UNIT 2

UNIT II SYMMETRIC CIPHERS 9

Number theory – Algebraic Structures – Modular Arithmetic - Euclid‘s algorithm – Congruence and matrices – Group, Rings, Fields, Finite Fields

SYMMETRIC KEY CIPHERS: SDES – Block Ciphers – DES, Strength of DES – Differential and linear cryptanalysis – Block cipher design principles – Block cipher mode of operation – Evaluation criteria for AES – Pseudorandom Number Generators – RC4 – Key distribution.

DIVISIBILITY

a $\quad$ b $\quad$ <u>quotient</u>

$45 \div 5 \Rightarrow 9$ $\quad$ rem $= 0$ $\Rightarrow$ 5 is a divisor of 45.

$45 \div 10 \Rightarrow 4$ $\quad$ rem $= 5$

$b \mid a$

Properties

- If $a \mid 1$, then $a = \pm 1$. ✓
- If $\underline{a \mid b}$ and $\underline{b \mid a}$, then $a = \pm b$. ✓
- Any $b \neq 0$ divides 0.
- If $a \mid b$ and $b \mid c$, then $a \mid c$:

$a \quad b$

$5 \quad -5$

$0/x \quad x \neq 0$

$\Rightarrow \dfrac{45 \to b}{5 \to a} \qquad \dfrac{90 - c}{45 \; - b} \qquad \Rightarrow \dfrac{90}{5}$ ✓

- If $b \mid g$ and $b \mid h$, then $b \mid (mg + nh)$ for arbitrary integers m and n.

Division Algorithm

a   b

90   8

$q \Rightarrow 11$

$8 \,\overline{)\,90}$

88

rem $\Rightarrow \underline{2}$

$90 = 11 \times 8 + 2$ → remainder

↳ divisor

↳ quotient

$a = n\,b + \text{rem}$; $\underline{0 \le r < n}$

↳ quotient

$q = \left\lfloor \frac{a}{b} \right\rfloor$ → floor

$\frac{45}{10} = \lfloor 4.5 \rfloor = 4$ //

The Division Algorithm

Given any positive integer n and any nonnegative integer a, if we divide a by n, we get an integer quotient q and an integer remainder r that obey the following relationship:

$$\boxed{a = qn + r} \qquad 0 \le r < n; \; q = \lfloor a/n \rfloor \tag{2.1}$$

$$\begin{array}{lllll}
a = 11; & n = 7; & 11 = 1 \times 7 + 4; & r = 4 & q = 1 \\
a = -11; & n = 7; & -11 = (-2) \times 7 + 3; & r = 3 & q = -2
\end{array}$$

LIKE

COMMENT

SHARE

SUBSCRIBE

Euclidean Algorithm - To Find GCD/HCF

The Highest Common Factor (HCF) of two numbers is the highest possible number that divides both the numbers completely. The Highest Common Factor (HCF) is also called the Greatest Common Divisor (GCD).

✓ ✓

45, 15

$\frac{\cancel{45}^{9}}{\cancel{5}}$ ✓ $\frac{\cancel{15}^{3}}{\cancel{5}}$ ✓ $\Rightarrow \boxed{5}$ // X

$\frac{\cancel{45}^{3}}{\cancel{15}}$ ~~45~~ $\frac{\cancel{15}^{1}}{\cancel{15}}$ ✓ $\Rightarrow \boxed{15}$

