20170269 김은진 Homework6

Ex1)

(a) quotient = 2
remainder = 5

(b) quotient = −11
remainder = 10

(c) quotient = 34
remainder = 7.

(d) quotient = −1.
remainder = 2.

Ex2)

(a) 13 mod 3 = 1

(b) −97 mod 11 = 2.

(c) 155 mod 19 = 3

(d) −221 mod 23 = 9

Ex3)

(a) a div m = 1
a mod m = 108.

(b) a div m = 40
a mod m = 89

(c) a div m = −4.
a mod m = 222

(d) a div m = −201
a mod m = 38150

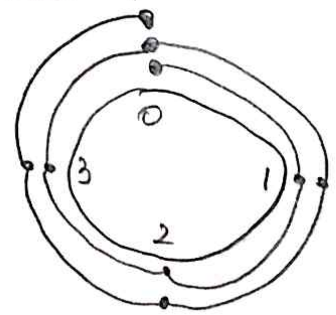
Ex4)

(a) (−133 mod 23 + 261 mod 23) mod 23
⇒ −133 + 261 = 128
⇒ (128 mod 23) mod 23
⇒ 13 mod 23
= 13.

(b) (457 mod 23 · 182 mod 23) mod 23
= ((457×182) mod 23) mod 23
⇒ 83174 mod 23 = 6.
⇒ 6 mod 23 = 6

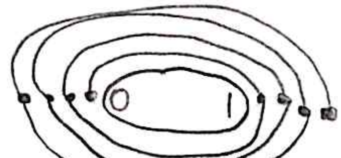
Ex5)

a) 8 mod 4



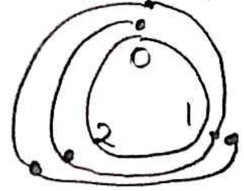
8 mod 4 = 0.

(b) 7 mod 2



7 mod 2 = 1.

(c) −5 mod 3.



−5 mod 3 = 1

Ex6)

(a) $55+26 \equiv (3+2) \pmod 4$

method 1)

$(55+26)-(3+2)=76$.

Since $4 | 76$ is multiple by 4.

method 2)

$$\frac{(55+26)-(3+2)}{4} = \frac{76}{4} = 19.$$

19 is integer.

$\therefore$ $55+26 \equiv (3+2) \pmod 4$ is true.

(b) $55-26 \equiv (3-2) \bmod 4$

method 1)

$(55-26)-(3-2) = 28$

Since $4 | 28$ is multiple by 4.

method 2)

$$\frac{(55-26)-(3-2)}{4} = 7$$

7 is integer

$\therefore$ $55-26 \equiv (3-2) \bmod 4$ is true.

(c) $55 \cdot 26 \equiv (3 \cdot 2) \bmod 4$

method 1)

$(55 \cdot 26)-(3 \cdot 2) = 1424$.

Since $4 | 1424$ is multiple by 4

method 2)

$$\frac{(55 \cdot 26)-(3 \cdot 2)}{4} = 356.$$

356 is integer

$\Rightarrow$ $(55 \cdot 26) \equiv (3 \cdot 2) \bmod 4$ is true.

(d) $55^2 \equiv 3^2 \pmod 4$

method 1)

$55^2 - 3^2 = 3016$.

Since $4 | 3016$ is multiple by 4

method 2)

$$\frac{55^2 - 3^2}{4} = 754$$

754 is integer

$\therefore$ $55^2 \equiv 3^2 \pmod 4$ is true.

Ex7)

(a) $31 \equiv 1 \pmod{10}$

method 1)

$31-1 = 30$.

Since $10 | 30$ is multiple by 10.

method 2)

$\frac{31-1}{10} = 3$. 3 is integer

$\therefore$ $31 \equiv 1 \pmod{}$ is true.

(b) $43 \equiv 22 \pmod 7$.

method 1)

$43-22=21$.

Since $7 | 21$ is multiple by integer.

method 2)

$\frac{43-22}{7} = 3$. 3 is integer

$\therefore$ $43 \equiv 22 \pmod 7$ is true.

(c) $8 \not\equiv -8 \pmod 3$.

$8-(-8) = 16$. 16 is not multiple by 3.

