Universidad de la República - Facultad de Ingeniería - IMERL: Matemática Discreta 2

Primer parcial - 5 de mayo de 2016. Duración: 3 horas

Ejercicio 1.

a. Calcular el inverso de 5 módulo 121.

Solución: Es fácil ver que $121 - 5 \cdot 24 = 1$ (si no me doy cuenta, uso el Algoritmo de Euclides Extendido). Entonces el inverso de 5 módulo 121 es $-24 \equiv 97 \pmod{121}$.

b. Calcular el inverso de 5^4 módulo 121.

Solución: Usando la parte anterior, el inverso de 5^4 es 97^4 módulo 121. Calculamos $97^2 \equiv 92 \pmod{121}$ y $92^2 \equiv 115 \pmod{121}$. Entonces el inverso de 5^4 módulo 121 es 115.

Verificación: $5^4 \equiv 125 \cdot 5 \equiv 4 \cdot 5 \equiv 20 \pmod{121}$ y $20 \cdot 115 = 2300 = 19 \cdot 121 + 1$.

c. Calcular $15^{773} \pmod{121}$.

Solución: Como $121 = 11^2$, tenemos $\varphi(121) = 11 \cdot 10 = 110$. Como 15 es coprimo con 121, podemos usar el Teorema de Euler, obteniendo $15^{773} \equiv 15^3 \pmod{121}$. Ahora calculamos $15^2 \equiv 104 \pmod{121}$ y $104 \cdot 15 \equiv 108 \pmod{121}$. Concluimos que $15^{773} \equiv 108 \pmod{121}$.

d. Calcular $15^{773} \pmod{5^4 \cdot 121}$

Solución: Usando el Teorema Chino, tenemos:

$$x \equiv 15^{773} \pmod{5^4 \cdot 121} \iff \begin{cases} x \equiv 15^{773} \pmod{5^4} \\ x \equiv 15^{773} \pmod{121} \end{cases}$$

Para resolver la primera congruencia, observamos que 15^{773} es divisible por 5^4, entonces $x \equiv 0 \pmod{5^4}$. La segunda congruencia, por la parte (c), es $x \equiv 108 \pmod{121}$. Ahora volvemos a usar el Teorema Chino. Queremos un entero x de la forma $5^4 k$ que además sea congruente con 108 módulo 121. Planteamos $5^4 k \equiv 108 \pmod{121}$, y encontramos k usando el inverso calculado en (b): $k \equiv 115 \cdot 108 \equiv 78 \pmod{121}$. Concluimos que

$$\left.\begin{cases} x \equiv 0 \pmod{5^4} \\ x \equiv 108 \pmod{121} \end{cases}\right\} \iff x \equiv 5^4 \cdot 78 \pmod{5^4 \cdot 121}$$

Entonces la solución es $x \equiv 5^4 \cdot 78 \pmod{5^4 \cdot 121}$.

Ejercicio 2. Dado el sistema

$$\begin{cases} x & \equiv & 31 & (\text{mód } 56) \\ x & \equiv & 53 & (\text{mód } 105) \end{cases},$$

investigar si tiene solución, y en caso de que tenga encontrar todas sus soluciones.

Solución: Observemos que 56 y 105 no son coprimos. En efecto, como ambos son divisibles entre 7, podemos mirar las dos congruencias módulo 7. La primera congruencia implica que $x \equiv 31 \equiv 3 \pmod 7$ y la segunda implica que $x \equiv 53 \equiv 4 \pmod 7$. Como estas dos afirmaciones son contradictorias, concluimos que el sistema en cuestión no tiene ninguna solución.

Ejercicio 3.

a. Probar que todo entero $n > 1$ es producto de primos, sin utilizar el Teorema Fundamental de la Aritmética.

Solución: Por inducción completa (fuerte), podemos suponer que todo entero m con $1 < m < n$ es producto de primos. Ahora consideramos dos casos:

- Si n es primo, entonces n es producto de un primo (él mismo).
- Si n no es primo, entonces $n = ab$ con $1 < a < n$ y $1 < b < n$. Por la hipótesis inductiva, a es producto de primos y b también. Pero entonces ab es producto de primos.

b. Probar que si $p > 2$ primo entonces es de la forma $4k + 1$ o $4k - 1$ con k entero.

