Tarea 2.2 Miguel Angel Soto Hernández

- compute $\lambda, \mu \in \mathbb{Z}$ such that $89\lambda + 55\mu = 1$ and find all solutions $x \in \mathbb{Z}$ to $89x \equiv 7 \pmod{55}$

Realizamos el algoritmo Euclidiano a 89 y 55:

$89 = 55 + 34,$
$55 = 34 + 21,$
$34 = 21 + 13,$
$21 = 13 + 8$
$13 = 8 + 5$
$8 = 5 + 3$
$5 = 3 + 2$
$3 = 2 + 1$
$2 = 2 \cdot 1 + 0$

Por lo tanto:

$1 = 3 - 2 = 3 - (5-3) = 2 \cdot 3 - 5 = 2(8-5) - 5 = 2 \cdot 8 - 3 \cdot 5 =$
$= 2 \cdot 8 - 3(13-8) = 5 \cdot 8 - 3 \cdot 13 = 5(21-13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13$
$= 5 \cdot 21 - 8(34-21) = 13 \cdot 21 - 8 \cdot 34 = 13(55-34) - 8 \cdot 34 =$
$= 13 \cdot 55 - 21 \cdot 34 = 13 \cdot 55 - 21(89-55) = 34 \cdot 55 - 21 \cdot 89$

Por lo tanto

$\lambda = -21, \mu = 34.$

De $1 = 34 \cdot 55 - 21 \cdot 89$ podemos decir que

$$89(-21) \equiv 1 \pmod{55}$$

Multiplicando esta congruencia por 7 tenemos que

$$89(-21)(7) \equiv 7 \pmod{55}$$

Para simplificar, notemos que $(-21)(7) = -147 \equiv 18 \pmod{55}$

entonces $89 \cdot 18 \equiv 7 \pmod{55}$

Desde $(89, 55) = 1$, todas las soluciones son dadas por

$$x = 18 + k \cdot 55, \ k \in \mathbb{Z}$$

- Prove that $3 \mid 4^n - 1$, where $n \in \mathbb{N}$

Caso base $n=1$

$$4^1 - 1 = 4 - 1 = 3 \quad \therefore \text{ Verdadero para } n=1$$

Asumiendo $4^k - 1 = 3P$ donde $k, P \in \mathbb{Z}^+$

$\underline{4^{k+1} - 1 = 3Q}$, donde $Q \in \mathbb{Z}^+$

$$\begin{aligned}
LHS &= 4^{k+1} - 1 \\
&= 4 \cdot 4^k - 1 \\
&= 4^k - 1 + 3 \cdot 4^k \\
&= 3P + 3 \cdot 4^k \quad \text{asumiendo} \\
&= 3P\,(P + 4^k) \quad P \in \mathbb{Z}^+,\ 4^k \in \mathbb{Z}^+ \text{ as } k \in \mathbb{Z}^+ \\
&= 3Q \quad \text{donde } Q = P + 4^k
\end{aligned}$$

Verdadero para $n = k+1$

– Solve the system ([11][18]) $x \equiv 17 \pmod{504}$, $x \equiv -4 \pmod{35}$, $x \equiv 33 \pmod{16}$ of congruences in x

$x \equiv 17 \mod 504$
$x \equiv -4 \mod 35$
$x \equiv 33 \mod 16$

$504 = 8 \cdot 9 \cdot 7$

$35 = 5 \cdot 7$

$x \cdot 2$ $x = -1$ $x \cdot 2$

$x \equiv 17 \equiv 1 \mod 8$ $x \equiv -4 \equiv 1 \mod 5$
$x \equiv 17 \equiv -1 \mod 9$ $x \equiv -4 \equiv 3 \mod 7$ $x \equiv 1 \mod 16$
$x \equiv 17 \equiv 3 \mod 7$

El sistema original es congruente con el sistema

$x \equiv 1 \mod 16$ $x \equiv 3 \mod 7$
$x \equiv 1 \mod 9$ $x \equiv 1 \mod 5$

Ahora podemos aplicar el teorema Chino.