$\therefore$ $8 \not\equiv -8 \pmod{}$ is true.

(d) $91 \not\equiv 18 \pmod 6$.

$91-18 = 73$. 73 is not multiple by 6.

$\therefore$ $91 \not\equiv 18 \pmod 6$ is true.

Ex 8)

$16 \equiv a \pmod 5$.

↳ If that is congruent

$= 5 | (16-a)$

integer $a = 1, 6, 11, 16, 21, 26 \cdots$

Ex 9) $16 \equiv a \pmod 5$

$\Rightarrow 5 | (16-a)$

integer $a = 1, 6, 11, 16, 21, 26 \cdots$

$\therefore$ The least nonnegative integer is 1.

Ex 10)

a) $-10 \equiv a \pmod 4$

If that is congruent,

$4 | (-10-a)$

$\therefore$ integer $a = 2, 6, 10, 14, 18 \cdots$

b) The least nonnegative integer

is 2

Ex 11).

$x^2 \equiv 1 \pmod 5$

$0^2 \not\equiv 1 \pmod 5$

$1^2 \equiv 1 \pmod 5$

$2^2 \not\equiv 1 \pmod 5$

$3^2 \not\equiv 1 \pmod 5$

$4^2 \equiv 1 \pmod 5$

$\therefore x \equiv 1$ or $4 \pmod 5$

Ex 12)

(a) 231

$= (11100111)_{(2)}$

$$
\begin{array}{r|l}
2 & 231 \\
2 & 115 \cdots 1 \\
2 & 57 \cdots 1 \\
2 & 28 \cdots 1 \\
2 & 14 \cdots 0 \\
2 & 7 \cdots 0 \\
2 & 3 \cdots 1 \\
2 & 1 \cdots 1
\end{array}
$$

(b) 4532

$= (1000110110100)_{(2)}$.

$$
\begin{array}{r|l}
2 & 4532 \\
2 & 2266 \cdots 0 \\
2 & 1133 \cdots 0 \\
2 & 566 \cdots 1 \\
2 & 283 \cdots 0 \\
2 & 141 \cdots 1 \\
2 & 70 \cdots 1 \\
2 & 35 \cdots 0 \\
2 & 17 \cdots 1 \\
2 & 8 \cdots 1 \\
2 & 4 \cdots 0 \\
2 & 2 \cdots 0 \\
 & 1 \cdots 0
\end{array}
$$

Ex 13) $(12345)_{10}$

$$
\begin{array}{r|l}
8 & 12345 \\
8 & 1543 \cdots 1 \\
8 & 192 \cdots 7 \\
8 & 24 \cdots 0 \\
 & 3 \cdots 0
\end{array}
$$

$(30071)_{(8)}$.

Ex 14)

(a) $(11111)_2$.

$= (2^4 \times 1) + (2^3 \times 1) + (2^2 \times 1) + (2^1 \times 1) + (2^0 \times 1)$

$= 31$

(b) $(1000000001)_2$

$= (2^9 \times 1) + (2^8 \times 0) + (2^7 \times 0) + \cdots (2^1 \times 0) +$

$(2^0 \times 1) = 513$

Ex 15)

(a) $(572)_8 = 101111010$

(b) $(1604)_8 = 001110000100$

E16)

(a) $(80E)_{16} = (100000001110)_2$

(b) $(135AB)_{16} = (00010011010110101011)_2$

(c) $(ABBA)_{16} = (1010101110111010)_2$

E17)

$(1011\ 0111\ 1011)_2 \rightarrow (B7B)_{16}$

E18) $(7345321)_8$

$=(111\ 011\ 100\ 101\ 011\ 010\ 001)_2$

E19) $(1010111011)_2 = (001\ 010\ 111\ 011)_2$

$=(1273)_8$

E20)

a)

Sum –

```
  1000111
  1110111
 --------
 10111110
```

Product –

```
        1000111
        1110111
 --------------
        1000111
       1000111
      1000111
     0000000
    1000111
   1000111
  1000111
 --------------
 1101010100001
```

b) Sum –

```
  1110111
  1011101
 --------
 11010100
```

Product –

```
         1110111
         1011101
 ---------------
         1110111
        0000000
       1110111
      1110111
     1110111
    1110111
   00000000
  1110111
 ---------------
 1100000011
```

E21)

$3^{200} \bmod 50$

$3^1 \Rightarrow 3 \bmod 50 = 3$. $3^2 \Rightarrow 9 \bmod 50 = 9$.

