Last week:

$3a \equiv 1 \mod 26$

means

$3^{-1} \equiv a \mod 26$

So $3^{-1} \equiv 9 \mod 26$

Today:
Give a method for calculating $n^{-1} \mod m$.

Motivating Example

You intercept the ciphertext

OH7F86BB46R3627026BB9

and you know:

1) A 37-letter alphabet was used

$\phi, 1, 2, \ldots, 9, A=10, B=11, \ldots, Z=35, \_=36$

2) Affine cryptosystem

$$x \longmapsto \alpha x + \beta$$

is used on single letter message units.

3) plaintext ends with $\phi\, 7$.

Decipher the message.

Solution

enciphering procedure

$\phi \longmapsto B$

$7 \longmapsto 9$

$11 = \alpha\phi + \beta$

$9 = \alpha 7 + \beta$

Thus

$\boxed{\beta = 11}$

$9 = 7\alpha + 11 \mod 37$

$-2 = 7\alpha \mod 37$

$35 = 7\alpha \mod 37$

So $\alpha = 5$

The enciphering function is

$$X \longmapsto 5X + 11 \mod 37$$

The deciphering function is

$$X \longmapsto 5^{-1}(X-11) \mod 37$$

To calculate $5^{-1} \mod 37$ let's first note that

$$\gcd(5, 37) = 1.$$

Let's use the Euclidean algorithm to compute $\gcd(5, 37)$.

$37 = 7.5 + 2$

$5 = 2.2 + 1$ ← gcd(5, 37)

$2 = 2.1 + 0$

We can re-use these calculations:

$1 = 5 - 2.2$

$= 5 - 2(37 - 7.5)$

$\equiv 5 + 14.5 \pmod{37}$

$\equiv 15.5 \pmod{37}$

So $5^{-1} \equiv 15 \pmod{37}$

So our deciphering function is

$X \longmapsto 5^{-1}(X - 11) \pmod{37}$

$x \mapsto 5^{-1}x - 5^{-1}.11 \mod 37$

$x \mapsto 15x - 15.11 \mod 37$

$x \mapsto 15x - 17 \mod 37$

$\boxed{x \mapsto 15x + 20 \mod 37}$

Example

Find $15^{-1} \mod 26$.

$26 = 1 \cdot 15 + 11$

$15 = 1 \cdot 11 + 4$

$11 = 2 \cdot 4 + 3$

$4 = 1 \cdot 3 + 1$ ← gcd(15, 26)

$3 = 3 \cdot 1 + 0$

Rewrite these calculations to get

$$
\begin{aligned}
1 &= 4 - 1 \cdot 3 \\
&= 4 - 1 \cdot (11 - 2 \cdot 4) \\
&= -11 + 3 \cdot 4 \\
&= -11 + 3(15 - 11) \\
&= -4 \cdot 11 + 3 \cdot 15 \\
&= -4(26 - 15) + 3 \cdot 15 \\
&= -4 \cdot 26 + 7 \cdot 15 \\
&\equiv 7 \cdot 15 \pmod{26}
\end{aligned}
$$

So $\boxed{15^{-1} \equiv 7 \pmod{26}}$