HCF (45, 15) = 15 //

Eg 1 . Find HCF of $\overset{a}{45}$,$\overset{b}{1\cancel{5}0}$

LHS max

Step 1 $a = qb + r$

$$45 = \overset{q}{4} \times \overset{b}{10} + \overset{rem}{5}$$

$$10 = 2 \times \boxed{5} + \underset{m}{0}$$

Rem $= 0 \Rightarrow$ Stop

HCF(45,10) = 5//

$$\begin{array}{r|l} & 4 \\ 10 & 45 \\ & 40 \\ \hline & 5 \end{array}$$

$$\begin{array}{r|l} & 2 \\ 5 & 10 \\ & 10 \\ \hline & 0 \end{array}$$

Eg 2 Find HCF of 710,310

$$\underline{a = qb + r}$$

$$710 = \overset{q}{2} \times \overset{b}{310} + \overset{r}{90}$$

$$310 = 3 \times 90 + 40$$

$$90 = 2 \times 40 + 10$$

$$40 = 4 \times \boxed{10} + \underline{\underline{0}}$$

rem = 0

<u>Stop</u>

HCF (710,310)
= 10 //

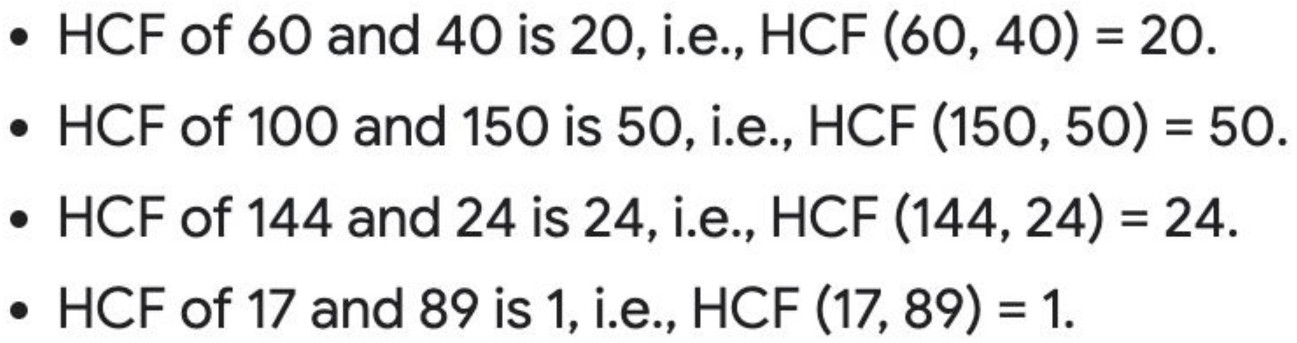
$$\begin{array}{r|l} & \;\;2 \\ \hline 310 & 710 \\ & -620 \\ \hline & \;\;\;90 \end{array}$$

$$\begin{array}{r|l} & \;\;3 \\ \hline 90 & 310 \\ & 270 \\ \hline & \;\;40 \end{array}$$

$$\begin{array}{r|l} & \;\;2 \\ \hline 40 & 90 \\ & 80 \\ \hline & 10 \end{array}$$

$$\begin{array}{r|l} & \;4 \\ \hline 10 & 40 \\ & 40 \\ \hline & \;0 \end{array}$$

Practise



- HCF of 60 and 40 is 20, i.e., HCF (60, 40) = 20.
- HCF of 100 and 150 is 50, i.e., HCF (150, 50) = 50.
- HCF of 144 and 24 is 24, i.e., HCF (144, 24) = 24.
- HCF of 17 and 89 is 1, i.e., HCF (17, 89) = 1.