$3^4 \Rightarrow 81 \bmod 50 = 31$ $3^8 \Rightarrow 961 \bmod 50 = 11$

$3^{16} \Rightarrow 121 \bmod 50 = 21$ $3^{32} \Rightarrow 441 \bmod 50 = 41$

$3^{64} \Rightarrow 1681 \bmod 50 = 31$. $3^{128} \Rightarrow 961 \bmod 50 = 11$.

$3^{200} = 3^{128} \cdot 3^{64} \cdot 3^8$

$\Rightarrow 3^{200} \bmod 50 = (3^{128} \cdot 3^{64} \cdot 3^8 \bmod 50) \bmod 50$

$= (11)(31)(11) \bmod 50 = 3751 \bmod 50 = 1$.

E22) $3^{94} \bmod 17$.

$3^1 \Rightarrow 3 \bmod 17 = 3$. $3^2 \Rightarrow 9 \bmod 17 = 9$

$3^4 \Rightarrow 81 \bmod 17 = 13$ $3^8 \Rightarrow 169 \bmod 17 = 16$

$3^{16} \Rightarrow 256 \bmod 17 = 1$ $3^{32} \Rightarrow 1 \bmod 17 = 1$

$3^{64} \Rightarrow 1 \bmod 17 = 1$.

$3^{94} = 3^{64} \cdot 3^{16} \cdot 3^8 \cdot 3^4 \cdot 3^2$

$\Rightarrow 3^{94} \bmod 50 = (3^{64} \cdot 3^{16} \cdot 3^8 \cdot 3^4 \cdot 3^2 \bmod 50) \bmod 50$

$= (9)(13)(16)(1)(1) \bmod 50 = 1872 \bmod 50 = 2$.

E23)

(a) 144^4 mod 713.

$144^1 \Rightarrow 144$ mod $713 = 144$

$144^2 \Rightarrow 20736$ mod $713 = 59$

$144^4 \Rightarrow 3481$ mod $713 = 629$

$\therefore 144^4$ mod $713 = 629$.

(b) 12^{43} mod 713

$12^1 \Rightarrow 12$ mod $713 = 12$. $12^2 = 144$ mod $713 = 144$

$12^4 \Rightarrow 20736$ mod $713 = 59$ $12^8 \Rightarrow 3481$ mod $713 = 629$

$12^{16} \Rightarrow 395641$ mod $713 = 639$ $12^{32} \Rightarrow$

408321 mod 713 = 485

$\therefore 12^{43} = 12^{32} \cdot 12^8 \cdot 12^2 \cdot 12^1$

$\Rightarrow 12^{43}$ mod $713 = (12^{32} \cdot 12^8 \cdot 12^2 \cdot 12^1$ mod $713)$ mod 713.

$= (12)(144)(629)(485)$ mod 713

$= 48$.

(c) 17^{27} mod 55

$17^1 \Rightarrow 17$ mod $55 = 17$. $17^2 \Rightarrow 289$ mod $55 = 14$

$17^4 \Rightarrow 196$ mod $55 = 31$ $17^8 \Rightarrow 961$ mod $55 = 26$.

$17^{16} \Rightarrow 676$ mod $55 = 16$ $17^{32} \Rightarrow 256$ mod $55 = 36$

$\therefore 17^{27} = 17^{16} \cdot 17^8 \cdot 17^2 \cdot 17^1$

$\Rightarrow 17^{27}$ mod $55 = (17^{16} \cdot 17^8 \cdot 17^2 \cdot 17^1$ mod $55)$ mod 55

$= 99008$ mod $55 = 8$

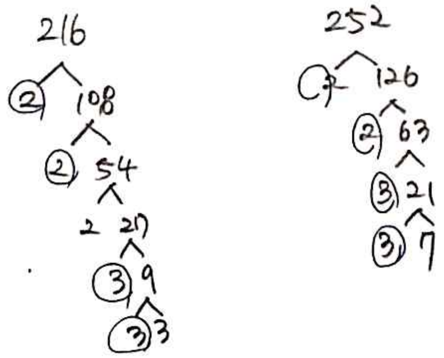
E24)

(a) 2, 5, 11, 13, 17, 23, 41, 71

(b) 6, 10, 15, 21, 28.