Solución: Por el Teorema de División Entera, sabemos que $p = 4q + r$ con q entero y $r \in \{0, 1, 2, 3\}$. Como p es impar, no puede ser $r = 0$ o $r = 2$. En el caso en que $r = 1$, tenemos $p = 4k + 1$ (donde $k = q$). En el caso en que $r = 3$, tenemos $p = 4k - 1$ (donde $k = q + 1$).

c. Probar que si un entero $n > 1$ es de la forma $4k-1$, entonces hay algún primo de la forma $4k - 1$ que lo divide.

Solución: Por la parte (a) n es un producto de primos. Si 2 aparece en el producto, n sería par, contradicción. Si todos los primos que aparecen en el producto fueran de la forma $4k + 1$, entonces n sería también de la forma $4k + 1$, contradicción. Entonces en la factorización de n debe aparecer al menos un primo de la forma $4k - 1$.

d. Probar que existen infinitos primos de la forma $4k - 1$.

Solución: Supongamos que los primos de la forma $4k-1$ son una cantidad finita, digamos que son $p_1, p_2, \ldots, p_t$. Consideramos

$$n = 4 \cdot p_1 \cdot p_2 \cdot \cdots \cdot p_t - 1,$$

que es de la forma $4k-1$. Por la parte (c) hay algún primo q de la forma $4k-1$ que divide a n. Entonces debería ser $q = p_i$ para algún i, luego $p_i \mid n$ y $p_i \mid 4p_1 \cdot p_2 \cdot \cdots \cdot p_t$, entonces $p_i \mid 1$, contradicción.

Ejercicio 4. Sean $a \in \mathbb{Z}$ y $n \in \mathbb{N}$ tales que $\mathrm{mcd}(a, n) = 1$. Definimos los conjuntos

$$A = \{0 \leq i < n\}\,,$$
$$B = \{0 \leq i < n \ : \ \mathrm{mcd}(i, n) = 1\}\,.$$

Definimos $f_a : A \to A$ de la siguiente manera

$$f_a(i) = a \cdot i \text{ mód } n\ ,$$

es decir $f_a(i)$ es el resto de la división entera de $a \cdot i$ entre n.

a. Probar que si $i \in B$ entonces $f_a(i) \in B$.

Solución: Por hipótesis a es invertible módulo n. Si $i \in B$ entonces i es invertible módulo n. Pero entonces $a \cdot i$ también es invertible (su inverso es el producto de los inversos de a y de i), es decir que $f_a(i) = a \cdot i \in B$.

b. Probar que f_a define una biyección de B con B.

Solución: Denotemos b al inverso de a módulo n. Entonces la función $f_b : B \to B$ es la inversa de f_a ya que $f_b(f_a(i)) = f_b(a \cdot i) = b \cdot a \cdot i \equiv i \pmod{n}$, y de la misma manera $f_a(f_b(i)) = f_a(b \cdot i) = a \cdot b \cdot i \equiv i \pmod{n}$. Entonces f_a es biyectiva.

c. Probar que $a^{\#B} \equiv 1 \pmod{n}$.

Solución: Consideramos $P \equiv \prod_{i \in B} i \pmod{n}$. Como f_a es una biyección, entonces también $P \equiv \prod_{i \in B} f_a(i) \pmod{n}$, ya que la función f_a solamente cambia el orden de los factores. Entonces:

$$P \equiv \prod_{i \in B} f_a(i) \equiv \prod_{i \in B} a \cdot i \equiv a^{\#B} \prod_{i \in B} i \equiv a^{\#B}\, P \pmod{n}\ .$$

Como P es producto de invertibles, debe ser invertible y entonces podemos cancelarlo en la congruencia anterior, obteniendo así $1 \equiv a^{\#B} \pmod{n}$.