Name: Rajat Rajesh Shetty Assignment 2.
CWID: 10477484

Exercise 2.1

Solve a linear congruence $17x \equiv 3 \mod 210$

⇒ Step 1: Given $17x \equiv 3 \mod (210)$

$\therefore x = 17^{-1} 3 \mod 210$

Let calculate $17^{-1} \mod 210$

$210 = 17 \times 12 + 6$

$17 = 6 \times 2 + 5$

$6 = 5 \times 1 + 1$

Trace back,

$1 = 6 - 5$

$= 6 - (17 - 6 \cdot 2)$

$= 3 \times 6 - 17$

$= 3(210 - 17 \cdot 12) - 17$

$\Rightarrow 3 * 210 - 36 * 17 - 17$

$\Rightarrow 3 * 210 - 37 \cdot 17$

$210 - 37 = 173$

Thus, $17^{-1} \mod 210 = -37 \mod 210 = 173 \mod 210$

Step 2: hence

$x \equiv 17^{-1} * 3 \mod 210$

$\equiv 173 * 3 \mod 210$

$= 519 \mod 210$

$= 99 \mod 210$

Thus $x \equiv 99 \mod 210$

$\therefore 17 * 19 = 1683 \equiv 3 \mod 210$

Exercise 2.2

Find a general soln for linear Diophantine equation

$1485x + 1745y = 15$.

$\Rightarrow \quad 1485x + 1745y = 15.$

gcd(1485, 1785) gives:

$1785 = 1 \times 1485 + 260$

$1485 = 5 \times 260 + 185$

$260 = 1 \cdot 185 + 75$

$185 = 2 \cdot 75 + 35$

$75 = 2 \times 35 + 5$

$35 = 7 \cdot 5 + 0$

Back track, (extended eucidean algo)

$5 = (1 \cdot 75) + (-2 \cdot 35)$

$= (-2 \cdot 185) + (5 \cdot 75)$

$= (5 \cdot 260) + (-7 \cdot 185)$

$= (-7 \cdot 1485) + (40 \cdot 260)$

$= (40 \cdot 1785) + (-47 \cdot 1485)$

$\therefore$ particular soln $= x_0 = -141$

$y_0 = 120.$

Complete soln or general : $x = -141 + 349n$

$y = 120 - 297n.$

← reason →

gcd(1485, 1745) = 5

however, right side hand we are considering is not 5 but 15.

$\therefore (5) \times 3.$

$y_0 = 40 \times 3 = 120$

$x_0 = -47 \times 3 = -141$

$15 = 5 \times 3$

$= 3[40(1745) + (-47 \cdot 1485)$

$\Rightarrow 120(1745) - 141 \cdot 1485$

$\downarrow y_0 \qquad \downarrow x_0$

Exercise 2.3.

(a) find all unit modulo 24. for each unit find its multiplica-tive inverse.

$\Rightarrow U_{24} = \{1, 5, 7, 11, 13, 17, 19, 23\}$

$\because$ (i) $\gcd(24,1) = 1$ ✓
$\gcd(24,2) = 2$
$\gcd(24,3) = 3$
$\gcd(24,4) = 4$
$\gcd(24,5) = 1$ ✓
$\gcd(24,6) = 6$
$\gcd(24,7) = 1$ ✓
$\gcd(24,8) = 8$
$\gcd(24,9) = 3$
$\gcd(24,10) = 2$
$\gcd(24,11) = 1$ ✓
$\gcd(24,12) = 12$
$\gcd(24,13) = 1$ ✓
$\gcd(24,14) = 2$
$\gcd(24,15) = 3$
$\gcd(24,16) = 8$
$\gcd(24,17) = 1$ ✓
$\gcd(24,18) = 6$
$\gcd(24,19) = 1$ ✓
$\gcd(24,20) = 4$
$\gcd(24,21) = 3$
$\gcd(24,22) = 2$
$\gcd(24,23) = 1$ ✓

Multiplicative inverse.

