1.5 Question 5

1.5.A Find gcd(85327, 59840).

$$
\begin{array}{rrcl}
a = 85327,\ b = 59840 & & & \\
\Rightarrow & 85327 \div 59840 & = & 1\ R\ 25487 \\
\text{SWITCH: } a = b,\ b = R & & & \\
a = 59840,\ b = 25487 & & & \\
\Rightarrow & 59840 \div 25487 & = & 2\ R\ 8866 \\
\text{SWITCH: } a = b,\ b = R & & & \\
a = 25487,\ b = 8866 & & & \\
\Rightarrow & 25487 \div 8866 & = & 2\ R\ 7755 \\
\text{SWITCH: } a = b,\ b = R & & & \\
a = 8866,\ b = 7755 & & & \\
\Rightarrow & 8866 \div 7755 & = & 1\ R\ 1111 \\
\text{SWITCH: } a = b,\ b = R & & & \\
a = 7755,\ b = 1111 & & & \\
\Rightarrow & 7755 \div 1111 & = & 6\ R\ 1089 \\
\text{SWITCH: } a = b,\ b = R & & & \\
a = 1111,\ b = 1089 & & & \\
\Rightarrow & 1111 \div 1089 & = & 1\ R\ 22 \\
\text{SWITCH: } a = b,\ b = R & & & \\
a = 1089,\ b = 22 & & & \\
\Rightarrow & 1089 \div 22 & = & 49\ R\ 11 \\
\text{SWITCH: } a = b,\ b = R & & & \\
a = 22,\ b = 11 & & & \\
\Rightarrow & 22 \div 11 & = & 2\ R\ 0
\end{array}
$$

1.5.B Are numbers in A relative prime? Justify your answer.

No, they are not because 11 is their greatest common divisor.

$$
\begin{aligned}
85327 \div 11 &= 7757 \\
59840 \div 11 &= 5440
\end{aligned}
$$

1.5.C Using Fermat's theorem find 4^{225} *mod* 13

We know from FERMAT'S LITTLE THEOREM that :

$$4^{12} \equiv 1\ (mod\ 13)$$

Furthermore from the rules of modulo-arithmetic, we know:

$$
\begin{array}{lc}
if & a \equiv b\ (mod\ n)\ and\ c \equiv d\ (mod\ n) \\
then & ac \equiv bd\ (mod\ n)
\end{array}
$$

Therefore we know that:

$$4^{216} \equiv 1 \; (mod \; 13)$$

Because:

$$4^9 = 262.144 \equiv 12 \; (mod \; 13)$$

Our result would be:

$$4^{225} \; mod \; 13 = 12$$

1.5.D Using the Miller-Rabin test, say whether n=104717 is probably prime.

Find k and q:

$$n - 1 = 104716 = 2^2 \times 26179 = 2^k \times q$$

RNG for a: $a = 10$

$$10^{26179} \; mod \; 104717 = 1$$
$$\Rightarrow \textit{Test returns "inconclusive"}$$

RNG for a: $a = 7312$

$$7312^{26179} \; mod \; 104717 = 104716$$
$$\Rightarrow \textit{Test returns "inconclusive"}$$

RNG for a: $a = 18988$

$$18988^{26179} \; mod \; 104717 = 1$$
$$\Rightarrow \textit{Test returns "inconclusive"}$$

RNG for a: $a = 23753$

$$23753^{26179} \; mod \; 104717 = 1618$$
$$(23753^{26179})^2 \; mod \; 104717 = 104716$$
$$\Rightarrow \textit{Test returns "inconclusive"}$$

Therefore 104717 is a prime with a chance of more than 99.6%!

1.5.E Compute the set of integers that solve the equation $3^k \equiv 12(\; \boldsymbol{mod} \; 23)$ for k.

We know from the rules of modulo-arithmetic:

$$\begin{array}{ll} \textit{if} & a \equiv b \; (mod \; n) \; \textit{and} \; c \equiv d \; (mod \; n) \\ \textit{then} & ac \equiv bd \; (mod \; n) \end{array}$$

Furthermore we know (because 23 is prime) that:

$$3^{22} \equiv 1 \; (mod \; 23)$$

Therefore we need to find j:

$$3^j \equiv 12 \; (mod \; 23) \qquad , 0 < j < 22$$

This is the case for $j = 4$ and $j = 15$. Hence, the set of integers, that solve this equation would be:

$$\mathcal{S} = \{k \mid k = a \times 22 + j, \; a \in \mathbb{N}, \; j \in \{4, 15\}\}$$