (6449) \times (529) \times (6430) \pmod{6731}$

3411521

$91^{239} = (5635) \times (6430) \pmod{6731}$

36233050

$\boxed{91^{239} = 77 \pmod{6731}}$

FLT: $a^{p-1} \equiv 1 \pmod{p}$

$\Rightarrow 2^4 \equiv 1 \pmod{5}$

If Mod $p = 5$ is prime then $(p-1) = 4$

and $2^4 = 1 \pmod{5}$

Eg. Calculate $2^{340} \pmod{11}$ using FLT. $a = 2$

Type here to search — 14°C — 08:49 09/10/2023

OneNote for Windows 10 — Blathnaid Sheridan

Eg. Calculate $2^{340} \pmod{11}$ using FLT. $a = 2$

we can use FLT because the mod = 11 is prime $p = 11$

$\Rightarrow 2^{(11-1)} = 1 \pmod{11}$

$2^{10} \equiv 1 \pmod{11}$ .... by FLT

$(10 \times 34 = 340) \Rightarrow (2^{10})^{34} = (1)^{34} \pmod{11}$

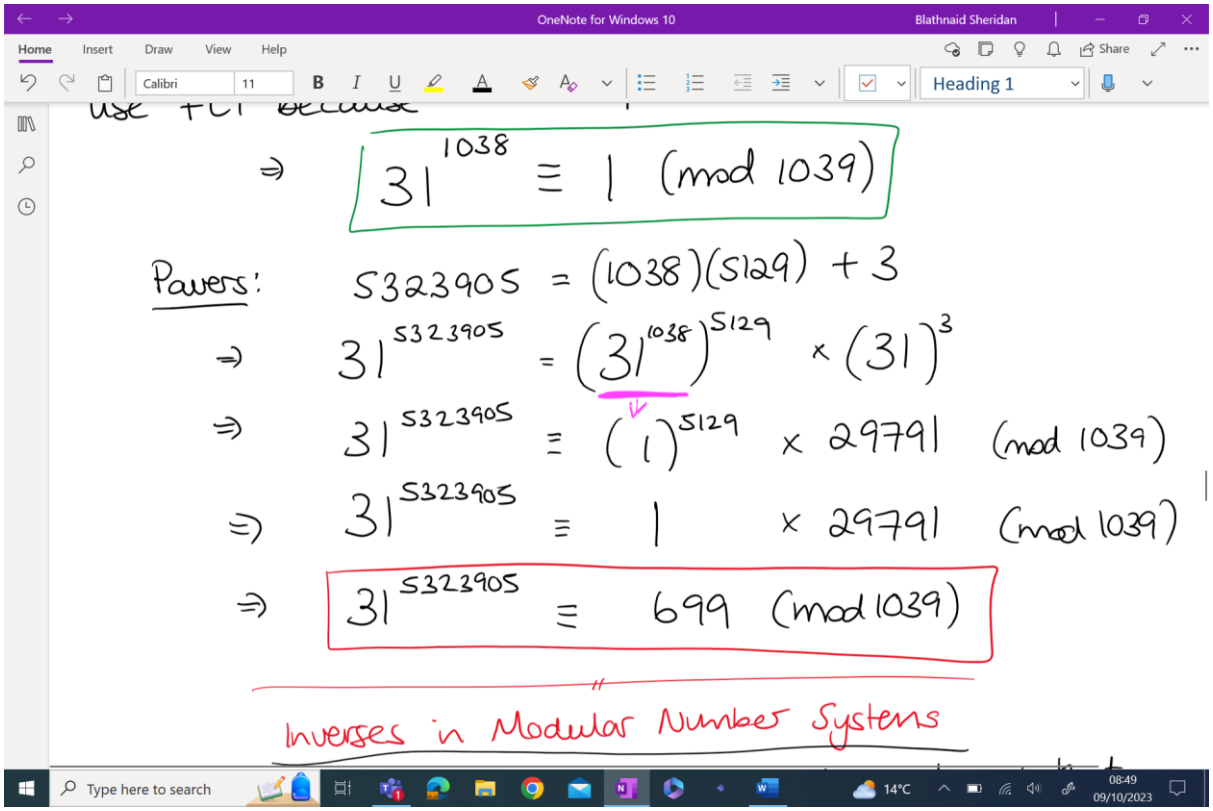
$\boxed{2^{340} \equiv 1 \pmod{11}}$

Eg. Calculate $31^{5323905} \pmod{1039}$ given that 1039 is prime. $(a = 31 \quad p = 1039)$

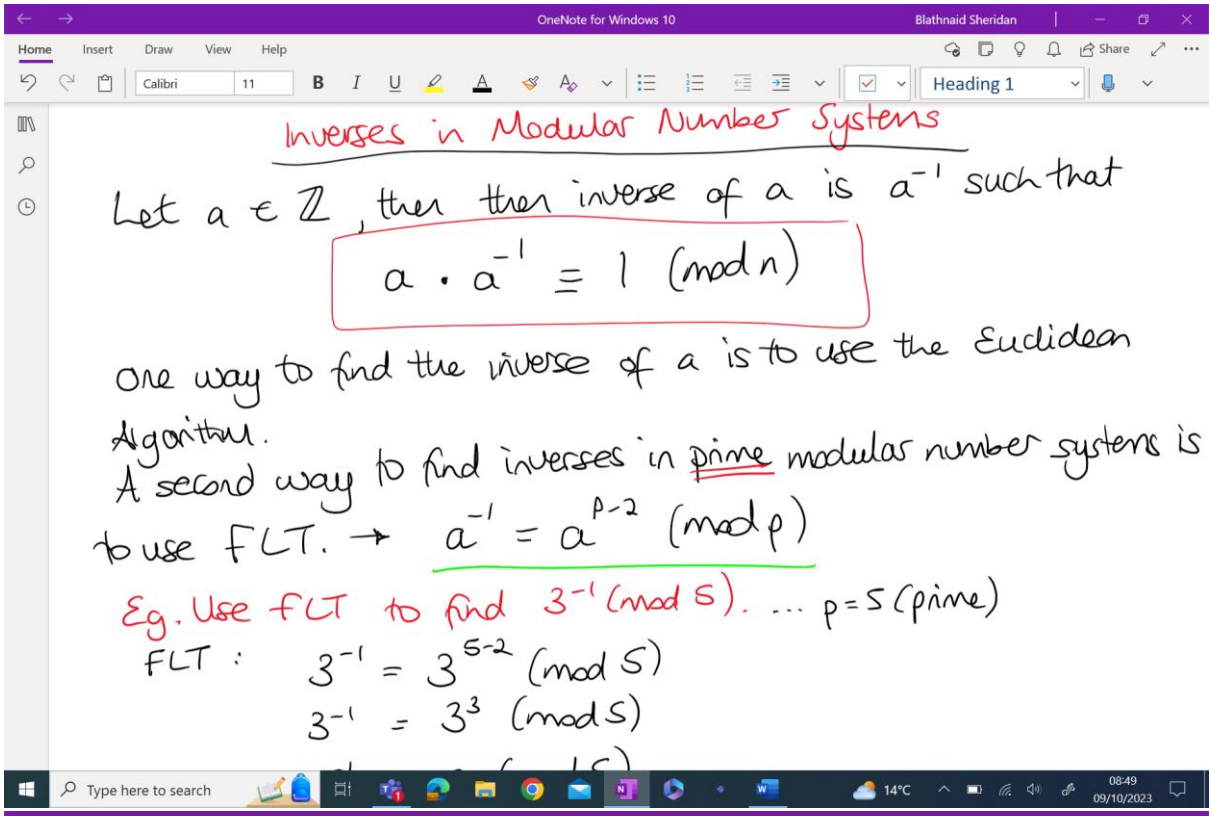
Use FLT because 1039 is prime.

