CSE4003- CyberSecurity

Digital Assignment-1

Alokam Nikhitha

19BCE2555

19BCE2555

Method1 Inspection method

a) gcd (24,54)

This involves 2 numbers 24 and 54

Start with smallest number i.e, 24

→ 24 divides 24 but it doesnot divide 54

So we take next largest integer that divides only 24. It is 12. by inspection.

→ 12 divides 24 but it doesnot divide 54

So, we take next largest integer that divides only 24. It is '8'. by inspection.

→ 8 divides 24 but it doesnot divide 54

So, we take next largest integer that divides only 24. It is '6'.

→ 6 divides both 24 and 54

∴ '6' is GCD of given two numbers 24 and 54.

b) gcd (18,42)

Start with 18 (because it is small between given 2 numbers)

→ 18 doesnot divide 42.

so, we take next largest number that divides only 18 by inspection. It is '9'.

→ 9 divides 18 but it doesnot divide 42.

so, we take next largest number by inspection it is '6'

→ 6 divides both 18 and 42.

Hence, GCD of 18 and 42 is '6'

Method 2 Prime Factorization method

(c) gcd (244, 354)

$244 = 2^2 \cdot 61 = 2 \cdot 2 \cdot 61$

$$\begin{array}{r|l} 2 & 244 \\ \hline 2 & 122 \\ \hline & 61 \end{array}$$

$354 = 2 \cdot 3 \cdot 59 = 2 \cdot 3 \cdot 59$

$$\begin{array}{r|l} 2 & 354 \\ \hline 3 & 177 \\ \hline & 59 \end{array}$$

The common factors is/are = '2'

$\therefore$ gcd (244, 354) = 2.

(d) gcd (128, 423)

$$\begin{array}{r|l} 2 & 128 \\ \hline 2 & 64 \\ \hline 2 & 32 \\ \hline 2 & 16 \\ \hline 2 & 8 \\ \hline 2 & 4 \\ \hline & 2 \end{array} \qquad \begin{array}{r|l} 3 & 423 \\ \hline 3 & 141 \\ \hline & 47 \end{array}$$

$128 = 2^7 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2$

$423 = 3^2 \cdot 47 = 3 \cdot 3 \cdot 47$

There are no common factors

$\therefore$ GCD (128, 423) = 1

Method3 Euclidean Algorithm 19BCE2555

(e) gcd (2415, 3289).

$$\begin{array}{r} 2415\overline{)3289}(1 \\ 2415 \\ \hline 874 \end{array}$$

$3289 = 2415\times1 + 874$

$$\begin{array}{r} 874\overline{)2415}(2 \\ 1748 \\ \hline 667 \end{array}$$

$2415 = 874\times2 + 667$

$$\begin{array}{r} 667\overline{)874}(1 \\ 667 \\ \hline 207 \end{array}$$

$874 = 667\times1 + 207$

$$\begin{array}{r} 207\overline{)667}(3 \\ 621 \\ \hline 46 \end{array}$$

$667 = 207\times3 + 46$

$$\begin{array}{r} 46\overline{)207}(4 \\ 184 \\ \hline 23 \end{array}$$

$207 = 46\times4 + 23$

$$\begin{array}{r} 23\overline{)46}(2 \\ 46 \\ \hline 0 \end{array}$$

$46 = 23\times2 + 0$

$\therefore$ GCD of 2415 and 3289 is '23'.

(f) GCD (4278, 8602)

19BCE2555

$$4278 \overline{)\,8602\,}(2$$
$$8556$$
$$46$$

$8602 = 4278 \times 2 + 46$

$$46 \overline{)\,4278\,}(93$$
$$4278$$
$$0$$

$4278 = 46 \times 93 + 0$

$\therefore$ GCD of 4278 and 8602 is '46'

(g) GCD(406, 555)

$$406 \overline{)\,555\,}(1$$
$$406$$
$$149$$

$555 = 406 \times 1 + 149$

$$149 \overline{)\,406\,}(2$$
$$298$$
$$108$$

$406 = 149 \times 2 + 108$

$$108 \overline{)\,149\,}(1$$
$$108$$
$$41$$

$149 = 108 \times 1 + 41$

$$41 \overline{)\,108\,}(2$$
$$82$$
$$26$$

$108 = 41 \times 2 + 26$

$$26 \overline{)\,41\,}(1$$
$$26$$
$$15$$

$41 = 26 \times 1 + 15$

$$15 \overline{)\,26\,}(1$$
$$15$$
$$11$$

$26 = 15 \times 1 + 11$

19BCE2555

$11\overline{)15}(1$
$\underline{11}$
4

$15 = 11\times 1 + 4$

$4\overline{)11}(2$
$\underline{8}$
3

$11 = 4\times 2 + \cancel{8}3$

$3\overline{)4}(1$
$\underline{3}$
1

$4 = 3\times 1 + 1$

$1\overline{)3}(3$
$\underline{3}$
0

$3 = 3\times 1 + 0$

$\therefore$ GCD of 406 and 555 is '<u>1</u>'.