$1^{-1} \bmod 24 = 1$ //
$5^{-1} \bmod 24 = 5$ //
$7^{-1} \bmod 24 = 7$ //
$11^{-1} \bmod 24 = 11$ //
$13^{-1} \bmod 24 = 13$ //
$17^{-1} \bmod 24 = 17$ //
$19^{-1} \bmod 24 = 19$ //
$23^{-1} \bmod 24 = 23$ //

$23^{-1} \bmod 24 = x$
$24 = 23 \times 1 + 1$
$\therefore x = 23$

How to find inverse

one eg.
$5^{-1} \bmod 24 = x$
$\gcd(5,24) = 1$
using eulean method
$24 = 5 \times 4 + 4$
$5 = 4 \times 1 + 1$
$\therefore x = 5$

(b) Compute PPF(2520) and $\varphi(2520)$

PPF (2520)
$2520 = 1260 * 2$
$\Rightarrow 630 * 2 \times 2$
$\Rightarrow 315 * 2 \times 2 \times 2$
$\Rightarrow 105 \times 3 * 2 \times 2 \times 2$
$\Rightarrow 35 \times 3^2 \times 2^3$
$\Rightarrow 7 \times 5 \times 3^2 \times 2^3$

$\therefore$ PPF(2520) $= 2^3 . 3^2 . 5 . 7$

$\varphi(2520)$
since we solved PPF of (2520)
$\varphi(2520) = \varphi(2^3) . \varphi(3^2) . \varphi(5) . \varphi(7)$
$\Rightarrow 4 . 6 . 4 . 6$
$\Rightarrow 576$

$|\varphi(n) = |on|$

we know Eulers formula of $\varphi(p^n)$
so $\varphi(p^n) = p^{n-1}(p-1)$
$\therefore \varphi(2^3) = 2^2 . (2-1)$
$\Rightarrow 4$

$\varphi(3^2) = 3 . (2)$
$\Rightarrow 6$

Exercise 2.4.

Solve the following system of congruences using $\sum c_i m_i d_i$ formula.

$$\begin{cases} x \equiv_1 3, \\ x \equiv_8 2, \\ x \equiv_9 1, \end{cases} \quad \text{or} \quad \begin{aligned} x &\equiv 3 \bmod 7 \\ x &\equiv 2 \bmod 8 \\ x &\equiv 1 \bmod 9 \end{aligned}$$

$c_i \to b_i$
$m_i \to n_i$
$d_i \Rightarrow x_i$

⇒ Lets solve it using general form.

So the general form is

$$x \equiv b_1 \pmod{n_1}$$
$$x \equiv b_2 \pmod{n_2}$$
$$x \equiv b_3 \pmod{n_3}$$

b_i	$N_i = \frac{N}{N_i}$	x_i	$b_i N_i x_i$
b_1	$N_1 = n_2 n_3$	x_1	$b_1 N_1 x_1$
b_2	$N_2 = N_1 n_3$	x_2	$b_2 N_2 x_2$
b_3	$N_3 = n_1 n_2$	x_3	$b_3 N_3 x_3$

b_i: remainder; x_i: inverse of N_i

$$N_i = \frac{N}{n_i}$$

$$N = n_1 n_2 n_3$$

$$x = \sum_{i=1}^{3} b_i N_i x_i \pmod{N}$$

So Lets us this general form to solve the given question,

$N = 7 \cdot 8 \cdot 9 = 504$

$n_1 = 7$, $n_2 = 8$, $n_3 = 9$

$N_1 = \frac{504}{7} = 72$

$N_2 = \frac{504}{8} = 63$ $\quad N_3 = \frac{504}{9} = 56$

b_i	N_i	x_i	$b_i N_i x_i$
3	72	4	864
2	63	7	882
1	56	5	280

To calculate x_i, we need to take inverse

$72 x_1 \equiv 1 \bmod 7$
$2 x_1 \equiv 1 \bmod 7$
$x_1 \equiv 4 \bmod 7$

$63 x_2 \equiv \bmod 8$
$7 x_2 \equiv 1 \bmod 8$
$x_2 \equiv 7 \bmod 8$

$56 x_3 \equiv 1 \bmod 9$
$2 x_3 \equiv 1 \bmod 9$
$x_3 \equiv 5 \bmod 9$

$\therefore x = 864 + 882 + 280 = 2026$ using formula, $x = \sum_{i=1}^{3} b_i N_i x_i \pmod{N}$

$x \equiv 2026 \bmod 504$.

