Department of Computer Science
Ashoka University

Discrete Mathematics: CS-1104-1 & CS-1104-2

Assignment 8

Collaborators: None **Name: Rushil Gupta**

1 Straightforward

1. (a) $(1001011010)_2 = (001)_2(001)_2(011)_2(010)_2 = (1232)_8$

   (b) $(27365)_8 = (2)(7)(3)(6)(5) = (010)_2(111)_2(011)_2(110)_2(101) = (010111011110101)_2$
   $= (0010)_2(1110)_2(1111)_2(0101)_2 = (2EF5)_{16}$

   (c) $(5A2B79)_{16} = (0101)(1010)(0010)(1011)(0111)(1001)_2 = (010)(110)(100)(010)(101)(101)(111)(001)$
   $= (2)(6)(4)(2)(5)(5)(7)(1) = (26425571)_8$

2. (a) The Euclid's Algorithm for 143 and 91 is as follows:

$$\begin{aligned}
143 &= 91 \cdot 1 + 52 \\
91 &= 52 \cdot 1 + 39 \\
52 &= 39 \cdot 1 + 13 \\
39 &= 13 \cdot 3 + 0
\end{aligned}$$

   So, the GCD of 143 and 91 is 13. Now, we can find the Bezout's Coefficients by working backwards.

$$\begin{aligned}
13 &= 52 - 39 \cdot 1 \\
&= 52 - (91 - 52 \cdot 1) \cdot 1 \\
&= 52 - 91 + 52 \\
&= 2 \cdot 52 - 91 \\
&= 2 \cdot (143 - 91 \cdot 1) - 91 \\
&= 2 \cdot 143 - 3 \cdot 91
\end{aligned}$$

   Therefore, the Bezout's Coefficients for 143 and 91 are 2 and -3.

(b) The Euclid's Algorithm for 1932 and 735 is as follows:

$$\begin{aligned}
1932 &= 735 \cdot 2 + 462 \\
735 &= 462 \cdot 1 + 273 \\
462 &= 273 \cdot 1 + 189 \\
273 &= 189 \cdot 1 + 84 \\
189 &= 84 \cdot 2 + 21 \\
84 &= 21 \cdot 4 + 0
\end{aligned}$$

So, the GCD of 1932 and 735 is 21. Now, we can find the Bezout's Coefficients by working backwards.

$$\begin{aligned}
21 &= 189 - 84 \cdot 2 \\
&= 189 - (273 - 189 \cdot 1) \cdot 2 \\
&= 189 - 273 \cdot 2 + 189 \cdot 2 \\
&= 189 \cdot 3 - 273 \cdot 2 \\
&= (462 - 273 \cdot 1) \cdot 3 - 273 \cdot 2 \\
&= 462 \cdot 3 - 273 \cdot 5 \\
&= 462 \cdot 3 - (735 - 462 \cdot 1) \cdot 5 \\
&= 462 \cdot 8 - 735 \cdot 5 \\
&= (1932 - 735 \cdot 2) \cdot 8 - 735 \cdot 5 \\
&= 1932 \cdot 8 - 735 \cdot 21
\end{aligned}$$

Therefore, the Bezout's Coefficients for 1932 and 735 are 8 and -21.

(c) The Euclid's Algorithm for 45 and 64 is as follows:

$$\begin{aligned}
64 &= 45 \cdot 1 + 19 \\
45 &= 19 \cdot 2 + 7 \\
19 &= 7 \cdot 2 + 5 \\
7 &= 5 \cdot 1 + 2 \\
5 &= 2 \cdot 2 + 1 \\
2 &= 1 \cdot 2 + 0
\end{aligned}$$

So, the GCD of 45 and 64 is 1. Now, we can find the Bezout's Coefficients by working backwards.

$$\begin{aligned}
1 &= 5 - 2 \cdot 2 \\
&= 5 - (7 - 5 \cdot 1) \cdot 2 \\
&= 5 \cdot 3 - 7 \cdot 2 \\
&= (19 - 7 \cdot 2) \cdot 3 - 7 \cdot 2 \\
&= 19 \cdot 3 - 7 \cdot 8 \\
&= 19 \cdot 3 - (45 - 19 \cdot 2) \cdot 8 \\
&= 19 \cdot 19 - 45 \cdot 8 \\
&= (64 - 45 \cdot 1) \cdot 19 - 45 \cdot 8 \\
&= 64 \cdot 19 - 45 \cdot 27
\end{aligned}$$

Therefore, the Bezout's Coefficients for 45 and 64 are 19 and -27.