$\Rightarrow \boxed{31^{1038} \equiv 1 \pmod{1039}}$

Type here to search — 14°C — 08:49 09/10/2023


OneNote for Windows 10
Blathnaid Sheridan
Home
Insert
Draw
View
Help
Share
Calibri
11
Heading 1
use FLT because
$\Rightarrow 31^{1038} \equiv 1 \pmod{1039}$
Powers: $5323905 = (1038)(5129) + 3$
$\Rightarrow 31^{5323905} = (31^{1038})^{5129} \times (31)^3$
$\Rightarrow 31^{5323905} \equiv (1)^{5129} \times 29791 \pmod{1039}$
$\Rightarrow 31^{5323905} \equiv 1 \times 29791 \pmod{1039}$
$\Rightarrow 31^{5323905} \equiv 699 \pmod{1039}$
Inverses in Modular Number Systems
Type here to search
14°C
08:49
09/10/2023

v



OneNote for Windows 10 — Blathnaid Sheridan

Home Insert Draw View Help — Calibri 11 — Heading 1

Inverses in Modular Number Systems

Let $a \in \mathbb{Z}$, then the inverse of a is a^{-1} such that

$$a \cdot a^{-1} \equiv 1 \pmod{n}$$

One way to find the inverse of a is to use the Euclidean Algorithm.

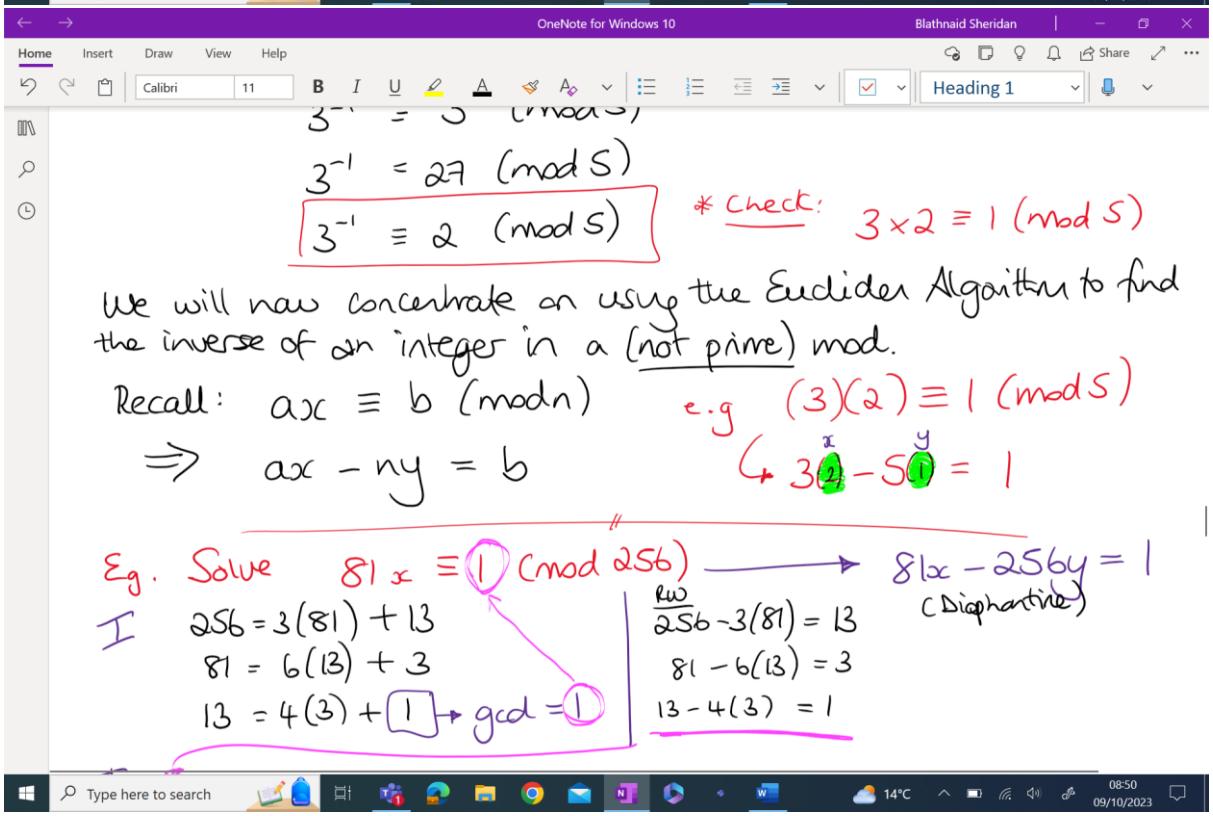
A second way to find inverses in prime modular number systems is to use FLT. → $a^{-1} = a^{p-2} \pmod{p}$

Eg. Use FLT to find $3^{-1} \pmod 5$. … $p = 5$ (prime)

FLT: $3^{-1} = 3^{5-2} \pmod 5$

$3^{-1} = 3^3 \pmod 5$

Type here to search — 14°C — 08:49 09/10/2023



OneNote for Windows 10 — Blathnaid Sheridan

Home Insert Draw View Help — Calibri 11 — Heading 1

$3^{-1} = 27 \pmod 5$

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

* Check: $3 \times 2 \equiv 1 \pmod 5$

We will now concentrate on using the Euclidean Algorithm to find the inverse of an integer in a (not prime) mod.

