Solution of Homework 7: *Basic Number Theory*

Q1. Compute $615^{31} \bmod 713$.

Answer

$$
\begin{aligned}
31 &= 2^4 + 2^3 + 2^2 + 2^1 + 2^0 = 16 + 8 + 4 + 2 + 1 \\
615^{31} \bmod 713 &= (615^{16} \times 615^8 \times 615^4 \times 615^2 \times 615) \bmod 713 \\
&= \Big((615^{16} \bmod 713) \times (615^8 \bmod 713) \times (615^4 \bmod 713) \times \\
&\quad (615^2 \bmod 713) \times (615 \bmod 713)\Big) \bmod 713 \ldots\ldots (1) \\
615 \bmod 713 &= 615 \\
615^2 \bmod 713 &= 378225 \bmod 713 = 335 \\
615^4 \bmod 713 &= 335^2 \bmod 713 = 112225 \bmod 713 = 284 \\
615^8 \bmod 713 &= 284^2 \bmod 713 = 80656 \bmod 713 = 87 \\
615^{16} \bmod 713 &= 87^2 \bmod 713 = 7569 \bmod 713 = 439 \\
\text{Substituting in (1):} & \\
615^{31} \bmod 713 &= (615 \cdot 335 \cdot 284 \cdot 87 \cdot 439) \bmod 713 \\
&= 398
\end{aligned}
$$

Q2. Prove that 937 is the inverse of 13 modulo 2436.

Answer

Solution #1: Simply

$$13 \times 937 \bmod 2436 = 12181 \bmod 2436 = 1.$$

Solution #2: Use the Euclidean algorithm to get the inverse of 13 modulo 2435 as follows:

$$
\begin{aligned}
2436 &= 187 \cdot 13 + 5 \ldots\ldots (1) \\
13 &= 2 \cdot 5 + 3 \ldots\ldots (2) \\
5 &= 1 \cdot 3 + 2 \ldots\ldots (3) \\
3 &= 1 \cdot 2 + 1 \ldots\ldots (4)
\end{aligned}
$$

Note, the $gcd(2436, 13) = 1$. To calculate the inverse of 13 modulo 2436, we proceed backwards as follows:

$$\begin{aligned}
1 &= 3 - 2 \ldots\ldots \text{ from (4)} \\
&= 3 - (5 - 3) = 2 \times 3 - 5 \ldots\ldots \text{ from (3)} \\
&= 2 \cdot (13 - 2 \times 5) - 5 = 2 \times 13 - 5 \times 5 \ldots\ldots \text{ from (2)} \\
&= 2 \times 13 - 5 \cdot (2436 - 187 \times 13) = 937 \times 13 - 5 \times 2436 \ldots\ldots \text{ from (1)}
\end{aligned}$$

Therefore, the inverse of 13 modulo 2436 is **937**.

Q3. Solve $13x = 5 \bmod 2436$.

Answer

First, we calculate the inverse of 13 mod 2436 which is 937 (from the previous problem).

Second, in order to get rid of 13 from the L.H.S., we multiply both sides by its inverse modulo 2436 as follows:

$$\begin{aligned}
13x &= 5 \bmod 2436 \\
\Rightarrow 937 \times 4x &= 937 \times 5 \bmod 2436 \\
\Rightarrow x &= 4685 \bmod 2436 \\
\Rightarrow x &= 2249.
\end{aligned}$$

Q4. Encrypt the message CRYPTO using the RSA system with $n = 43 \cdot 59$ and $e = 13$, translating each letter into integers (where $A = 00$, $B = 01, \ldots Z = 25$) and grouping pairs of integers, as we did in class.

Answer

The letter translation will be as follows: $C \rightarrow 02$, $R \rightarrow 17$, $Y \rightarrow 24$, $P \rightarrow 15$, $T \rightarrow 19$, and $O \rightarrow 14$. Thus, the word CRYPTO will be translated to 0217 2415 1914.

Let M_i be the i^{th} message to be encrypted, and C_i be the result of encrypting M_i. That is, $C_i = M_i^e \pmod{n}$. Moreover, by grouping pairs of integers, we will have to encrypt the following messages: (calculations are done as in problem 1 of this homework)

$M_1 =$'CR' $\to$ 0217: $C_1 = 0217^{13} \pmod{43 \cdot 59} = 710$
$M_2 =$'YP' $\to$ 2415: $C_2 = 2415^{13} \pmod{43 \cdot 59} = 1512$
$M_3 =$'TO' $\to$ 1914: $C_3 = 1914^{13} \pmod{43 \cdot 59} = 2367$.

Thus, the new message is: 0710 1512 2367.