CISS451/MATH451: Cryptography and Computer Security
Assignment 5

This is an assignment on the congruence notation.

Q1. Using the extended euclidean algorithm, compute the multiplicative inverse of 19 (mod 709). Show all your steps.

SOLUTION.

Step 1:

$$\begin{aligned}
c = 1, d = 0, c' = 0, d' = 1, r = 709, r' = 19 \\
c' = 0 \\
d' = 1 \\
c - \left\lfloor \frac{r}{r'} \right\rfloor \cdot c' = 1 - \left\lfloor \frac{709}{19} \right\rfloor \cdot 0 = 1 \\
d - \left\lfloor \frac{r}{r'} \right\rfloor \cdot d' = 0 - \left\lfloor \frac{709}{19} \right\rfloor \cdot 1 = 0 - 37 = -37 \\
r' = 19 r - \left\lfloor \frac{r}{r'} \right\rfloor \cdot r' = 709 - \left\lfloor \frac{709}{19} \right\rfloor \cdot 19 = 709 - 703 = 6
\end{aligned}$$

Step 2:

$$\begin{aligned}
c = 0, d = 1, c' = 1, d' = -37, r = 19, r' = 6 \\
c' = 1 \\
d' = -37 \\
c - \left\lfloor \frac{r}{r'} \right\rfloor \cdot c' = 0 - \left\lfloor \frac{19}{6} \right\rfloor \cdot 1 = -3 \\
d - \left\lfloor \frac{r}{r'} \right\rfloor \cdot d' = 1 - \left\lfloor \frac{19}{6} \right\rfloor \cdot -37 = 1 + 111 = 112 \\
r' = 6 r - \left\lfloor \frac{r}{r'} \right\rfloor \cdot r' = 19 - \left\lfloor \frac{19}{6} \right\rfloor \cdot 6 = 19 - 18 = 1
\end{aligned}$$

Step 3:

$$\begin{aligned}
c = 1, d = -37, c' = -3, d' = 112, r = 6, r' = 1 \\
c' = -3 \\
d' = 112 \\
c - \left\lfloor \frac{r}{r'} \right\rfloor \cdot c' = 1 - \left\lfloor \frac{6}{1} \right\rfloor \cdot -3 = 1 + 18 = 19 \\
d - \left\lfloor \frac{r}{r'} \right\rfloor \cdot d' = -37 - \left\lfloor \frac{6}{1} \right\rfloor \cdot 112 = -37 - 672 = -709 \\
r' = 1 r - \left\lfloor \frac{r}{r'} \right\rfloor \cdot r' = 6 - \left\lfloor \frac{6}{1} \right\rfloor \cdot 1 = 6 - 6 = 0
\end{aligned}$$

Step 4:

$$c = 3, d = 112, c' = 19, d' = -709, r = 1, r' = 0$$

Now the r' is 0 so we can stop! And the x is 112.

OR......

Let $a = 19$ and $n = 709$, then we need to find out if an inverse exist. If there is an inverse then $ax + by = gcd(a, n) = 1$ will be satisfied.

$$\therefore \quad 1 = ax + 0(modn)$$

$$1 = 19 \cdot 1 - 18 \cdot 1(mod709)$$

So we can find an inverse x such that:

$$1 = ax + 0(modn)$$

Now we need to write 18 in terms of two numbers one of which we nee to write in terms of 709 times a number plus 19 times a number, in other words find a,b,c,d integers such that $a \cdot b = 18$ and $a = 709 \cdot c + 19 \cdot d$ or $b = 709 \cdot c + 19 \cdot d$

Some ways to write 18 are:

$$18 = 1 \cdot 18$$
$$18 = 2 \cdot 9$$
$$18 = 3 \cdot 6$$

After some trial and error I find that 3 and 6 work:

$$1 = 19 \cdot 1 - 3 \cdot 6(mod709)$$
$$6 = 709 \cdot 1 - 19 \cdot 37(mod709)$$

Now substitute for the 6:

$$
\begin{aligned}
1 &= 19 \cdot 1 - 3(709 \cdot 1 - 19 \cdot 37)(mod 709) \\
1 &= 19 \cdot 1 - 3 \cdot 709 + (3 \cdot 19 \cdot 37)(mod 709) \\
1 &= 19 \cdot 1 - 3 \cdot 709 + (19 \cdot 111)(mod 709) \\
1 &= 19 \cdot 112 - 3 \cdot 709(mod 709) \\
\therefore \quad 1 &= 19 \cdot 112(mod 709)
\end{aligned}
$$

Therefore our inverse $x = 112$.

Q2. Define the function

$$E(x) = 19x + 5 \pmod{709}$$

Note that this is a function from $\mathbb{Z}/709$ to $\mathbb{Z}/709$. Find another function $D(x)$ also from $\mathbb{Z}/709$ to $\mathbb{Z}/709$ and also of the form

$$D(x) = ax + b \pmod{709}$$

such that

$$D(E(x)) = x \pmod{709}$$

Explain very carefully why your $D(x)$ works.

SOLUTION.

$$\begin{aligned} y &= ax + b \\ y - b &= ax \\ a^{-1}(y - b) &= a^{-1}(ax) \\ a^{-1}y - a^{-1}b &= x \\ \therefore \quad y &= a^{-1}x - a^{-1}b \end{aligned}$$

$$\begin{aligned} a^{-1} &= 112(mod 709) \\ y &\equiv 19x + 5(mod 709) \\ y - 5 &\equiv 19x(mod 709) \\ 112(y - 5) &\equiv 112(19x)(mod 709) \\ 112y - 112 \cdot 5 &\equiv x(mod 709) \\ \therefore \quad y &\equiv 112x - 112 \cdot 5(mod 709) \\ \therefore \quad y &\equiv 112x - 560(mod 709) \\ \therefore \quad y &\equiv 112x + 149(mod 709) \end{aligned}$$