3. (a) To prove the statement, we start by noting that:

$$\operatorname{lcm}(a,b,c)\cdot\gcd(a,b,c)=a\cdot b\cdot c$$

This follows from the general property for three numbers x, y, z:

$$\operatorname{lcm}(x,y,z)\cdot\gcd(x,y,z)=\operatorname{lcm}(\gcd(x,y),\gcd(y,z),\gcd(z,x))\cdot\gcd(x,y,z)$$

And knowing:

$$\operatorname{lcm}(x,y)\cdot\gcd(x,y)=x\cdot y$$

Now, considering the properties of gcd and lcm:

- $\operatorname{lcm}(a,b)\cdot\gcd(a,b)=a\cdot b$
- $\operatorname{lcm}(b,c)\cdot\gcd(b,c)=b\cdot c$
- $\operatorname{lcm}(c,a)\cdot\gcd(c,a)=c\cdot a$

Substituting these into the equation, we get:

$$a\cdot b\cdot c\cdot\operatorname{lcm}(a,b,c)=\gcd(a,b,c)\cdot\left(\frac{a\cdot b}{\gcd(a,b)}\right)\cdot\left(\frac{b\cdot c}{\gcd(b,c)}\right)\cdot\left(\frac{c\cdot a}{\gcd(c,a)}\right)$$

We then rearrange and simplify using properties of gcd (gcd is multiplicative under independent products), leading us to:

$$a\cdot b\cdot c\cdot\operatorname{lcm}(a,b,c)=\gcd(a,b,c)\cdot\operatorname{lcm}(a,b)\cdot\operatorname{lcm}(b,c)\cdot\operatorname{lcm}(c,a)$$

(b) To prove the statement, we start by noting that:

$$\operatorname{lcm}(a,b,c)\cdot\gcd(a,b)\cdot\gcd(b,c)\cdot\gcd(c,a)=\gcd(a,b,c)\cdot a\cdot b\cdot c$$

Using the identity:

$$\operatorname{lcm}(x,y,z)\cdot\gcd(x,y,z)=x\cdot y\cdot z$$

We apply it directly here. By considering the multiplicative properties of gcd and the identity for lcm and gcd:

- $\gcd(a,b,c)$ is a factor of $\gcd(a,b)$, $\gcd(b,c)$, and $\gcd(c,a)$
- $\operatorname{lcm}(a,b,c)\cdot\gcd(a,b,c)=a\cdot b\cdot c$

Thus, the product on the left:

$$\operatorname{lcm}(a,b,c)\cdot\gcd(a,b)\cdot\gcd(b,c)\cdot\gcd(c,a)$$

is equivalent to multiplying each a, b, c by their respective gcd terms, and these are all parts of the product $a\cdot b\cdot c$, hence:

$$\operatorname{lcm}(a,b,c)\cdot\gcd(a,b,c)=a\cdot b\cdot c$$

4. (a) To solve the linear congruence $3x \equiv 4 \pmod 7$, we first find the multiplicative inverse of 3 modulo 7. We need an integer y such that $3y \equiv 1 \pmod 7$. By trial, checking multiples of 3:

$$\begin{aligned}
&3 \times 1 \equiv 3 \pmod 7 \\
&3 \times 2 \equiv 6 \pmod 7 \\
&3 \times 3 \equiv 9 \equiv 2 \pmod 7 \\
&3 \times 4 \equiv 12 \equiv 5 \pmod 7 \\
&3 \times 5 \equiv 15 \equiv 1 \pmod 7
\end{aligned}$$

Thus, $y = 5$ is the inverse of 3 modulo 7. Multiplying both sides of the congruence $3x \equiv 4 \pmod 7$ by 5 gives:

$$\begin{aligned}
5 \cdot 3x &\equiv 5 \cdot 4 \pmod 7 \\
x &\equiv 20 \equiv 6 \pmod 7
\end{aligned}$$

Therefore, the solution to the linear congruence is $x \equiv 6 \pmod 7$.

(b) To solve the linear congruence $5x \equiv -5 \pmod{12}$, we seek the multiplicative inverse of 5 modulo 12. Checking multiples of 5:

$$\begin{aligned}
&5 \times 1 \equiv 5 \pmod{12} \\
&5 \times 2 \equiv 10 \pmod{12} \\
&5 \times 3 \equiv 15 \equiv 3 \pmod{12} \\
&5 \times 5 \equiv 25 \equiv 1 \pmod{12}
\end{aligned}$$

So, the inverse is 5. Multiplying the congruence $5x \equiv -5 \pmod{12}$ by 5:

$$\begin{aligned}
25x &\equiv -25 \pmod{12} \\
x &\equiv -25 \equiv 11 \pmod{12}
\end{aligned}$$

Therefore, the solution to the linear congruence is $x \equiv 11 \pmod{12}$.

