Ciencia de la computación

Laboratorio 05

Álgebra Abstracta

Juan Pablo Galindo Coronel

Tercer semestre

2021

"El alumno declara haber realizado el presente trabajo de acuerdo a las normas de la Universidad Católica San Pablo"

FIRMA

1. (6 points) Sea a x ≡ 1 (mod n), implementar un algoritmo para calcular x (el inverso multiplicativo de a, módulo n). El programa debe permitir ingresar el número a y n, luego debe retorna el valor de x (si es que existe). Crear un repositorio en GitHub (con README).

https://github.com/juanpa022/Laboratorio_05-

2. (6 points) Resolver utilizando el Pequeño Teorema de Fermat.

(a) (1 point) 3^{181} mod 7.

TEOREMA:

Según el pequeño teorema de Fermat

$(3^{180}.3^{1})$ mod 7

330*6.3 mod 7

Por lo tanto:

$\boxed{3^{3} \equiv 3 \text{ mod } 7}$

(b) (1 point) 2^{245} mod 7.

TEOREMA:

Según el pequeño teorema de Fermat

$2^{40}.2^{5}$ mod 7

240*6.25 mod 7

Por lo tanto:

$\boxed{2^{32} \equiv 4 \text{ mod } 7}$

(c) (1 point) 128^{129} mod 17.

TEOREMA:

Según el pequeño teorema de Fermat

$128^{16} \equiv 9^{16} \equiv 1$ mod 17.

Por lo tanto:

$128^{129} \equiv 9^{1} \equiv 9$ mod 17.

$\boxed{\text{RPTA : } 128^{129} \equiv 9 \text{ mod } 17}$

(d) (1 point) ¿Cual es el residuo de dividir 2^{1000} entre 13?

TEOREMA:

Según el pequeño teorema de Fermat

$2^{12} \equiv 1$ mod 13.

Por lo tanto:

$2^{1000} \equiv 2^{400} \equiv 2^{40} \equiv 2^{4} \equiv 16 \equiv 3$ mod 13.

$\boxed{\text{RPTA: } 2^{1000} \equiv 3 \text{ mod } 13}$

(e) (2 points) $(2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60})$ mod 7.

TEOREMA:

Según el pequeño teorema de Fermat:

$2^6 \equiv 3^6 \equiv 4^6 \equiv 5^6 \equiv 6^6 \equiv 1$ mod 7.

Por lo tanto:

$$2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60}$$
$$\equiv$$
$$2^2 + 3^0 + 4^4 + 5^2 + 6^0 \equiv 4 + 1 + 28 + 25 + 1$$
$$\equiv$$
$$4 + 1 + 4 + 4 + 1 \equiv 14 \equiv 0 \text{ mod } 7.$$

RPTA: $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \equiv 0$ mod 7

3. (3 points) Resolver $x^{103} \equiv 4$ (mod 11), para $0 \leq x < 11$.

   TEOREMA:

   Según el pequeño teorema de Fermat:
   $x^{10} \equiv 1$ mod 11. Por lo tanto, $x^{103} \equiv x^3$ mod 11.
   Entonces, solo necesitamos
   Resolver:
   $x^3 \equiv 4$ mod 11.
   Si probamos todos los valores desde
   $x = 1$ hasta $x = 10$
   encontramos que :
   $5^3 \equiv 4$ mod 11.

   Por lo tanto, $x \equiv 5$ mod 11.

4. (5 points) Un googol es igual a 10100, un número tan grande que supera el cantidad de ´átomos en el universo (≈ 1080). Ahora, un googolplex es igual a 10googol. ¿Que día de la semana sería un googolplex de días a partir de ahora? (Hoy es Viernes)

   TEOREMA:

   Según el pequeño teorema de Fermat

   $10^6 \equiv 1$ mod 7 → 10^{100} es mod 6
   $10^2 = 100 \equiv 4 \equiv 10$ mod 6

   Inducción

   $10^k \equiv 10 \equiv 4$ mod 6 → $10^{100} \equiv 4$mod 6
   Entonces:
   $10^{100} = 6c + 4$ para © positivo

   Remplazamos:

   $$10^{10^{100}} = 10^{6c+4} = (10^c)^6 . 10^4 => 10^{10^{100}} \equiv 1^c . 100^2 \equiv 100^2 \equiv 2^2 \equiv 4\text{mod } 7$$

   Conclusión:
   Tenemos que googolplex es 4 veces mas el múltiplo de 7→en el dia de la semana aumenta en 4.

   RPTA:Viernes +4=Martes.