Oscar, Nathan, Braydon

Start: Solve

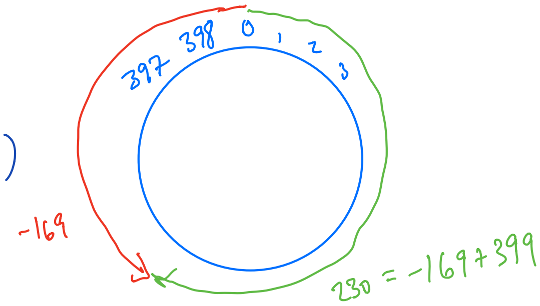
1. $314x \equiv 73 \pmod{399}$

Q: Does 314 have a mult. inv. in mod 399?
A: Yes, since $\gcd(314, 399) = 1$.
OK, so what is it? By EEA, write $1 = t \cdot 314 + s \cdot 399$

$t = -169 \equiv 230 \pmod{399}$

So 230 is mult. inv. of 314
Now take $314x \equiv 73 \pmod{399}$
and use inv.

$$(230)(314)x \equiv (230)(73) \pmod{399}$$
$$x \equiv 16790 \equiv 32 \pmod{399}$$



2. $9x \equiv 207 \pmod{399}$

Bad news here: $\gcd(9, 399) = 3$, not 1. So, 9 has no mult. inv.
Use the defn of congruence

$9x \equiv 207 \pmod{399} \longleftrightarrow 399 \mid 9x - 207$

or $\exists$ some $k \in \mathbb{Z}$ so that $399k = 9x - 207$.

Key: 3 divides all of 399, 9, and 207. Using this

$399k = 9x - 207$ becomes $133k = 3x - 69$.

or $3x \equiv 69 \pmod{133}$

Note that $\gcd(3, 133) = 1$. By the EEA, get
$-44 \equiv 89 \pmod{133}$ is mult. inv. of 3 (in mod 133).

Solve
$3x \equiv 69 \pmod{133}$ using mult. inv.
$(89)(3)x \equiv (89)(69) \pmod{133}$ or $x \equiv 6141 \equiv 23 \pmod{133}$

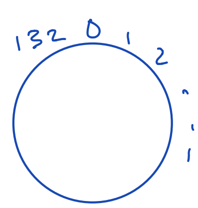
In mod 133

23, 156, 289, 422, 555, ...

are all the same. But in mod 399

$\underbrace{23, 156, 289}_{\text{all different.}}$, ~~422~~, ~~555~~

start repeating



Answers to orig. prob.
$x \equiv 23, 156, 289 \pmod{399}$.

This page added to give Extended Euclidean Algorithm details for Example 1 above:

<u>Euclidean Algorithm</u>

Set $r_0 = 399$, $r_1 = 314$

(1) $399 = 314 + 85$ $(r_2 = 85)$

(2) $314 = 85(3) + 59$ $(r_3 = 59)$

(3) $85 = 59 + 26$ $(r_4 = 26)$

(4) $59 = 26(2) + 7$ $(r_5 = 7)$

(5) $26 = 7(3) + 5$ $(r_6 = 5)$

(6) $7 = 5 + 2$ $(r_7 = 2)$

(7) $5 = 2(2) + 1$ $(r_8 = 1)$

$2 = 2(1) + 0$

last nonzero remainder: gcd = 1.

<u>Preparation for Extended Euclidean Algorithm</u>

Equations from the left column can be rearranged:

(7′) $r_8 = 5 - 2(2) = r_6 - 2r_7$

(6′) $r_7 = 7 - 5 = r_5 - r_6$

(5′) $r_6 = 26 - 7(3) = r_4 - 3r_5$

(4′) $r_5 = 59 - 26(2) = r_3 - 2r_4$

(3′) $r_4 = 85 - 59 = r_2 - r_3$

(2′) $r_3 = 314 - 85(3) = r_1 - 3r_2$

(1′) $r_2 = 399 - 314 = r_0 - r_1$

Starting with the modified (7′), the EEA just repeatedly substitutes until r_8 (the gcd) is written as $sr_0 + tr_1$:

$$
\begin{aligned}
r_8 &= r_6 - 2r_7 \\
&= r_6 - 2(r_5 - r_6) = 3r_6 - 2r_5 \\
&= 3(r_4 - 3r_5) - 2r_5 = 3r_4 - 11r_5 \\
&= 3r_4 - 11(r_3 - 2r_4) = 25r_4 - 11r_3 \\
&= 25(r_2 - r_3) - 11r_3 = 25r_2 - 36r_3 \\
&= 25r_2 - 36(r_1 - 3r_2) = 133r_2 - 36r_1 \\
&= 133(r_0 - r_1) - 36r_1 = 133r_0 - 169r_1 = 133r_0 + (-169)r_1
\end{aligned}
$$

So, we have written gcd(314, 399) as the weighted sum

$$1 = 133r_0 + (-169)r_1 = (133)(399) + (-169)(314)$$

and get that $-169 \equiv 230 \pmod{399}$ is the multiplicative inverse of 314 in $\mathbb{Z}_{399}$.

3. $9x \equiv 206 \pmod{399}$

Still have $\gcd(9, 399) = 3$, but now 206 isn't divisible by 3.

$\Rightarrow$ No solution. $x \in \mathbb{Z}$.

Affine ciphers: $f(x) = ax + b \pmod{26}$

$A \leftrightarrow 0$	$G \leftrightarrow 6$	$L \leftrightarrow 11$	$Q \leftrightarrow 16$	$V \leftrightarrow 21$
$B \leftrightarrow 1$	$H \leftrightarrow 7$	$M \leftrightarrow 12$	$R \leftrightarrow 17$	$W \leftrightarrow 22$
$C \leftrightarrow 2$	$I \leftrightarrow 8$	$N \leftrightarrow 13$	$S \leftrightarrow 18$	$X \leftrightarrow 23$
$D \leftrightarrow 3$	$J \leftrightarrow 9$	$O \leftrightarrow 14$	$T \leftrightarrow 19$	$Y \leftrightarrow 24$
$E \leftrightarrow 4$	$K \leftrightarrow 10$	$P \leftrightarrow 15$	$U \leftrightarrow 20$	$Z \leftrightarrow 25$
$F \leftrightarrow 5$				

Ex.) $a = 1$, $b = 3$

Orig. message: HELP

Encrypt

$H \to 7$ $\quad f(7) = (1)(7) + 3 \mod 26 = 10 \to K$

$E \to 4$ $\quad f(4) = (1)(4) + 3 \mod 26 = 7 \to H$

$L \to 11$ $\quad f(11) = (1)(11) + 3 \mod 26 = 14 \to O$

$P \to 15$ $\quad f(15) = (1)(15) + 3 \mod 26 = 18 \to S$

Ex.) $a = 5$, $b = 19$

$f(7) = (5)(7) + 19 \mod 26 = 2 \to C$

$f(4) = (5)(4) + 19 \mod 26 = 13 \to N$

and so on.

Q: How does the recipient decode an S ?

A: Must solve

$$ax + b \bmod 26 = 18$$

knowing $a = 5$, $b = 19$

Same as solving

$$5x + 19 \equiv 18 \pmod{26}$$

Doable because $\gcd(5, 26) = 1$.

Some really bad choices for a (lead to bad cipher systems)

$a = 2, 10, 13$ (all are not relatively prime w/ 26).