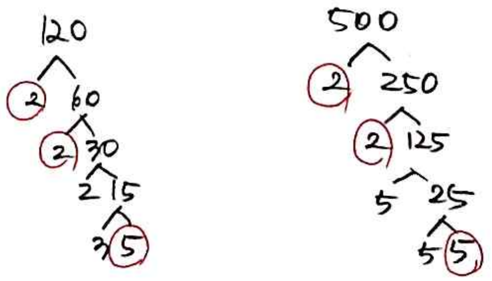
(c) 1.

E25)



$\therefore \gcd(216, 252) = 2 \cdot 2 \cdot 3 \cdot 3 = 36$.

E27)



$\therefore \gcd(120, 500) = 2 \cdot 2 \cdot 5 = 20$.

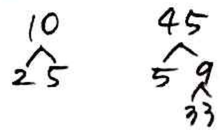
E27) $\gcd(120, 500) = 20$.

$500 = 120(4) + 20$

$120 = 20(6) + 0$

E28) $\gcd(10, 45)$.

a) P.F



$\therefore \gcd(10, 45) = 5$

b) $45 = 10(4) + 5$

$10 = 5(2) + 0$ $\therefore \gcd(10, 45) = 5$

E29) $\gcd(1701, 3768) = 3$.

$3768 = 1701(2)+366$

$1701 = 366(4)+237$

$366 = 237(1)+129$

$237 = 129(1)+108$

$129 = 108(1)+21$

$108 = 21(5)+3$

$21 = 3(7)+0$

E30) $\gcd(12345, 54321) = 3$.

$54321 = 12345(4)+4941$

$12345 = 4941(2)+2463$

$4941 = 2463(2)+15$.

$2463 = 15(164)+3$

$15 = 3(5)+0$

E31) $\gcd(310, 710) = 10$.

$710 = 310(2)+90$

$310 = 90(3)+40$.

$90 = 40(2)+10$

$40 = 10(4)+0$

$10 = 90-(2)[310-90(3)]$

$= -(2)310+(7)90$.

$= -(2)310+(7)[710-310(2)]$.

$= (7)710-(16)310$.

$\therefore s = -16,\ t = 7$

E32) $\gcd(1701, 3768) = 3$.

$3768 = 1701(2)+366$.

$1701 = 366(4)+237$.

$366 = 237(1)+129$.

$237 = 129(1)+108$

$129 = 108(1)+21$

$108 = 21(5)+3$

$21 = 3(7)+0$

$3 = 108-5[129-108(1)]$.

$= (6)108-(5)129$

$= -(5)129+(6)[237-129(1)]$.

$= -(11)129+(6)237$.

$= (6)237-(11)[366-237(1)]$.

$= (17)237-(11)366$

$= -(11)366+(17)[1701-366(4)]$.

$= -(79)366+(17)1701$

$= (17)1701-(79)[3768-1701(2)]$

$= -(79)3768+(175)1701$.

$\therefore$ BI $= -79,\ 175$.

E33) $\gcd(12345, 54321) = 3$.

$54321 = 12345(4)+4941$.

$12345 = 4941(2)+2463$

$4941 = 2463(2)+15$.

$2463 = 15(164)+3$

$15 = 3(5)+0$

$3 = 2463-(164)[4941-2463(2)]$.

$= (329)2463-(164)4941$

$= -(164)4941+(329)[12345+4941(2)]$.

$= -(822)4941+(329)12345$.

$= (329)12345-(822)[54321-12345(4)]$.

$= -(822)54321+(3617)12345$

$\therefore$ B·I $= -822,\ 3617$.

E34) $\gcd(6664, 765) = 17$

$6664 = 765(8)+544$

$765 = 544(1)+221$

$544 = 221(2)+102$.

$221 = 102(2)+17$

$102 = 17(6)+0$

$17 = 221-(2)[544-221(2)]$.

$= -(2)544+(5)221$

$= -(2)544+(5)[765-544(1)]$.