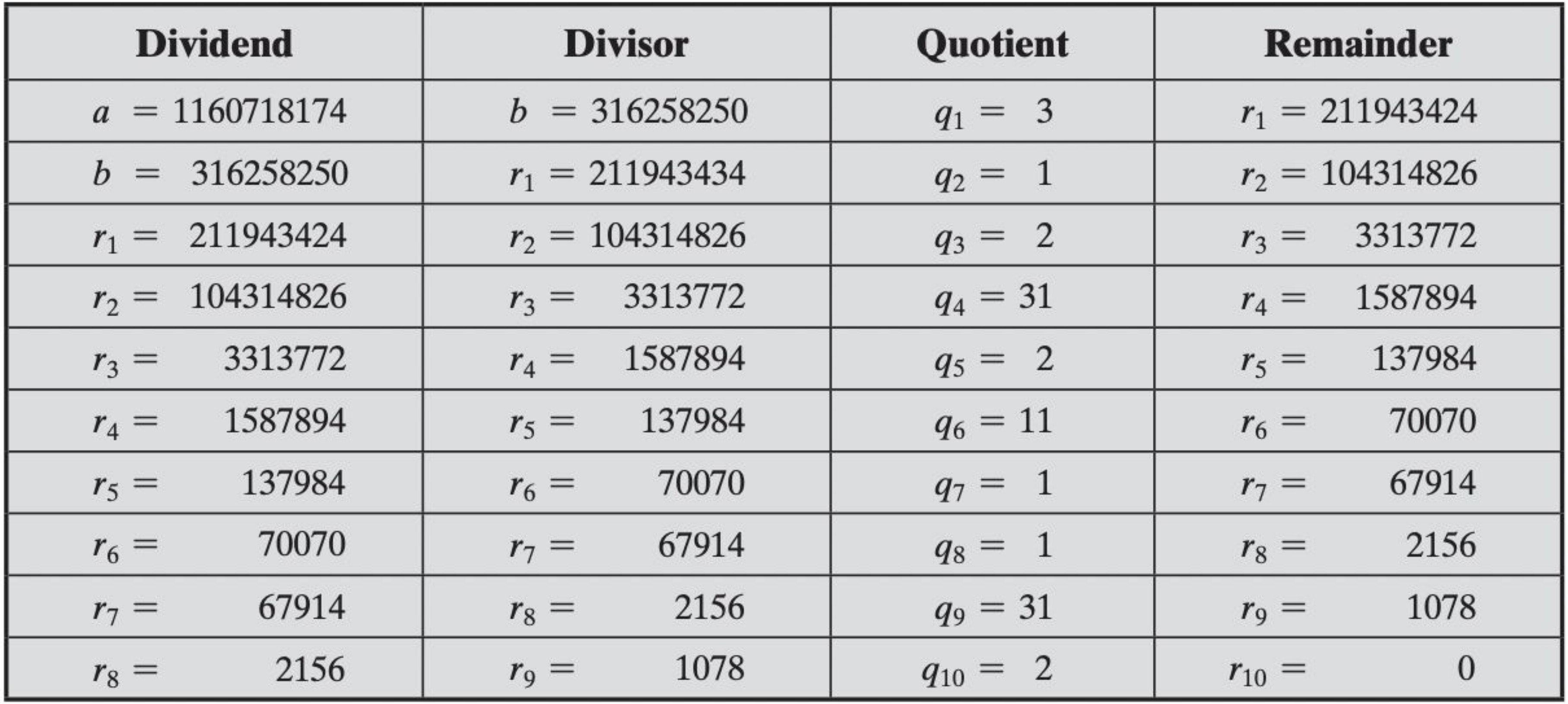


Table 2.1 Euclidean Algorithm Example

Dividend	Divisor	Quotient	Remainder
$a = 1160718174$	$b = 316258250$	$q_1 = 3$	$r_1 = 211943424$
$b = 316258250$	$r_1 = 211943434$	$q_2 = 1$	$r_2 = 104314826$
$r_1 = 211943424$	$r_2 = 104314826$	$q_3 = 2$	$r_3 = 3313772$
$r_2 = 104314826$	$r_3 = 3313772$	$q_4 = 31$	$r_4 = 1587894$
$r_3 = 3313772$	$r_4 = 1587894$	$q_5 = 2$	$r_5 = 137984$
$r_4 = 1587894$	$r_5 = 137984$	$q_6 = 11$	$r_6 = 70070$
$r_5 = 137984$	$r_6 = 70070$	$q_7 = 1$	$r_7 = 67914$
$r_6 = 70070$	$r_7 = 67914$	$q_8 = 1$	$r_8 = 2156$
$r_7 = 67914$	$r_8 = 2156$	$q_9 = 31$	$r_9 = 1078$
$r_8 = 2156$	$r_9 = 1078$	$q_{10} = 2$	$r_{10} = 0$

Flowchart

Modular Arithmetic

↳ remainder

+ve

a mod n

45 mod 20 = 5//

$$\begin{array}{r} 2 \\ 20\,\overline{)\,45} \\ 40 \\ \hline 5 \end{array}$$

1) 11 mod 3 = 2//

2) 11 mod 40 = 11

3) 11 mod 11 = 0

4) 11 mod 5 = 1//

5) 11 mod 7 = 4//

Mod of Negative Numbers

$$\boxed{-a \bmod n \Rightarrow n - (a \bmod n)}$$

① $-\overset{a}{11} \bmod \overset{n}{3} = 3 - (11 \bmod 3)$

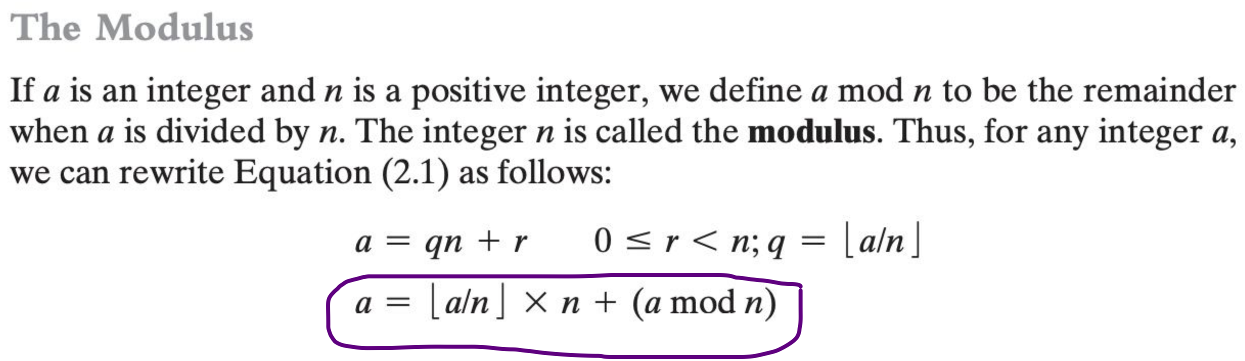
$= 3 - 2 = 1$ //

② $-11 \bmod 40 \Rightarrow 40 - (11 \bmod 40)$

$= 40 - 11 = 29$

③ $-11 \bmod 5 \Rightarrow 5 - (11 \bmod 5)$

$= 5 - 1 = 4$ //



The Modulus

If a is an integer and n is a positive integer, we define a mod n to be the remainder when a is divided by n. The integer n is called the **modulus**. Thus, for any integer a, we can rewrite Equation (2.1) as follows:

$$a = qn + r \qquad 0 \le r < n; q = \lfloor a/n \rfloor$$

$$\boxed{a = \lfloor a/n \rfloor \times n + (a \bmod n)}$$

Congruent Modulo

$\overset{a}{73}$ mod $\overset{n}{23}$ = 4 //

$\underset{b}{4}$ mod $\underset{n}{23}$ = 4

=> $a \equiv b \bmod n$ => $73 \equiv 4 \bmod 23$ //

Properties of Congruences

Congruences have the following properties:

1. $a \equiv b \pmod{n}$ if $n \mid (a - b)$.
2. $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$.
3. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply $a \equiv c \pmod{n}$.

a

$73 \bmod 23$

$b \equiv 4 \bmod 23$

$69/23$ ✓

$73 \equiv 4 \bmod 23$

$4 \equiv 73 \bmod 23$

Modular arithmetic exhibits the following properties:

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

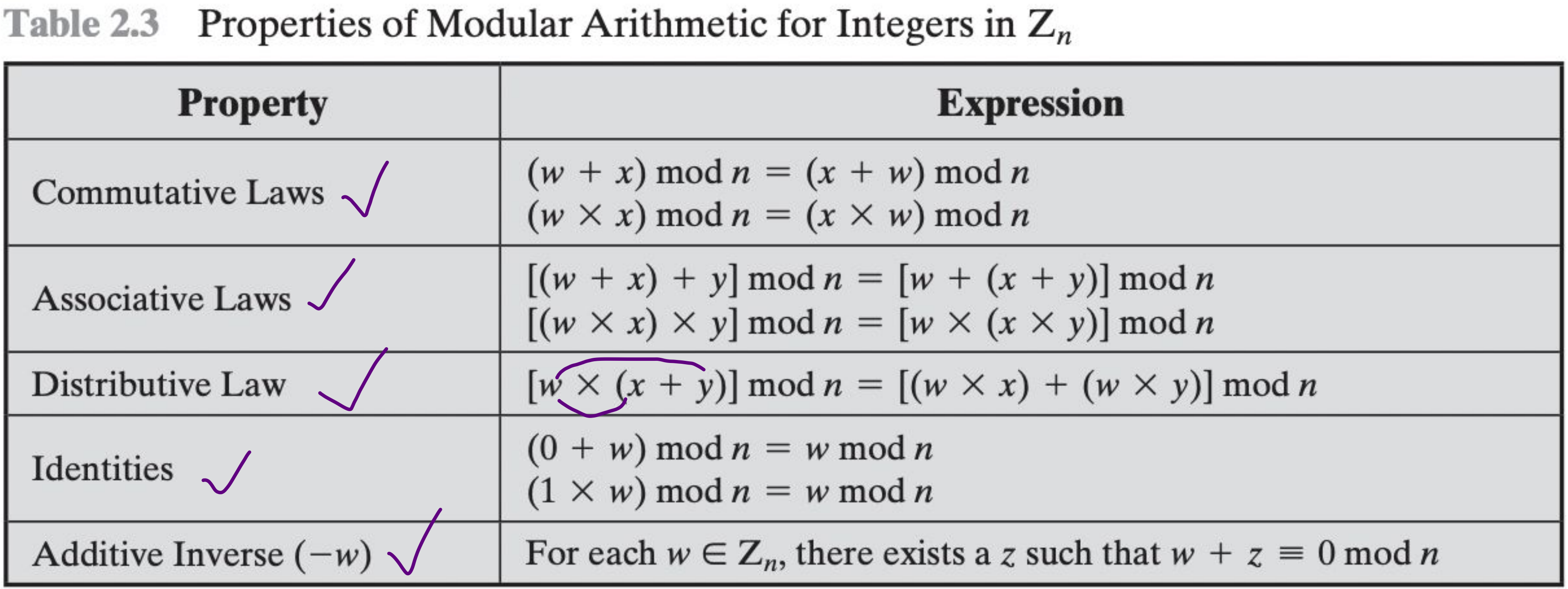


Table 2.3 Properties of Modular Arithmetic for Integers in Z_n

Property	Expression
Commutative Laws ✓	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative Laws ✓	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive Law ✓	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
Identities ✓	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive Inverse $(-w)$ ✓	For each $w \in Z_n$, there exists a z such that $w + z \equiv 0 \bmod n$

Extended Euclid- When needed

$\underline{\underline{x, y}}$

LIKE

COMMENT

SHARE

SUBSCRIBE