Recall: $ax \equiv b \pmod n$

$\Rightarrow ax - ny = b$

e.g $(3)(2) \equiv 1 \pmod 5$

$3(2) - 5(1) = 1$ (x, y)

Eg. Solve $81x \equiv 1 \pmod{256}$ → $81x - 256y = 1$ (Diophantine)

I
$256 = 3(81) + 13$
$81 = 6(13) + 3$
$13 = 4(3) + 1$ → gcd = 1

RW
$256 - 3(81) = 13$
$81 - 6(13) = 3$
$13 - 4(3) = 1$

Type here to search — 14°C — 08:50 09/10/2023

OneNote for Windows 10 — Blathnaid Sheridan

II

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

$1(13) - 4[81 - 6(13)] = 1$

$25(13) - 4(81) = 1$

$25[256 - 3(81)] - 4(81) = 1$

$25(256) - 79(81) = 1$

$0 \qquad (-79)(81) \equiv 1 \pmod{256}$

Therefore $(81)^{-1} = (-79) \pmod{256}$ ie $x = -79$

But $(-79) \notin (\text{Mod } 256) \Rightarrow -79 + 256 \equiv 177$

$\Rightarrow \boxed{x \equiv 177}$

* Check: $81x \equiv 1 \pmod{256}$

$(81)(177) = 14337$

$\equiv 1 \pmod{256}$ ✓

Type here to search — 14°C — 08:50 09/10/2023

OneNote for Windows 10 — Blathnaid Sheridan

Hill Digraph Cipher

① Find the inverse of an integer in a Mod. ✓

② Multiply Matrices.

③ Find inverse of (2x2) Matrices.

$$\begin{pmatrix} 4 & 3 \\ 2 & 7 \end{pmatrix}\begin{pmatrix} 4 & -1 & 2 \\ 3 & 0 & -5 \end{pmatrix} = \begin{pmatrix} (4)(4)+(3)(3) & (4)(-1)+(3)(0) & (4)(2)+(3)(-5) \\ (2)(4)+(7)(3) & (2)(-1)+(7)(0) & (2)(2)+(7)(-5) \end{pmatrix}$$

$$= \begin{pmatrix} 25 & -4 & -7 \\ 29 & -2 & -31 \end{pmatrix}$$

$$A = \begin{pmatrix} 3 & 2 \\ 7 & 5 \end{pmatrix}$$

- $\det(A) = (3)(5) - (2)(7) = 15 - 14 = 1$
- $\text{adj}(A) = \begin{pmatrix} 5 & -2 \\ -7 & 3 \end{pmatrix}$

Type here to search — 14°C — 08:50 09/10/2023

$$\Rightarrow A^{-1} = \frac{1}{\det(A)} \cdot \text{adj}(A) = \frac{1}{1}\begin{pmatrix} 5 & -2 \\ -7 & 3 \end{pmatrix} = \begin{pmatrix} 5 & -2 \\ -7 & 3 \end{pmatrix}$$

Eg. Encrypt the message "TUD" using the encryption matrix $A = \begin{pmatrix} 5 & 3 \\ 2 & 1 \end{pmatrix}$

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
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

Plaintext: TU, D X,

19 20, 3 23,

we write each block as a column

$$\Rightarrow \begin{pmatrix} 19 & 3 \\ 20 & 23 \end{pmatrix}$$

we now multiply (on the left) the encryption matrix by plaintext matrix

$$\begin{pmatrix} 5 & 3 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 19 & 3 \\ 20 & 23 \end{pmatrix} = \begin{pmatrix} 155 & 84 \\ 58 & 29 \end{pmatrix} \equiv \begin{pmatrix} 25 & 6 \\ 6 & 3 \end{pmatrix} \pmod{26}$$

$$\rightarrow \begin{pmatrix} Z & G \\ G & D \end{pmatrix}$$

Ciphertext: Z G G, D

Eg. Encrypt the plaintext TREE using the matrix $\begin{pmatrix} 4 & 6 \\ 2 & 7 \end{pmatrix}$ modulo 26.