(c) To solve the linear congruence $4x \equiv 12 \pmod 8$, we simplify the congruence:

$$4x \equiv 12 \equiv 4 \pmod 8$$

Dividing through by 4 (noting gcd(4, 8) divides 4):

$$x \equiv 1 \pmod 2$$

Therefore, the solution to the linear congruence is $x \equiv 1 \pmod 2$ (all odd numbers).

(d) To solve the linear congruence $4x \equiv 11 \pmod 8$, we first reduce $11 \pmod 8$:

$$4x \equiv 11 \equiv 3 \pmod 8$$

The equation $4x \equiv 3 \pmod 8$ suggests no solution because $4x \mod 8$ can only be 0, 4 due to x being an integer, and $4x$ is always even while 3 is odd.

5. (a) We have the following congruences:

- $x \equiv 3 \pmod 5$
- $x \equiv 2 \pmod 7$
- $x \equiv 5 \pmod{11}$

We can solve the system of congruences using the Chinese Remainder Theorem. We first find $M = 5 \cdot 7 \cdot 11 = 385$. Now we can find the partial products, $M_1 = 385/5 = 77$, $M_2 = 385/7 = 55$, and $M_3 = 385/11 = 35$. Now we can find the modular inverses of the partial products with respect to the moduli.

- Inverse of 77 modulo 5: The inverse of 77 modulo 5 is 3, since $77 \cdot 3 \equiv 231 \equiv 1 \pmod 5$.
- Inverse of 55 modulo 7: The inverse of 55 modulo 7 is 6, since $55 \cdot 6 \equiv 330 \equiv 1 \pmod 7$.
- Inverse of 35 modulo 11: The inverse of 35 modulo 11 is 6, since $35 \cdot 6 \equiv 210 \equiv 1 \pmod{11}$.

Now we can find the solution to the system of congruences:

$$\begin{aligned} x &= 3 \cdot 77 \cdot 3 + 2 \cdot 55 \cdot 6 + 5 \cdot 35 \cdot 6 \\ &= 693 + 660 + 1050 \\ &= 2403 \equiv 385 \cdot 6 + 93 \equiv 93 \pmod{385} \end{aligned}$$

(b) We have the following congruences:

- $x \equiv 5 \pmod 6$
- $x \equiv 2 \pmod{35}$
- $x \equiv 37 \pmod{143}$

We can solve the system of congruences using the Chinese Remainder Theorem. We first find $N = 6 \cdot 35 \cdot 143 = 30030$. Now we can find the partial products, $M_1 = 30030/6 = 5005$, $M_2 = 30030/35 = 858$, and $M_3 = 30030/143 = 210$. Now we can find the modular inverses of the partial products with respect to the moduli.

- Inverse of 5005 modulo 6: The inverse of 5005 modulo 6 is 1, since $5005 \cdot 1 \equiv 1 \pmod 6$.
- Inverse of 858 modulo 35: The inverse of 858 modulo 35 is 2, since $858 \cdot 2 \equiv 1 \pmod{35}$.
- Inverse of 210 modulo 143: The inverse of 210 modulo 143 is 111, since $210 \cdot 111 \equiv 1 \pmod{143}$.

Now we can find the solution to the system of congruences:

$$\begin{aligned} x &= 5 \cdot 5005 \cdot 1 + 2 \cdot 858 \cdot 2 + 37 \cdot 210 \cdot 111 \\ &= 25025 + 3432 + 862470 \\ &= 890927 \equiv 20057 \pmod{30030} \end{aligned}$$

(c) We have the following congruences:

- $11x \equiv 33 \pmod{55}$
- $5x \equiv 10 \pmod{35}$
- $7x \equiv 35 \pmod{77}$

First, we can divide each of the congruences to simplify them as follows:

- $x \equiv 3 \pmod 5$
- $x \equiv 2 \pmod 7$
- $x \equiv 5 \pmod{11}$

From part (a), we know that the solution to this system of congruences is $x \equiv 93 \pmod{385}$.

(d) We have the following congruences:

- $x \equiv 5 \pmod 6$
- $2x \equiv 6 \pmod 8 \equiv x \equiv 3 \pmod 4$

By brute force, we can see that $x = 11$ satisfies the equations.

2 $\neg$Straightforward

1. a

3 Bonus

1. a