MATH 136—HOMEWORK 3

Ricardo J. Acuña

(862079740)

1 Solve: $\begin{cases} 3x \equiv 3 (\text{mod } 37) \\ 2x \equiv 15 (\text{mod } 53) \end{cases}$

Slu .:

$3 \equiv 3(\text{mod } 37)$ and $3 \cdot x \equiv 3 \cdot 1(\text{mod } 37) \implies x \equiv 1(\text{mod } 37)$

$2 \equiv 15 \equiv 53 + 15 \equiv 68 \equiv 2 \cdot 34(\text{mod}53) \implies 2 \cdot x \equiv 2 \cdot 34(\text{mod } 53)$

$2 \equiv 2(\text{mod } 53)$ and $2 \cdot x \equiv 2 \cdot 34(\text{mod } 53) \implies x \equiv 34(\text{mod } 53)$

So, $\begin{cases} 3x \equiv 3(\text{mod } 37) \\ 2x \equiv 15(\text{mod } 53) \end{cases} = \begin{cases} x \equiv 1(\text{mod } 37) \\ x \equiv 34(\text{mod } 53) \end{cases}$

By the Chinese Remainder Theorem

$x = 1 \cdot 53 \cdot y_1 + 34 \cdot 37 \cdot y_2$, where $y_1 = 53^{-1}(\text{mod } 37)$ and $y_2 = 37^{-1}(\text{mod } 53)$:
$\exists! x' : x \equiv x'(\text{mod } 34 \cdot 53)$ and $0 \leq x' < 34 \cdot 53$

$\iff \gcd(37, 53) = 1 \iff$ 37 and 53 are relatively prime

So, do the Euclidean Algorithm:

$53 = 1 \cdot 37 + 16$
$37 = 2 \cdot 16 + 5$
$16 = 3 \cdot 5 + 1$
$5 = 5 \cdot 1 + 0$

We conclude $\gcd(37, 53) = 1$.

Furthermore, one can now express 1 as a linear combination of 37 and 53 as such:

$16 = 3 \cdot 5 + 1 \implies 16 - 3 \cdot 5 = 1$
$37 = 2 \cdot 16 + 5 \implies 37 - 2 \cdot 16 = 5$
$53 = 1 \cdot 37 + 16 \implies 53 - 1 \cdot 37 = 16$
$\implies 1 = 53 - 1 \cdot 37 - 3 \cdot (37 - 2 \cdot (53 - 1 \cdot 37))$

By counting one can check that $1 = 7 \cdot 53 - 10 \cdot 37$

Immediately $1 \equiv -10 \cdot 37(\text{mod } 53)$ and $1 \equiv 7 \cdot 53(\text{mod } 37)$

so, $y_2 = -10$ and $y_1 = 7$, from the definition of y_1 and y_2

Therefore $x = 1 \cdot 53 \cdot 7 + 34 \cdot 37 \cdot -10 = -12209$

$7 \cdot 37 \cdot 53 - 12209 = 1518 \implies -12209 \equiv 1518(\text{mod } 37 \cdot 53)$
and $0 \leq 1518 < 37 \cdot 53 = 1961 \implies x' = 1518$

So, $\forall t \in \mathbb{Z} : x = t \cdot 1961 + 1518$ is a solution of $\begin{cases} 3x \equiv 3(\text{mod } 37) \\ 2x \equiv 15(\text{mod } 53) \end{cases}$

■

2 Solve: $345118 \cdot x + 6753y = 1$ » ∗ «

Slu .

Do the Euclidean Algorithm to find the initial value (x_0, y_0)

$345118 = 51 \cdot 6753 + 715$
$6753 = 9 \cdot 715 + 318$
$715 = 2 \cdot 318 + 79$
$318 = 4 \cdot 79 + 2$
$79 = 39 \cdot 2 + 1$
$2 = 2 \cdot 1 + 0$

One can conclude $\gcd(345118, 6753) = 1$, and one can say $1 = x \cdot 345118 + y \cdot 6753$ some integers x, y:

$345118 = 51 \cdot 6753 + 715 \implies 345118 - 51 \cdot 6753 = 715$
$6753 = 9 \cdot 715 + 318 \implies 6753 - 9 \cdot 715 = 318$
$715 = 2 \cdot 318 + 79 \implies 715 - 2 \cdot 318 = 79$
$318 = 4 \cdot 79 + 2 \implies 318 - 4 \cdot 79 = 2$
$79 = 39 \cdot 2 + 1 \implies 79 - 39 \cdot 2 = 1$
$\implies 6753 - 9 \cdot (345118 - 51 \cdot 6753) = 318$
$\implies 345118 - 51 \cdot 6753 - 2 \cdot (6753 - 9 \cdot (345118 - 51 \cdot 6753)) = 79$
$\implies 6753 - 9 \cdot (345118 - 51 \cdot 6753) - 4 \cdot (345118 - 51 \cdot 6753 - 2 \cdot (6753 - 9 \cdot (345118 - 51 \cdot 6753))) = 2$
$\implies$
$345118 - 51 \cdot 6753 - 2 \cdot (6753 - 9 \cdot (345118 - 51 \cdot 6753))$
$- 39 \cdot (6753 - 9 \cdot (345118 - 51 \cdot 6753) - 4 \cdot (345118 - 51 \cdot 6753 - 2 \cdot (6753 - 9 \cdot (345118 - 51 \cdot 6753))))$
$= 1$
$\implies$
$345118 - 51 \cdot 6753 - 2 \cdot 6753 + 18 \cdot (345118 - 51 \cdot 6753)$
$- 39 \cdot 6753 + 351 \cdot (345118 - 51 \cdot 6753) + 156 \cdot (345118 - 51 \cdot 6753 - 2 \cdot (6753 - 9 \cdot (345118 - 51 \cdot 6753)))$
$=$
$345118 - 51 \cdot 6753 - 2 \cdot 6753 + 18 \cdot 345118 - 918 \cdot 6753$
$- 39 \cdot 6753 + 351 \cdot 345118 - 17901 \cdot 6753 + 156 \cdot 345118 - 7956 \cdot 6753 - 312 \cdot (6753 - 9 \cdot (345118 - 51 \cdot 6753))$
$=$
$345118 - 51 \cdot 6753 - 2 \cdot 6753 + 18 \cdot 345118 - 918 \cdot 6753$
$- 39 \cdot 6753 + 351 \cdot 345118 - 17901 \cdot 6753 + 156 \cdot 345118 - 7956 \cdot 6753 - 312 \cdot 6753 + 2808 \cdot (345118 - 51 \cdot 6753)$
$=$
$345118 - 51 \cdot 6753 - 2 \cdot 6753 + 18 \cdot 345118 - 918 \cdot 6753$
$- 39 \cdot 6753 + 351 \cdot 345118 - 17901 \cdot 6753 + 156 \cdot 345118 - 7956 \cdot 6753 - 312 \cdot 6753 + 2808 \cdot 345118 - 143208 \cdot 6753$
$=$
$345118 + 18 \cdot 345118 + 351 \cdot 345118 + 156 \cdot 345118 + 2808 \cdot 345118$
$- 51 \cdot 6753 - 2 \cdot 6753 - 918 \cdot 6753 - 39 \cdot 6753 - 17901 \cdot 6753 - 7956 \cdot 6753 - 312 \cdot 6753 - 143208 \cdot 6753$
$=$
$(1 + 18 + 351 + 156 + 2808) \cdot 345118 + (-51 - 2 - 918 - 39 - 17901 - 7956 - 312 - 143208) \cdot 6753$
$= 3334 \cdot 345118 - 170387 \cdot 6753 = 1$

So, a particular solution$(x_0, y_0) = (3334, -170387)$

And by Theorem 9 in the lecture notes:

$\{(x, y) : x = 3334 - 6753 \cdot t, y = -170387 + 345118 \cdot t, t \in \mathbb{Z}\}$ is the set of all solutions to » ∗ «

■

3 Prove that if c admits an inverse modulo m, then c and m are relatively prime.

Pf .

Assume $\exists c^{-1} \in \mathbb{Z} : c^{-1}c \equiv 1(\text{mod } m)$
$\implies \exists t \in \mathbb{Z} : c^{-1}c = mt + 1$ (by Theorem 3 (iv) in the lecture notes)
$\implies 1 = c^{-1}c - tm$
$\implies c$ and m are relatively prime (by Corollary 1 in the lecture notes)

■

4 In a certain city, mayoral elections occur every 5 years and last occurred 2 years ago. Dog-catcher elections, on the other hand, occur every 7 and occurred last year. If it is 2019, find the next year that will feature both mayoral and dog-catcher elections.

Slu .

Model the problem as a system of congruences

$$\begin{cases} x \equiv 2019 - 2 \pmod 5 \\ x \equiv 2019 - 1 \pmod 7 \end{cases} \implies \begin{cases} x \equiv 2017 \equiv 403 \cdot 5 + 2 \pmod 5 \\ x \equiv 2018 \equiv 288 \cdot 7 + 2 \pmod 7 \end{cases} \implies \begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

By Chinese Remainder Theorem

$x = 2 \cdot 5 \cdot y_1 + 2 \cdot 7 \cdot y_2$, where $y_1 = 5^{-1}(\text{mod } 7)$, and $y_2 = 7^{-1}(\text{mod } 5)$

Do the Euclidean Algorithm to find y_1 and y_2

$7 = 1 \cdot 5 + 2$
$5 = 2 \cdot 2 + 1$
$2 = 2 \cdot 1 + 0$

$7 = 1 \cdot 5 + 2 \implies 7 - 1 \cdot 5 = 2$
$5 = 2 \cdot 2 + 1 \implies 5 - 2 \cdot 2 = 1$
$\implies 1 = 5 - 2 \cdot (7 - 1 \cdot 5) = 3 \cdot 5 - 2 \cdot 7$

So, $y_1 = 3$ and $y_2 = -2$

Therefore, $x = 2 \cdot 5 \cdot 3 + 2 \cdot 7 \cdot -2 = 2$

Therefore, $x = t \cdot 5 \cdot 7 + 2$ some $t \in \mathbb{Z}$ is a general solution to the system

Since $2019 = 57 \cdot 5 \cdot 7 + 24$, and 35 doesn't divide 24.

Choosing $t = 57 + 1$ will give us the answer.

So, $x = 58 \cdot 5 \cdot 7 + 2 = 2032$ works.

Because, $2032 = 2017 + 3 \cdot 5 = 2018 + 2 \cdot 7$

■