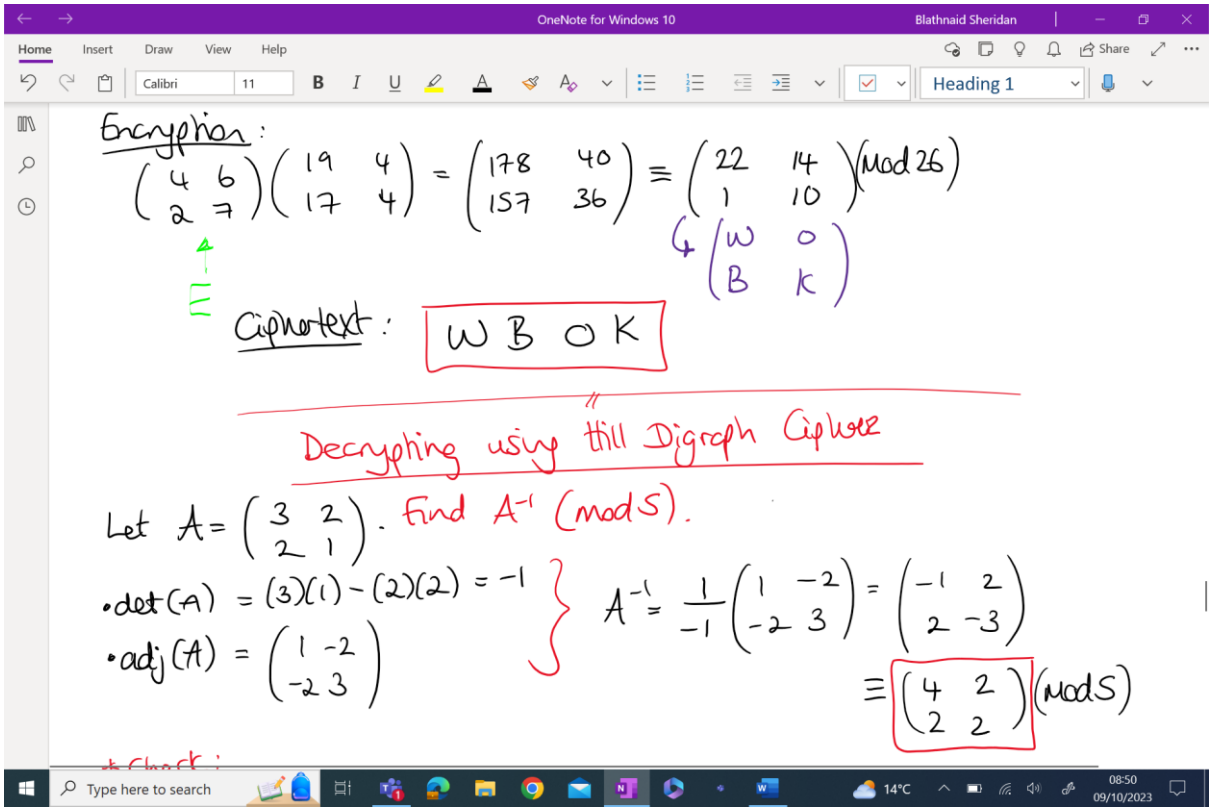
Plaintext: TR, EE

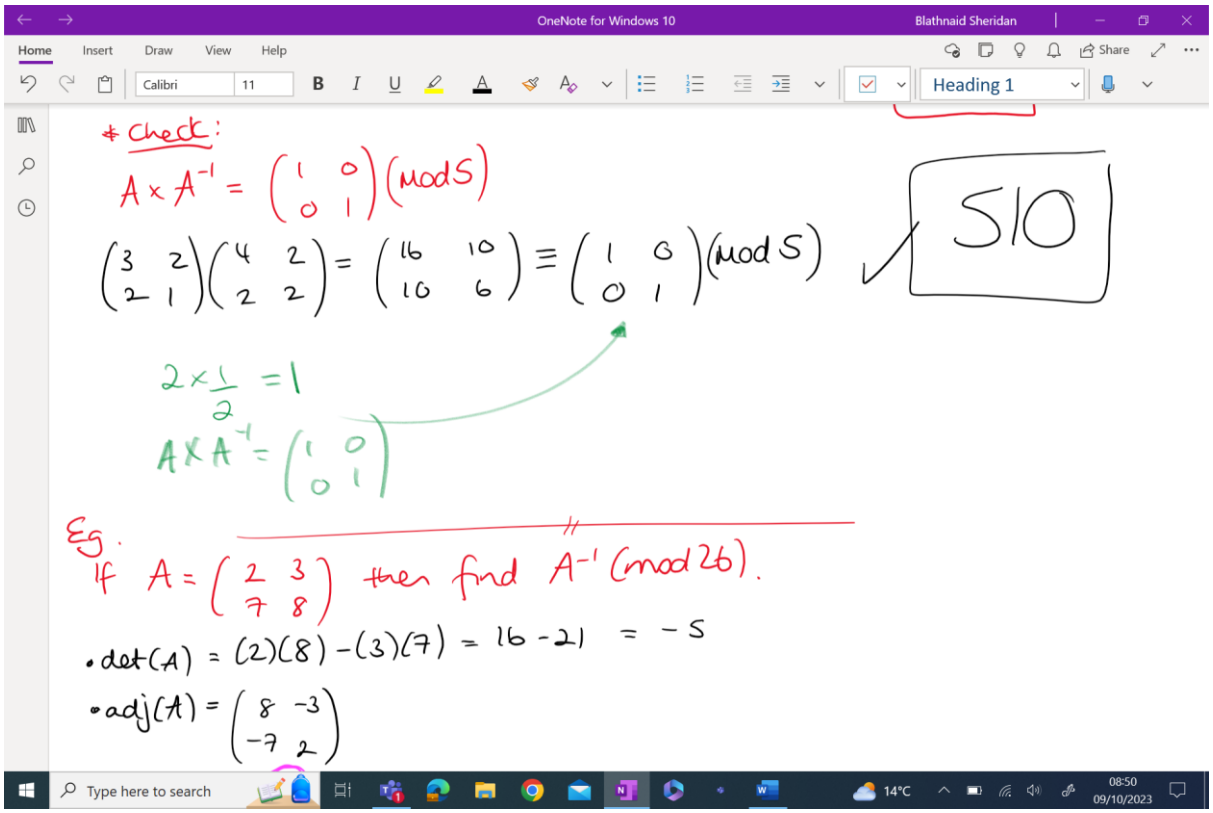
19 17 4 4

$$\rightarrow \begin{pmatrix} 19 & 4 \\ 17 & 4 \end{pmatrix}$$

Encryption:

$$\begin{pmatrix} 4 & 6 \\ 2 & 7 \end{pmatrix}\begin{pmatrix} 19 & 4 \\ 17 & 4 \end{pmatrix} = \begin{pmatrix} 178 & 40 \\ 157 & 36 \end{pmatrix} \equiv \begin{pmatrix} 22 & 14 \\ 1 & 10 \end{pmatrix} \pmod{26}$$


OneNote for Windows 10
Blathnaid Sheridan
Home Insert Draw View Help
Heading 1
Encryption:
$\begin{pmatrix} 4 & 6 \\ 2 & 7 \end{pmatrix}\begin{pmatrix} 19 & 4 \\ 17 & 4 \end{pmatrix} = \begin{pmatrix} 178 & 40 \\ 157 & 36 \end{pmatrix} \equiv \begin{pmatrix} 22 & 14 \\ 1 & 10 \end{pmatrix} \pmod{26}$
$\begin{pmatrix} W & O \\ B & K \end{pmatrix}$
Ciphertext: WB OK
Decrypting using this Digraph Cipher
Let $A = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}$. Find $A^{-1} \pmod 5$.
• $\det(A) = (3)(1) - (2)(2) = -1$
• $\text{adj}(A) = \begin{pmatrix} 1 & -2 \\ -2 & 3 \end{pmatrix}$
$A^{-1} = \frac{1}{-1}\begin{pmatrix} 1 & -2 \\ -2 & 3 \end{pmatrix} = \begin{pmatrix} -1 & 2 \\ 2 & -3 \end{pmatrix}$
$\equiv \begin{pmatrix} 4 & 2 \\ 2 & 2 \end{pmatrix} \pmod 5$
* Check:
Type here to search
14°C
08:50
09/10/2023


OneNote for Windows 10
Blathnaid Sheridan
Home Insert Draw View Help
Heading 1
* Check:
$A \times A^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 5$
$\begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 4 & 2 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 16 & 10 \\ 10 & 6 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 5$
SIO
$2 \times \frac{1}{2} = 1$
$A \times A^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Eg. If $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$ then find $A^{-1} \pmod{26}$.
• $\det(A) = (2)(8) - (3)(7) = 16 - 21 = -5$
• $\text{adj}(A) = \begin{pmatrix} 8 & -3 \\ -7 & 2 \end{pmatrix}$
Type here to search
14°C
08:50
09/10/2023

OneNote for Windows 10 — Blathnaid Sheridan

$\Rightarrow A^{-1} = \frac{1}{-5}\begin{pmatrix} 8 & -3 \\ -7 & 2 \end{pmatrix}$

no fractions!

we need to find $(-5)^{-1} \pmod{26}$

ie $(21)^{-1} \pmod{26}$ ie $(21)x \equiv 1 \pmod{26}$

I
$26 = 1(21) + 5$
$21 = 4(5) + 1$

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

II
$1(21) - 4(5) = 1$
$1(21) - 4[26 - 1(21)] = 1$
$5(21) - 4(26) = 1 \pmod{26}$
0

