Solution of Homework 6: *Basic Number Theory*

Q1. Use the Euclidean algorithm to find

(a) $\gcd(1529, 14039)$,

(b) $\gcd(1111, 11111)$.

Answer

Note that in each iteration the larger value is replaced by the smaller value in the previous iteration and the smaller value is replaced by the remainder obtained in the previous iteration. This procedure is repeated until the remainder reaches 0 at which time we can conclude that the required *gcd* is the smaller value.

(a) $\gcd(1529, 14039)$:

a	b	$a \bmod b$
14039	1529	278
1529	278	139
278	139	0

Thus, $\gcd(1529, 14039) = \mathbf{139}$.

(b) $\gcd(1111, 11111)$:

a	b	$a \bmod b$
11111	1111	1
1111	1	0

Thus, $\gcd(1111, 11111) = \mathbf{1}$ (that is, 11111 and 1111 are relatively prime).

Q2. Compute $615^{31} \bmod 713$.

Answer

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

Q3. 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**.

Q4. Solve $4x = 5 \bmod 9$.

Answer

First, we calculate the inverse of $4 \bmod 9$ which is 7 (this is because $4 \times 7 = 28 \equiv 1 \bmod 9$ or you can use the Euclidean algorithm.) Second, in order to get rid of 4 from the L.H.S., we multiply both sides by its inverse mod 9 (7 in this case) as follows:

$$\begin{aligned} 4x &= 5 \bmod 9 \\ \Rightarrow 7 \times 4x &= 7 \times 5 \bmod 9 \\ \Rightarrow x &= 35 \bmod 9 \\ \Rightarrow x &= 8 \end{aligned}$$

Q5. Encrypt the message ATTACK 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: $A \longrightarrow 00$, $T \longrightarrow 19$, $C \longrightarrow 02$, and $K \longrightarrow 10$. Thus, the word ATTACK will be translated to 0019 1900 0210.

Let M_i be the i^{th} message to be encrypted, and C_i be the result of encrypting M_i. I.e., $C_i = M_i^e \pmod{n}$. Moreover, by grouping pairs of integers, we will have to encrypt the following messages: (calculations are done through the Windows built in calculator)
M_1 ='AT' $\longrightarrow$ 0019: $C_1 = 0019^{13} \pmod{43 \cdot 59} = 2299$
M_2 ='TA' $\longrightarrow$ 1900: $C_2 = 1900^{13} \pmod{43 \cdot 59} = 1317$
M_3 ='CK' $\longrightarrow$ 0210: $C_3 = 0210^{13} \pmod{43 \cdot 59} = 2117$.

Thus, the new message is: 2299 1317 2117.