$x \equiv 10 \bmod 504$

Check:

$10 \equiv 3 \bmod 7$
$10 \equiv 2 \bmod 8$
$10 \equiv 1 \bmod 9$

} rectified.

Exercise 2.5

(RSA Encryption) Let $n=91$ & $e=5$ by Alice public information. Encrypt the message $m=9$.

$\Rightarrow n=91 \quad e=5 \quad m=9.$

Let $n = p \times q$. p, q large prime no. p, q with $p<q$.

$= 7 \times 13.$ $\quad p=7 \; q=13$ $\quad 91 = 7 \times 13.$

Let $k = \varphi(n) = (p-1)\cdot(q-1)$

$= (6)\cdot(12)$

$\Rightarrow \underline{72}$

for encryption we know that, 'c'

$c = M^e \bmod n$

$\Rightarrow 9^5 \bmod 91$

$\Rightarrow 59049 \bmod 91$

$\boxed{C \Rightarrow 81}$

Exercise 2.6

(Breaking RSA) Let $n=77$ & $e=7$ by Alice public information. Let $C=3$ be the cipher intercepted by Eve. find orginal message m.

$\Rightarrow n=77 \quad e=7 \quad C=3.$

Let $n = p \times q$

$= 7 \times 11 \quad p=7 \; q=11$

Let $k = \varphi(n) = (p-1)\cdot(q-1)$

$= 6 \cdot 10 = 60$

we know that, to decrypt & find orignal message, formula is

$M = C^d \bmod n.$

$\therefore M = 38 = 3^{43} \bmod 77 = ((3^{16} \bmod 77) \times (3^{16} \bmod 77) \times (3^8 \bmod 77) \times (3^2 \bmod 77) \times (3 \bmod 77))$

$= (25 \times 25 \times 16 \times 9 \times 3) \bmod 77$

$= 270000 \bmod 77 = \underline{38}$

to calculate d we know that

$d = e^{-1} \bmod k$

$= 7^{-1} \bmod 60$

$43 \times 7 = 1 \bmod 60$

$\underline{d = 43}.$

$3^{43} = 3^{10} \cdot 3^{16} \cdot 3^8 \cdot 3^2 \cdot 3^1$

$3 \bmod 77 = 3$

$3^2 \bmod 77 = 9$

$3^8 \bmod 77 = 6561 \bmod 77 = 16$

$3^{16} \bmod 77 = 4304672 1 \bmod 77$

$= 25.$

Exercise 2.7

Check if the group axioms (G1), (G2), (G3) hold for the pairs $(G, \cdot)$ or $(G, +)$ in the table below. Put check marks in the corresponding cells. No explanation is required.

$a+0=0+a=a$
$a+(-a)=(-a)+a=0$

⇒

	identity (G1)	asso (G2)	inverse (G3)
$(\mathbb{Z}, +)$	✓	✓	✓
$(\mathbb{Z}, \cdot)$	✓	✓	×
$(\mathbb{N}, +)$	×	✓	×
$(\mathbb{N}, \cdot)$	✓	✓	×
$(\mathbb{Z}_n, +)$	✓	✓	✓
$(\mathbb{Z}_n, \cdot)$	✓	✓	×
$(\mathbb{Q}, +)$	✓	✓	✓
$(\mathbb{Q}, \cdot)$	✓	✓	×
$(\mathbb{Q} \setminus \{0\}, +)$	×	✓	✓
$(\mathbb{Q} \setminus \{0\}, \cdot)$	✓	✓	✓