$= (5)765-(7)544$.

$= (5)765-(7)[6664-765(8)]$

$= (61)765-(7)6664$.

$\therefore$ BI $= 61,\ -7$

E35) $\gcd(3,7)=1$

$7=3(2)+1$

$3=1(3)+0$

$\gcd=1$

$\Rightarrow 3 \pmod 7$ have inverse.

$1=(1)7-2(3)$.

$BI = 1,\ -2$.

$\therefore$ Inverse of $3 \pmod 7$ is 5

E36) 101 modulo 4621

$\gcd(101, 4621)=1$

$\Rightarrow 4621 = 101(45)+76$

$101 = 76(1)+25$

$76 = 25(3)+1$

$1=76-(3)25$ ...

$101=75(1)+26$.

$75=26(2)+23$.

$26=23(1)+3$.

$23=3(7)+2$

$3=2(1)+1$

$2=1(2)+0$

$1=3-(1)[23-3(7)]$

$=(8)3-(1)23$

$=-(1)23+8[26-23(1)]$

$=-(9)23+(8)26$

$=(8)26-9[75-26(2)]$

$=-(9)75+(26)26$

$\Rightarrow -(9)75+(26)[101-75(1)]$

$=(26)101-(35)75$

$=(26)101-(35)[4621-101(45)]$.

$=-(35)4621+(1601)101$.

$\therefore\ BI = -35,\ 1601$

$\therefore$ Inverse of 101 modulo 4620 is 1601

E37)

$\gcd(392, 27)=1$.

$\Rightarrow 392 = 27(14)+14$

$27 = 14(1)+13$.

$14 = 13(1)+1$

$13 = 1(13)+0$

$1=14-(1)[27-14(1)]$

$=-(1)27+(2)14$

$=-(1)27+(2)[392-27(14)]$

$=(2)392-(29)27$

$\therefore BI = 2,\ -29$

$\therefore 27^{-1} \pmod{392} = 363$.

E38) $(197)^{-1} \pmod{3000}$

$\gcd(3000, 197)=1$

$\Rightarrow 3000 = 197(15)+45$

$197 = 45(4)+17$

$45 = 17(2)+11$

$17 = 11(1)+6$.

$11 = 6(1)+5$

$6=5(1)+1$

$5=1(5)+0$

$1=6-(1)[11-6(1)]$.

$=-(1)(11)+2(6)$

$=-(1)11+(2)[17-11(1)] = (2)17-(3)11$

$=(2)17-(3)[45-17(2)] = -(3)45+(8)17$.

$=-(3)45+(8)[197-45(4)] = (8)197-(35)45$.

$=(8)197-(35)[3000-197(15)]$.

$=-(35)3000+(533)197$

$BI = -35,\ 533$.

$\therefore\ (197)^{-1} \pmod{3000}$ is 533

E39) inverse of $7 \pmod{25}$

$\gcd(7,25)=1$.

$\Rightarrow 25 = 7(3)+4$.

$7 = 4(1)+3$.

$4 = 3(1)+1$

$3 = 1(3)+0$

$1 = 4-(1)[7-4(1)]$

$=(2)4-(1)7 = -(1)7+(2)[25-7(3)]$.

$=(2)25-(7)7$

$\therefore BI = 2,\ -7$.

$\therefore$ Inverse of $7 \pmod{25} = 18$.

E40)

$9x \equiv 15 \pmod{24}$

$\gcd(9, 24) = 3$

$\Rightarrow 24 = 9(2)+6$

$9 = 6(1)+3$

$6 = 3(2)+0$

Since $3 \mid 15$, there are 3 solutions.

$3x \equiv 5 \pmod 8$ $=1$ ⇒ there is an inverse.

$\gcd(3, 8)$

$8 = 3(2)+2$

$3 = 2(1)+1$

$2 = 1(2)+0$

$1 = 3 - [8 - 3(2)]$

$= 3(3) - (1)8$

BI $= 3, -1$

∴ inverse is 3

$3 \cdot 3x \equiv 3 \cdot 5 \pmod 8$

$x = 15 \pmod 8$

∴ $x = 7$

∴ The solutions are

$7 \pmod{24}$, $15 \pmod{24}$, $23 \pmod{24}$.