$x = 5$ is the inverse of $21 \pmod{26}$

Type here to search — 14°C — 08:50 09/10/2023

OneNote for Windows 10 — Blathnaid Sheridan

$x = 5$ is the inverse of $21 \pmod{26}$

$\Rightarrow A^{-1} = 5\begin{pmatrix} 8 & -3 \\ -7 & 2 \end{pmatrix} = \begin{pmatrix} 40 & -15 \\ -35 & 10 \end{pmatrix} \equiv \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \pmod{26}$

*check

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

Hill Digraph Cipher - Decryption

Eg. Recover the plaintext given the ciphertext ZGGD which was encrypted using the matrix $A = \begin{pmatrix} 5 & 3 \\ 2 & 1 \end{pmatrix}$

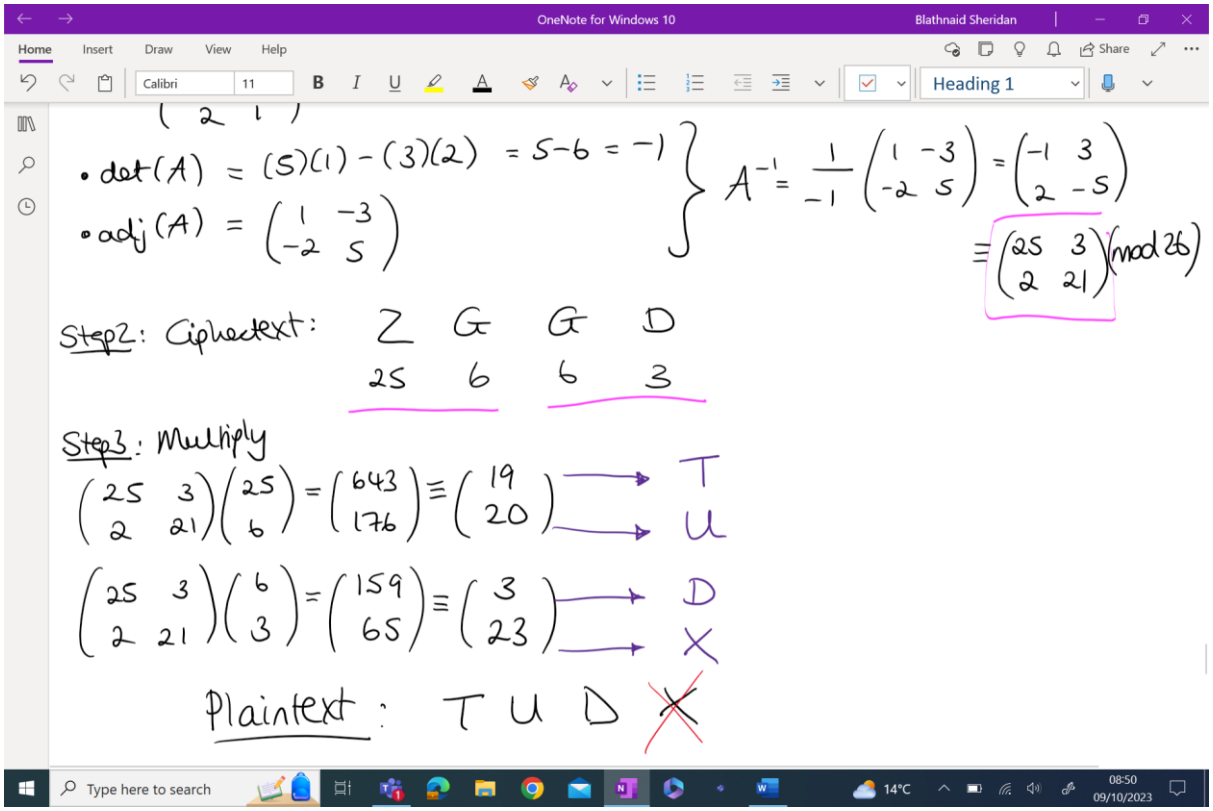
Step 1: Need $A^{-1} \pmod{26}$

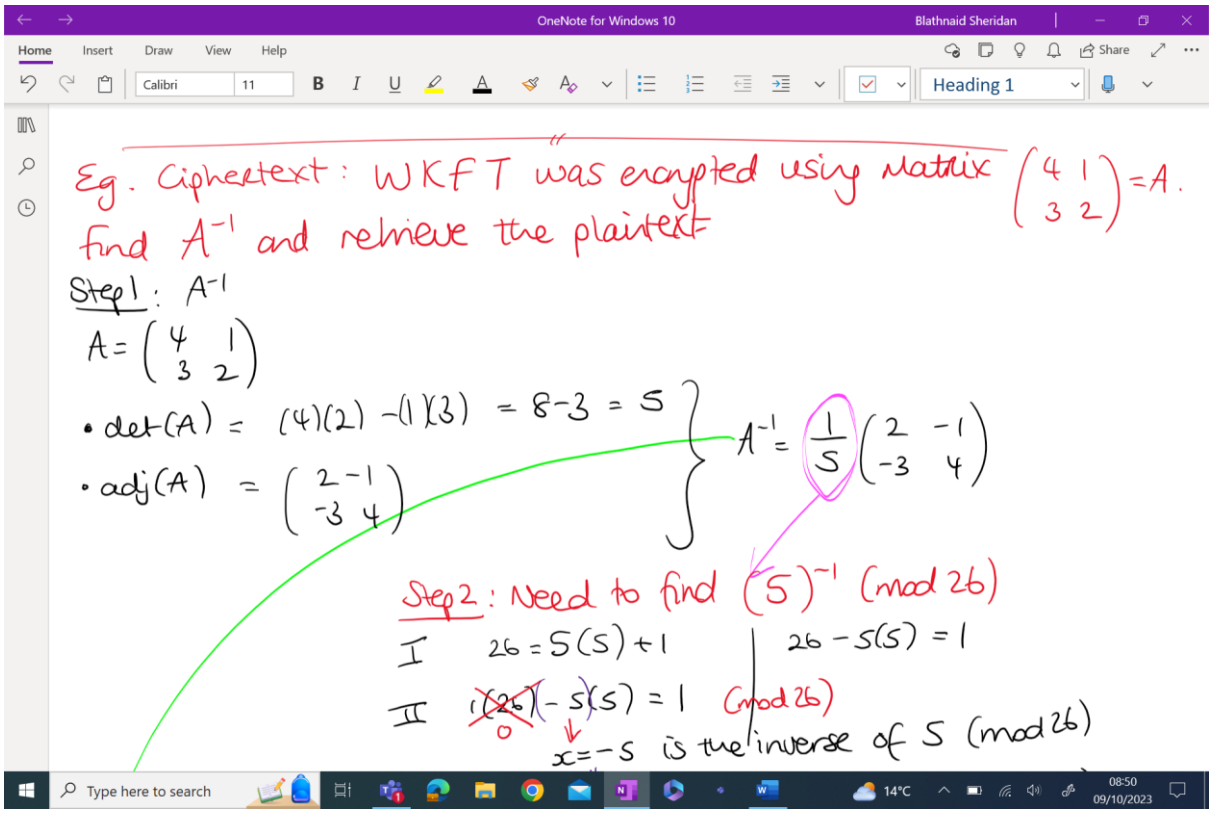
$A = \begin{pmatrix} 5 & 3 \\ 2 & 1 \end{pmatrix}$