$(-59) \cdot 16 + 3 \cdot (9 \cdot 7 \cdot 5) = 1,$
$249 \cdot 9 + (-4) \cdot 16 \cdot 7 \cdot 5 = 1,$
$103 \cdot 7 + (-1) \cdot 16 \cdot 9 \cdot 5 = 1,$
$(-403) \cdot 5 + 2(16 \cdot 9 \cdot 7) = 1,$

Entonces la solución de nuestro sistema esta dada por:

$$x = 3 \cdot (9 \cdot 7 \cdot 5) + (-1) \cdot (-4) \cdot 16 \cdot 7 \cdot 5 + 3 \cdot (-1) \cdot 16 \cdot 9 \cdot 5 + 2 \cdot (16 \cdot 9 \cdot 7) = \underline{3041}$$

- Verify that the reminder of 2^{340} after division by 341 is 1, using the repeating squaring algorith.

$$[2^{340}]_{341} = [2^{2^8} + 2^{2^6} + 2^{2^4} + 2^{2^2}]$$

$$[2^{2^2}] = [(2^2)^2] = [[2^2][2^2]] = 16$$

$$[2^{2^4}] = [(2^{2^2})^2] = [(2^{2^2})(2^{2^2})] = [16 \cdot 16] = 256$$

$$[2^{2^6}] = [(2^{2^4})^2] = [(2^{2^4})(2^{2^4})] = [256 \cdot 256] = [65536] = 64$$

$$[2^{2^8}] = [(2^{2^6})(2^{2^6})] = [64 \cdot 64] = [4090] = 4$$

$$[16 \cdot 256 \cdot 64 \cdot 4]_{341} = [1048576]_{341} = \boxed{1}$$

- An old women goes to market and a horse steps on her basket and crushes her eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left at the end. The same thing happened when she picked them out three, four, five, and six at a time, but when she took them out seven at time, no egg left at the end. What is the smallest number of eggs she could have had?

$$x \equiv 1 \pmod 2, \quad x \equiv 1 \pmod 3, \quad x \equiv 1 \pmod 4$$
$$x \equiv 1 \pmod 5, \quad x \equiv 1 \pmod 6, \quad x \equiv 0 \pmod 7.$$

los módulos no son primos relativos, sin embargo, hay que tener en cuenta las siguientes congruencias

$$x \equiv 1 \pmod 3, \quad x \equiv 1 \pmod 4, \quad x \equiv 1 \pmod 5, \quad x \equiv 0 \pmod 7$$

implican las dos congruencias restantes. Por lo tanto, este último sistema es congruente con el primero, y ahora los modulos son pares relativamente primos

Aplicando el teorema Chino

$$47 \cdot 3 + (-1) \cdot 4 \cdot 5 \cdot 7 = 1,$$

$$(-26) \cdot 4 + 1 \cdot 3 \cdot 5 \cdot 7 = 1,$$

$$17 \cdot 5 + (-1) \cdot 3 \cdot 4 \cdot 7 = 1,$$

$$(-17) \cdot 7 + 2 \cdot 3 \cdot 4 \cdot 5 = 1$$

La solución del sistema esta dada por:

$$x = (-1) \cdot 4 \cdot 5 \cdot 7 + 3 \cdot 5 \cdot 7 + (-1) \cdot 3 \cdot 4 \cdot 7 + 0 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = -119$$

La solución positiva más pequeña es: $-119 + 3 \cdot 4 \cdot 5 \cdot 7 = 301$

-Suppose that someone tricks you into believing that $233 \cdot 577 = 135441$. Use congruences to prove in a flash that this is wrong. Is there a smart way of using congruences to double-chec computations such as $a+b$ and ab for integers a an b? Give a few examples.

$$\underset{a}{233} \cdot \underset{b}{577} = \underset{ab}{135441}$$

$a \equiv b \mod c$ si $(b-a)/c$

$577 - 233 = 344$

$c = 344$

$[344]_{344} = 0$

$[233]_{344} = 233$

$[577]_{344} = 233$

$$\begin{array}{r} 393 \\ 344 \overline{)135441} \\ \underline{1032} \\ 3224 \\ \underline{3096} \\ 1281 \\ \underline{1032} \\ 248 \end{array}$$

$[ab]_{344} = [[a][b]]_{344}$

$[135441]_{344} = [[233][577]]_{344}$

$[135441]_{344} = 248$

$[233 \cdot 233]_{344} = [54289]_{344} = 281$

$\boxed{\text{como } 248 \neq 281 \text{ entonces es incorrecto}}$

- Let a be a number written (in base 10) as

$$a = a_0 + a_1 \cdot 10 + a_2 + 10^2 + \dots + a_n \cdot 10^n$$
donde $0 \leq a_i < 10$