E41) $42x \equiv 12 \pmod{90}$.

$\gcd(42, 90) = 6$. $6 \mid 12$, there are 6 Solutions.

$90 = 42(2)+6$

$42 = 6(7)+0$

$7x \equiv 2 \pmod{15}$ There is inverse.

$\gcd(7, 15) = 1$.

$15 = 7(2)+1$

$7 = 1(7)+0$

$1 = 15 - 7(2)$

BI $= 1$ & -2

∴ Inverse $= 13$

$\Rightarrow 13 \cdot 7 \equiv 13 \cdot 2 \pmod{15}$

$x = 26 \pmod{15} = 11$.

∴ The solutions are

$11 \pmod{90}$, $26 \pmod{90}$, $41 \pmod{90}$, $56 \pmod{90}$, $71 \pmod{90}$, $86 \pmod{90}$

E42) $55x \equiv 35 \pmod{75}$

$\gcd(55, 75) = 5$. Since $5 \mid 35$, there are 5 Solutions.

$75 = 55(1)+20$

$55 = 20(2)+15$

$20 = 15(1)+5$

$15 = 3(5)+0$

$11x \equiv 7 \pmod{15}$

$\gcd(11, 15) = 1$. gcd 1 ⇒ There is inverse

$15 = 11(1)+4$

$11 = 4(2)+3$

$4 = 3(1)+1$

$3 = 1(3)+0$

$1 = 4 - [11 - 4(3)]$

$= 11 + (3)[15 - 11(1)]$

$= (-4)11 + (3)15$

BI $= -4, 3$

∴ Inverse is 11.

$11 \cdot 11x \equiv 11 \cdot 7 \pmod{15}$

$x = 77 \pmod{15} = 2$.

∴ There are solutions

$2 \pmod{75}$

$17 \pmod{75}$

$32 \pmod{75}$

$47 \pmod{75}$

$62 \pmod{75}$

E43) $55x \equiv 36 \pmod{75} = 5$

$\gcd(55, 75)$

$75 = 55(1)+20$

$50 = 20(2)+5$

$20 = 5(4)+0$

$5 \nmid 36$, there is no solutions.

∴ Can't find x value

E44) $19x \equiv 4 \pmod{141}$

$\gcd(19, 141) = 1$

$141 = 19(7) + 8$

$19 = 8(2) + 3$

$8 = 3(2) + 2$

$3 = 2(1) + 1$

$2 = 1(2) + 0$

· Since $1 \mid 4$, there is 1 solution.

· $\gcd = 1 \Rightarrow$ there is inverse.

$1 = 3 - (1)[8 - 3(2)]$

$= -(1)8 + (3)3$

$= -(1)8 + (3)[19 - 8(2)]$

$= (3)19 - (7)8$

$= (3)19 - (7)[141 - 19(7)]$

$= (52)19 - (7)141$

BI $= 59, -7$ ∴ Inverse $= 52$.

$52 \cdot 19x \equiv 4 \cdot 52 \pmod{141}$

$x = 67$

∴ The Solution $\Rightarrow 67 \pmod{141}$
$= 67$.

E45) $55x \equiv 34 \pmod{89}$

$\gcd(55, 89) = 1$

$89 = 55(1) + 34$

$55 = 34(1) + 21$

$34 = 21(1) + 13$

$21 = 13(1) + 8$

$13 = 8(1) + 5$

$8 = 5(1) + 3$

$5 = 3(1) + 2$

$3 = 2(1) + 1$

$2 = 1(2) + 0$

· Since $1 \mid 34$, There is 1 solution

· $\gcd = 1$, there is inverse.

$1 = 3 - 2(1) = 3 - (1)[5 - 3(1)]$

$= -5 + (2)3 = -5 + (2)[8 - 5(1)]$

$= (2)8 - (3)5 = (2)8 - (3)[13 - 8(1)]$

$= (5)8 - (3)13 = -(3)13 + (5)[21 - 13(1)]$

$= (5)21 - (8)13 = (5)21 - 8[34 - 21(1)]$

$= -(8)34 + (13)21 = -(8)34 + (13)[55 - 34(1)]$

$= (13)55 - (21)34 = (13)55 - (21)[89 - 55(1)]$

$= -(21)89 + (34)55$

BI $= -21, 34$

∴ Inverse $= 34$

$34 \cdot 55x \equiv 34 \cdot 34 \pmod{89}$

$x = 1156 \pmod{89} = 88$

∴ The solution is $88 \pmod{89} = 88$.