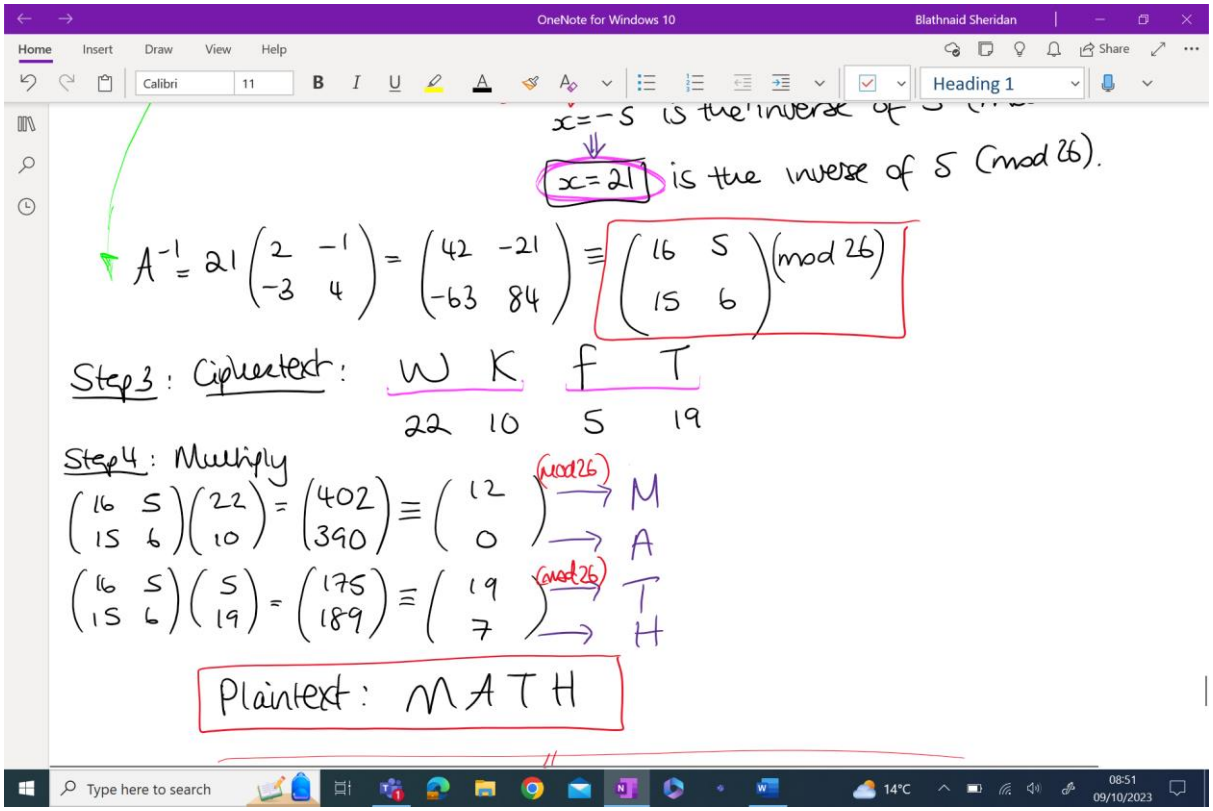
$\det(A) = (5)(1) - (3)(2) = 5 - 6 = -1$?

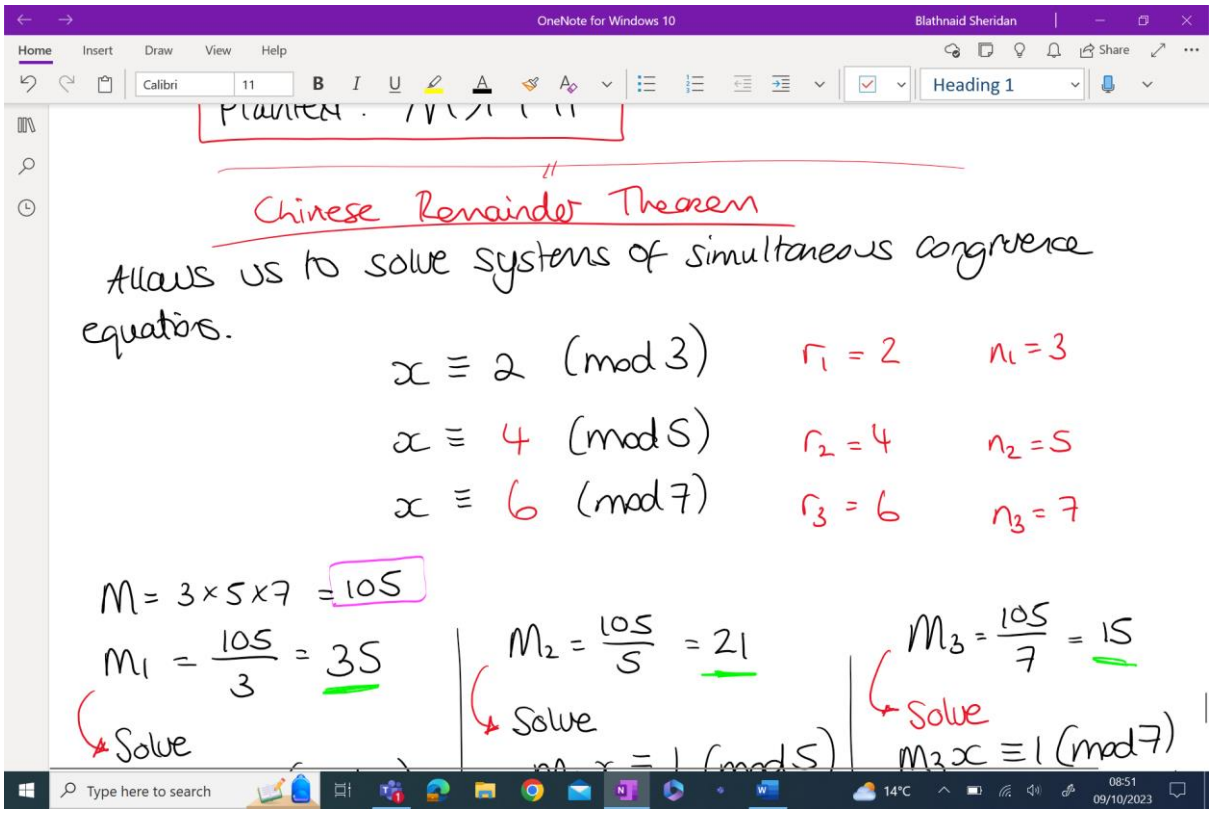
$A^{-1} = \frac{1}{-1}\begin{pmatrix} 1 & -3 \\ -2 & 5 \end{pmatrix} = \begin{pmatrix} -1 & 3 \\ 2 & -5 \end{pmatrix}$