~~a)~~ Prove that $a \equiv a_0 \pmod 2$. In particular, $2 | a$ if $2 | a_0$

~~b)~~ Prove that $a \equiv a_0 + 2a_1 \pmod 4$. In particular, $4 | a$ if $4 | a_0 + 2a_1$

~~c)~~ Prove that $a \equiv a_0 + 2a_1 + 4a_2 \pmod 8$. In particular, $8 | a$ if $8 | a_0 + 2a_1 + 4a_2$

~~d)~~ Prove that $a \equiv a_0 \pmod 5$. In particular, $5 | a$ if $5 | a_0$

e) Prove that $a \equiv a_0 + a_1 + \dots + a_n \pmod 9$. In particular $9 | a$ if $9 | a_0 + a_1 + \dots + a_n$

f) Prove that $a \equiv a_0 + a_1 + \dots + a_n \pmod 3$. In particular, $3 | a$ if $3 | a_0 + a_1 + \dots + a_n$

g) Prove that $a \equiv a_0 - a_1 + a_2 - \dots \pmod{11}$. In particular, $11 | a$ if $11 | a_0 - a_1 + a_2 - \dots$

Soluciones:

a) $a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_n \cdot 10^n$

Como $10^k \equiv 0 \pmod 2$ para $k > 0$, decimos que:

$$a \equiv a_0 \pmod 2$$

Por lo tanto, $2 | a$ si $2 | a_0$

d) De manera similar, $10^k \equiv 0 \pmod 5$ para $k > 0$:

$$a \equiv a_0 \pmod 5$$

Por lo tanto, $5 | a$ si $a_0 = 0$ o $a_0 = 5$

b) Ahora, $10 \equiv 2 \pmod 4$ y $10^k \equiv 0 \pmod 4$ para $k \geq 2$:

$$a \equiv a_0 + a_1 \cdot 10 \equiv a_0 + 2a_1 \pmod 4$$

resulta que $4 | a$ if $4 | a_0 + 2a_1$

c) De manera similar, tenemos que $10 \equiv 2 \pmod 8$, $10^2 \equiv 4 \pmod 8$ y $10^k \equiv 0 \pmod 8$ para $k \geq 3$

Por lo tanto, $a \equiv a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 \equiv a_0 + 2a_1 + 4a_2 \pmod 8$

- Prove that 15 is not strong pseudoprime relative to 11

Podemos notar que $15-1=2\cdot 7$

Entonces 15 es un fuerte pseudoprimo relativo a 11 si y solo si

$11^7 \equiv 1 \pmod{15}$ o $11^7 \equiv -1 \pmod{15}$

Pero $11^7 \equiv (-4)^7 = 16^3(-4) \equiv -4 \pmod{15}$

Por lo tanto 15 no es un fuerte pseudoprimo relativo a 11

- Prove that $a^{N-1} \not\equiv 1 \pmod{N}$ if $\gcd(a, N) > 1$, where $a, N \in \mathbb{Z}$ and $N \geq 1$

Sea $d = \gcd(a, N) > 1$

Entonces $a \equiv 0 \pmod{d}$ y por lo tanto $a^{N-1} \equiv 0 \not\equiv 1 \pmod{d}$.

Como d es el divisor de N, tenemos $a^{N-1} \not\equiv 1 \pmod{d}$

En particular, $8|a$ if $8|a_0+2a_1+4a_2$

Notemos que $10\equiv 1 \pmod 3$ y $10 \equiv 1 \pmod 9$. Por lo tanto $10^k \equiv 1 \pmod 3$ y $10^k \equiv 1 \pmod 9$ para cada $k \geq 0$. Resulta que:

$$a \equiv a_1 + a_1 + \dots + a_n \pmod 3 \quad y$$

$$a \equiv a_1 + a_1 + \dots + a_n \pmod 9$$

En particular $3|a$ si $3|a_1+a_1+\dots+a_n$. y $9|a$ si $9|a_1+a_1+\dots+a_n$

$10 \equiv -1 \pmod{11}$, tenemos que $10^k \equiv 1 \pmod{11}$ para k par y $10^k \equiv -1 \pmod{11}$ para k impar.

$$a \equiv a_0 - a_1 + a_2 - a_3 + \dots \pmod{11}$$

Por lo tanto $11|a$ si $11|a_0-a_1+a_2-a_3+\dots$