E46) $89x \equiv 2 \pmod{232}$

$\gcd(89, 232)$

$\Rightarrow 232 = 89(2) + 54$

$89 = 54(1) + 35$

$54 = 35(1) + 19$

$35 = 19(1) + 16$

$19 = 16(1) + 3$

$16 = 3(5) + 1$

$3 = 1(3) + 0$

· Since $1 \mid 2$, there is 1 solution

· $\gcd = 1 \Rightarrow$ There is inverse.

$1 = 16 - (5)[19 - 16(1)]$

$= (-5)19 + 6[35 - 19(1)]$

$= (6)35 - (11)[54 - 35(1)]$

$= (-11)54 + (17)[89 - 54(1)]$

$= (17)89 - (28)[232 - 89(2)]$

$= (73)89 - (28)232$

∴ Inverse is 73.

$73 \cdot 89x \equiv 73 \cdot 2 \pmod{232}$

$x = 146 \pmod{232}$

∴ $x = 146$

E47) $3x \equiv 4 \pmod 7$

$\gcd(3,7) = 1$. Since $1 \mid 4$, 1 solution.

$7 = 3(2) + 1$

$3 = 1(3) + 0$

$1 = 7 - 3(2)$

Inverse $= 5$

$5 \cdot 3x \equiv 5 \cdot 4 \pmod 7$

$x = 20 \pmod 7 = 6$

E48) $56x \equiv 1 \pmod{93}$

$\gcd(56, 93)$ Since $1 \mid 1$, 1 solution.

$93 = 56(1) + 37$

$56 = 37(1) + 19$

$37 = 19(1) + 18$

$19 = 18(1) + 1$

$18 = 1(18) + 0$

$1 = 19 - (1)[37 - 19(1)]$

$= (2)19 - (1)37 = -(1)37 + (2)[56 - 37(1)]$

$= -(3)37 + (2)56 = (2)56 - (3)[93 - 56(1)]$

$= -(3)93 + (5)56$

$\therefore$ Inverse $= 5$

$5 \cdot 56x \equiv 1 \cdot 5 \pmod{93}$

$x = 5 \pmod{93} = 5$

E49) $5x \equiv 12 \pmod{19}$

$\gcd(5,19) = 1$ Since $1 \mid 12$, there are 1 solution

$19 = 5(3) + 4$

$5 = 4(1) + 1$

$4 = 1(4) + 0$

$1 = 5 - (1)4$

$= 5 - [19 - 5(3)]$

$= -(1)19 + (4)5$ $\therefore$ Inverse $= 4$

$5 \cdot 4x \equiv 4 \cdot 12 \pmod{19}$

$x = 4 \cdot 12 \pmod{19}$

$= 28 \pmod{19} = 9$

E50) $42x \equiv 12 \pmod{90}$

$\gcd(42, 90) = 6$. Since $6 \mid 12$, there are 6 solutions.

$90 = 42(2) + 6$

$42 = 6(7) + 0$

$7x \equiv 2 \pmod{15}$. $\gcd = 1$, There are inverse.

$\gcd(7, 15) = 1$

$15 = 7(2) + 1$

$7 = 1(7) + 0$

$1 = 15 - 7(2)$

$\therefore$ Inverse $= 13$

$13 \cdot 7x \equiv 13 \cdot 2 \pmod{15}$

$x = 26 \pmod{15} = 11$

$\therefore$ # Solutions

$11 \pmod{90}$

$26 \pmod{90}$

$41 \pmod{90}$

$56 \pmod{90}$

$71 \pmod{90}$

$86 \pmod{90}$ (same as Ex41)

E51)

$\gcd(2,3) = \gcd(3,5) = \gcd(2,7) = 1$

$\Rightarrow$ Pairwise Relatively prime.