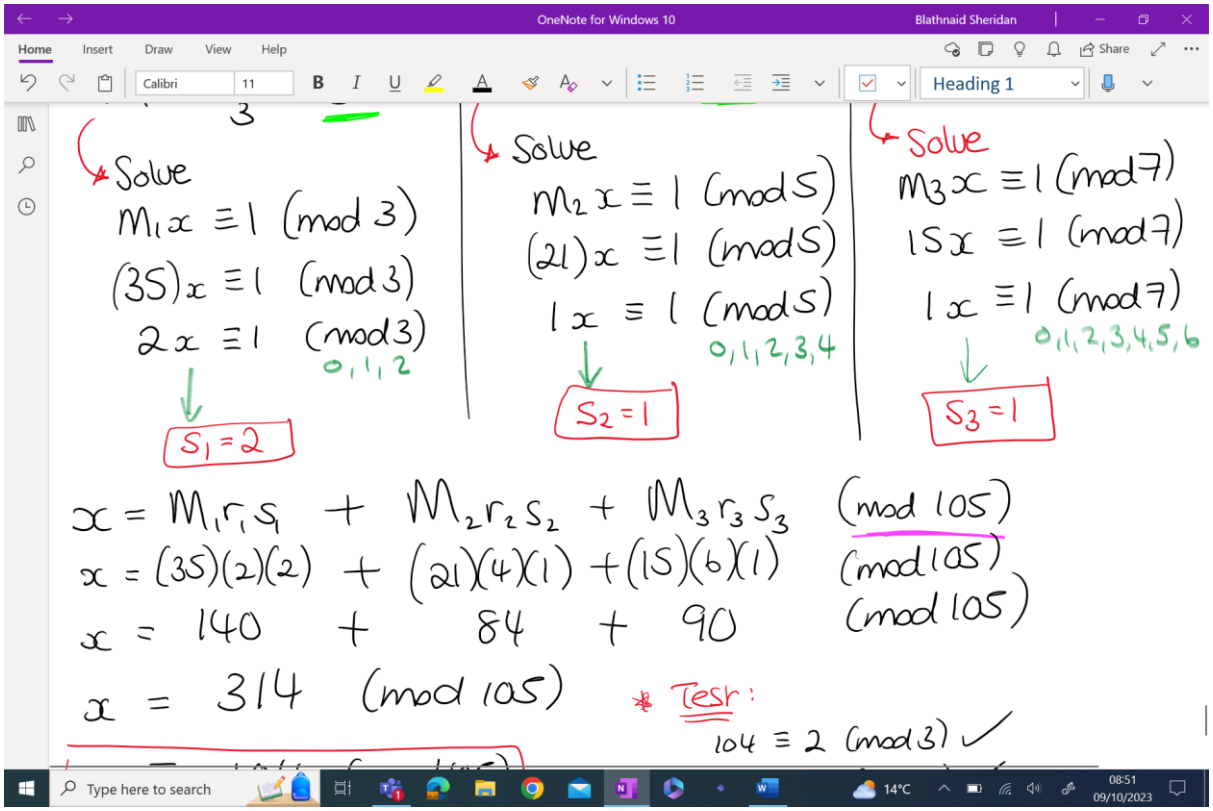
Type here to search — 14°C — 08:50 09/10/2023