19BCE2555

4) Fermant's theorom

h.) remainder when 3^{1105} divided by 23.

By Fermant's theorom,

we have $3^{22} \equiv 1 \mod 23$

Thus, $3^{1105} = 3^{22\times 50+5}$

$= (3^{22})^{50} \cdot (3^5)$

$\equiv 3^5 = 3^2 \cdot (27)$

$\equiv 9 \cdot (23+4) \equiv 9 \cdot 4$

$= \underline{13 \mod 23}$.

$$\begin{array}{r} 22)\,1105\,(50 \\ 110 \\ \hline (5) \end{array}$$

i.) remainder when 2^{9980} when divided by 37.

By Fermant's theorom, we have

$2^{36} \equiv 1 \mod 37$

$2^{9980} = 2^{36\times 277+8} = (2^{277})^{36} \cdot (2^8)$

$\equiv 2^8 = 2 \cdot (128) = 2 \cdot (111+17)$

$= 2 \cdot (3\times 37+17) \equiv \underline{34 \mod 37}$

$$\begin{array}{r} 36)\,9980\,(2778 \\ 9972 \\ \hline (8) \end{array}$$

$$\begin{array}{r} 37 \\ \times 3 \\ \hline 111 \end{array}$$

Ans: 34

Scanned with CamScanner

19BCE2555

j.) remainder of 2^{3000} when divided by 35.

By Fermant's theorom,

we have $2^{34} \equiv 1 \bmod 35$

$2^{3000} = 2^{34\times88+8} = \left(2^{88}\right)^{34} + 2^{8}$

$34 \overline{)3000}(88$
2992
8

$\equiv 2^{8} = 2.2^{7} = 2.(128)$

$= 2.(105+23)$

$= 2.(35\times3+23)$

$\equiv 2\times23 = 46$

$\equiv 11 \bmod 35$

$35 \times 3 = 105$

$46 - 35 = 11$

Ans: 11

k.) remainder of 2^{1000}, when divided by 27.

By Fermant's theorom, we have $2^{26} \equiv 1 \bmod 27$

$2^{1000} = 2^{26\times38+12} = \left(2^{38}\right)^{26} \times 2^{12}$

$26) 1000 (38$
988
12

$\equiv 2^{12} = 2^{2}.(2^{5})^{2}$

$= 4.(27+5)^{2}$

$\equiv 4.5^{2}$

$= 81+19$

$\equiv 19 \bmod 27$

$27 \times 3 = 81$

Ans: 19

19BCE2555

5) Euclidean Algorithm

1.) Find multiplicative inverse of 37 modulo 53.

We have, $53 = 1 \times 37 + 16$

$37 = 2 \times 16 + 5$

$16 = 3 \times 5 + 1$

Thus

$1 = 16 - 3 \times 5$

$1 = 16 - 3 \times (37 - 2 \times 16)$

$= 7 \times 16 - 3 \times 37$

Ans: 43

$= 7 \times (53 - 1 \times 37) - 3 \times 37$

$= 7 \times 53 - 10 \times 37$

$\therefore$ multiplicative inverse $(53 - 10) = 43$.

ii) Find multiplicative inverse of 35 modulo 59

$59 = 35 \times 1 + 24$

$35 = 24 \times 1 + 11$

$24 = 2 \times 11 + 2$

$11 = 5 \times 2 + 1$

$1 = 11 - 5 \times 2$

$= 11 - 5 \times (24 - 2 \times 11) = 11 \times 11 - 5 \times 24$

$= 11 \times (35 - 1 \times 24) - 5 \times 24$

$= 11 \times 35 - 16 \times 24$

$= 11 \times 35 - 16 \times (59 - 1 \times 35) = 27 \times 35 - 16 \times 59$

$= 27 \times 35 - 16 \times 59$

$\therefore$ Multiplicative inverse of 35 modulo 59

is 27.

Ans: 27