		$M=330$		$a_i m_i y_i$
$x \equiv 1 \pmod 2$	$a_1 = 1$	$m_1 = 165$	$y_1 = 1$	165
$x \equiv 2 \pmod 3$	$a_2 = 2$	$m_2 = 110$	$y_2 = 2$	440
$x \equiv 3 \pmod 5$	$a_3 = 3$	$m_3 = 66$	$y_3 = 1$	198
$x \equiv 4 \pmod{11}$	$a_4 = 4$	$m_4 = 30$	$y_4 = 7$	840

$\Sigma = 1643$

$x = 1643 \pmod{330} = 323$

E52)

Since $\gcd(2,3) = \gcd(3,5) = \gcd(2,7) = 1$ $\Rightarrow$ Pairwise Relatively prime.

		$M = 105$		$a_i m_i y_i$
$x \equiv 2 \pmod 3$	$a_1 = 2$	$m_1 = 35$	$y_1 = 2$	140
$x \equiv 3 \pmod 5$	$a_2 = 3$	$m_2 = 21$	$y_2 = 1$	63
$x \equiv 2 \pmod 7$	$a_3 = 2$	$m_3 = 15$	$y_3 = 1$	30

$\Sigma = 233$

$x = 233 \pmod{105} = 23$.

E53)

Since $\gcd(1,2) = \gcd(2,3) = \gcd(3,5) = \gcd(4,7) = 1$

$\Rightarrow$ Pairwise Relatively prime.

		$M=210$		$a_i M_i y_i$
$x \equiv 1 \pmod 2$	$a_1 = 1$	$m_1 = 105$	$y_1 = 1$	105
$x \equiv 2 \pmod 3$	$a_2 = 2$	$m_2 = 70$	$y_2 = 1$	140
$x \equiv 3 \pmod 5$	$a_3 = 3$	$m_3 = 42$	$y_3 = 3$	378
$x \equiv 4 \pmod 7$	$a_4 = 4$	$m_4 = 30$	$y_4 = 4$	480

$\Sigma = 1103$

$x = 1103 \bmod 210 = 53$.

E55)

$2x \equiv 1 \pmod 5$ $\qquad$ $6x \equiv x \equiv 3 \pmod 5$.

$3x \equiv 9 \pmod 6$ $\rightarrow$ $x \equiv 3 \pmod 2$

$4x \equiv 1 \pmod 7$ $\qquad$ $8x \equiv x \equiv 2 \pmod 7$.

		$M=70$		$a_i m_i y_i$
$x \equiv 3 \pmod 5$	$a_1 = 3$	$m_1 = 14$	$y_1 = 4$	168
$x \equiv 3 \pmod 2$	$a_2 = 3$	$m_2 = 35$	$y_2 = 3$	315
$x \equiv 2 \pmod 7$	$a_3 = 2$	$m_3 = 10$	$y_3 = 5$	100

$\Sigma = 583$

$x = 583 \bmod 70 = 23$

Ex 56)

$$
\begin{aligned}
2x &\equiv 1 \pmod 5 \\
3x &\equiv 9 \pmod 6 \\
4x &\equiv 1 \pmod 7 \\
5x &\equiv 9 \pmod{11}
\end{aligned}
\quad \rightarrow \quad
\begin{aligned}
6x \equiv x &\equiv 3 \pmod 5 \\
x &\equiv 3 \pmod 2 \\
8x \equiv x &\equiv 2 \pmod 7 \\
45x \equiv x &\equiv 81 \pmod{11} \\
&\equiv 4 \pmod{11}.
\end{aligned}
$$

Since $\gcd(3,5) = \gcd(3,2) = \gcd(2,7) = \gcd(4,11) = 1$.

$\Rightarrow$ Pair wise relatively prime.

		$M = 770$		$a_i M_i y_i$
$x \equiv 3 \pmod 5$	$a_1 = 3$	$M_1 = 154$	$y_1 = 4$	1848
$x \equiv 3 \pmod 2$	$a_2 = 3$	$M_2 = 385$	$y_2 = 1$	1155
$x \equiv 2 \pmod 7$	$a_3 = 2$	$M_3 = 110$	$y_3 = 3$	660
$x \equiv 4 \pmod{11}$	$a_4 = 4$	$M_4 = 70$	$y_4 = 3$	840

$\Sigma = 4503.$

$x = 4503 \pmod{770} = 653.$