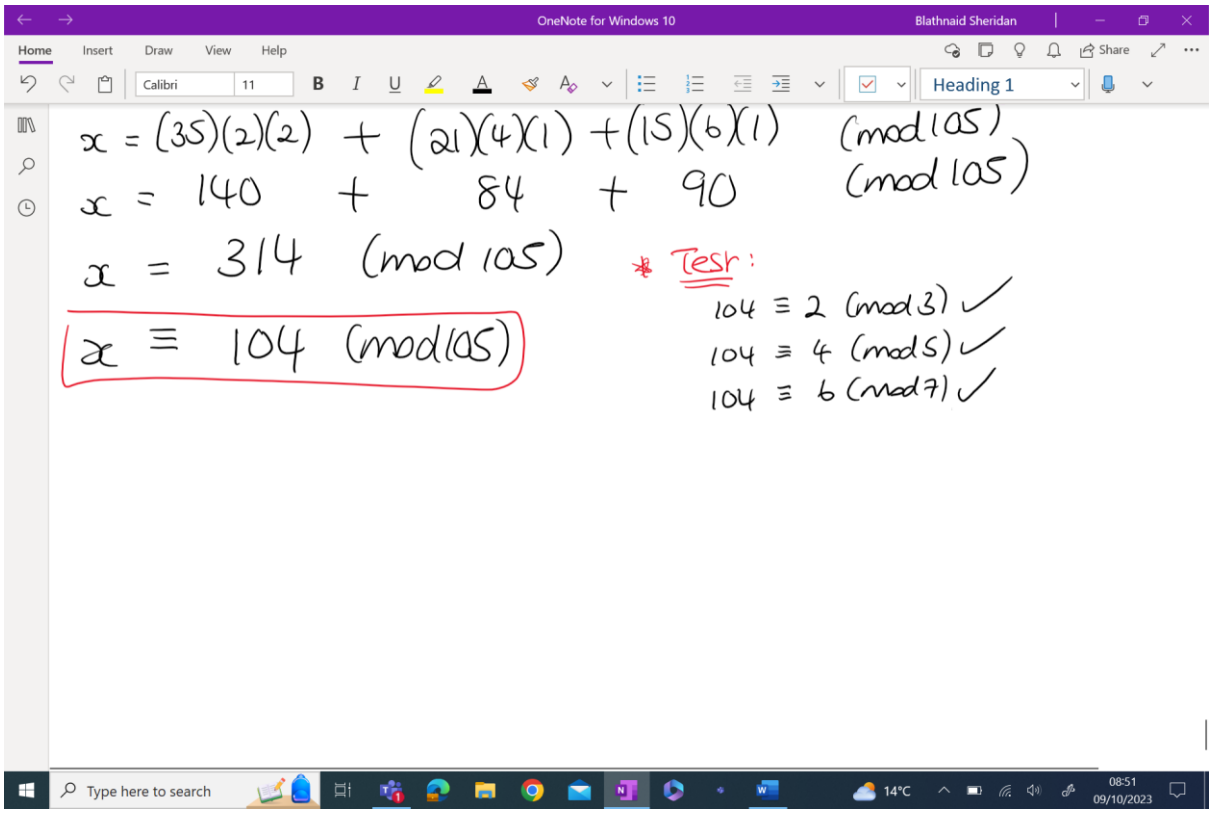

OneNote for Windows 10
Blathnaid Sheridan
Heading 1
$\begin{pmatrix} 2 & 1 \end{pmatrix}$
• $\det(A) = (5)(1) - (3)(2) = 5-6 = -1$
• $\text{adj}(A) = \begin{pmatrix} 1 & -3 \\ -2 & 5 \end{pmatrix}$
$A^{-1} = \frac{1}{-1}\begin{pmatrix} 1 & -3 \\ -2 & 5 \end{pmatrix} = \begin{pmatrix} -1 & 3 \\ 2 & -5 \end{pmatrix}$
$\equiv \begin{pmatrix} 25 & 3 \\ 2 & 21 \end{pmatrix} \pmod{26}$
Step2: Ciphertext: Z G G D
25 6 6 3
Step3: Multiply
$\begin{pmatrix} 25 & 3 \\ 2 & 21 \end{pmatrix}\begin{pmatrix} 25 \\ 6 \end{pmatrix} = \begin{pmatrix} 643 \\ 176 \end{pmatrix} \equiv \begin{pmatrix} 19 \\ 20 \end{pmatrix}$ → T, U
$\begin{pmatrix} 25 & 3 \\ 2 & 21 \end{pmatrix}\begin{pmatrix} 6 \\ 3 \end{pmatrix} = \begin{pmatrix} 159 \\ 65 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 23 \end{pmatrix}$ → D, X
Plaintext: T U D X
Type here to search
14°C
08:50
09/10/2023


OneNote for Windows 10
Blathnaid Sheridan
Heading 1
Eg. Ciphertext: WKFT was encrypted using matrix $\begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix} = A$.
Find A^{-1} and retrieve the plaintext
Step1: A^{-1}
$A = \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix}$
• $\det(A) = (4)(2) - (1)(3) = 8-3 = 5$
• $\text{adj}(A) = \begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix}$
$A^{-1} = \frac{1}{5}\begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix}$
Step2: Need to find $(5)^{-1} \pmod{26}$
I $26 = 5(5) + 1$ | $26 - 5(5) = 1$
II $1(26) - 5(5) = 1 \pmod{26}$
0
$x = -5$ is the inverse of 5 $\pmod{26}$
Type here to search
14°C
08:50
09/10/2023


OneNote for Windows 10
Blathnaid Sheridan
$x = -5$ is the inverse of 5 (mod 26).
$x = 21$ is the inverse of 5 (mod 26).
$A^{-1} = 21\begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix} = \begin{pmatrix} 42 & -21 \\ -63 & 84 \end{pmatrix} \equiv \begin{pmatrix} 16 & 5 \\ 15 & 6 \end{pmatrix} \pmod{26}$
Step 3: Ciphertext: W K f T
22 10 5 19
Step 4: Multiply
$\begin{pmatrix} 16 & 5 \\ 15 & 6 \end{pmatrix}\begin{pmatrix} 22 \\ 10 \end{pmatrix} = \begin{pmatrix} 402 \\ 390 \end{pmatrix} \equiv \begin{pmatrix} 12 \\ 0 \end{pmatrix} \xrightarrow{\pmod{26}} M, A$
$\begin{pmatrix} 16 & 5 \\ 15 & 6 \end{pmatrix}\begin{pmatrix} 5 \\ 19 \end{pmatrix} = \begin{pmatrix} 175 \\ 189 \end{pmatrix} \equiv \begin{pmatrix} 19 \\ 7 \end{pmatrix} \xrightarrow{\pmod{26}} T, H$
Plaintext: MATH
Type here to search
14°C
08:51
09/10/2023


OneNote for Windows 10
Blathnaid Sheridan
Chinese Remainder Theorem
Allows us to solve systems of simultaneous congruence equations.
$x \equiv 2 \pmod 3$ $r_1 = 2$ $n_1 = 3$
$x \equiv 4 \pmod 5$ $r_2 = 4$ $n_2 = 5$
$x \equiv 6 \pmod 7$ $r_3 = 6$ $n_3 = 7$
$M = 3 \times 5 \times 7 = 105$
$M_1 = \frac{105}{3} = 35$
Solve
$M_2 = \frac{105}{5} = 21$
Solve
$M_3 = \frac{105}{7} = 15$
Solve
$M_3 x \equiv 1 \pmod 7$
Type here to search
14°C
08:51
09/10/2023


OneNote for Windows 10
Blathnaid Sheridan
Home Insert Draw View Help
Heading 1
Solve
$M_1 x \equiv 1 \pmod 3$
$(35)x \equiv 1 \pmod 3$
$2x \equiv 1 \pmod 3$
0, 1, 2
$S_1 = 2$
Solve
$M_2 x \equiv 1 \pmod 5$
$(21)x \equiv 1 \pmod 5$
$1x \equiv 1 \pmod 5$
0, 1, 2, 3, 4
$S_2 = 1$
Solve
$M_3 x \equiv 1 \pmod 7$
$15x \equiv 1 \pmod 7$
$1x \equiv 1 \pmod 7$
0, 1, 2, 3, 4, 5, 6
$S_3 = 1$
$x = M_1 r_1 s_1 + M_2 r_2 s_2 + M_3 r_3 s_3 \pmod{105}$
$x = (35)(2)(2) + (21)(4)(1) + (15)(6)(1) \pmod{105}$
$x = 140 + 84 + 90 \pmod{105}$
$x = 314 \pmod{105}$
Test:
$104 \equiv 2 \pmod 3$ ✓
Type here to search
14°C
08:51
09/10/2023


OneNote for Windows 10
Blathnaid Sheridan
Home Insert Draw View Help
Heading 1
$x = (35)(2)(2) + (21)(4)(1) + (15)(6)(1) \pmod{105}$
$x = 140 + 84 + 90 \pmod{105}$
$x = 314 \pmod{105}$
$x \equiv 104 \pmod{105}$
Test:
$104 \equiv 2 \pmod 3$ ✓
$104 \equiv 4 \pmod 5$ ✓
$104 \equiv 6 \pmod 7$ ✓
Type here to search
14°C
08:51
09/10/2023