Pontificia Universidad Católica de Chile
Facultad de Matemáticas
Departamento de Matemática
Segundo Semestre de 2018

Tarea 4

Teoría de Números - MAT 2225

Fecha de Entrega: 2018/09/11

Integrantes del grupo:
Nicholas Mc-Donnell, Camilo Sánchez

Problema 1 (3 pts)**.** Encuentre todas las soluciones $x \in \mathbb{Z}$ para el siguiente sistema de congruencias:

$$\begin{cases} 5x \equiv 4 \mod 7 \\ 3x \equiv 2 \mod 8 \end{cases}$$

Solución problema 1: Desarrollando las expresiones de la siguiente forma

$$\begin{aligned} 5x \equiv 4 \mod 7 3x &\qquad \equiv 2 \mod 8 \\ x \equiv 5 \mod 7x &\qquad \equiv 6 \mod 8 \end{aligned}$$

Ahora se puede usar el teorema chino del resto y su inversa, con lo que tenemos

$$\psi : \mathbb{Z}_{56} \to \mathbb{Z}_7 \times \mathbb{Z}_8$$

Además $-1 \cdot 7 + 1 \cdot 8 = 1$, por lo que $\psi(-7) = (0, 1)$ y $\psi(8) = (1, 0)$. Vemos que encontrar x que cumple las ecuaciones es equivalente a encontrar $\psi(x) = (5, 6)$.

$$\begin{aligned} (5, 6) &= 5 \cdot (1, 0) + 6 \cdot (0, 1) \\ &= 5\psi(8) + 6\psi(-7) \\ &= \psi(5 \cdot 8 - 6 \cdot 7) \\ &= \psi(-2) \\ &= \psi(54) \end{aligned}$$

Por lo que $\forall k \in \mathbb{Z}, x = 54 + 56k$ es solución del sistema

■

Problema 2 (3 pts)**.** Sea $p > 2$ un primo. Demuestre que -1 es un cuadrado módulo p si y solo si $p \equiv 1 \mod 4$

Solución problema 2: Sea p primo distinto de 2, entonces $p \equiv 1 \mod 4$ o $p \equiv 3 \mod 4$, veamos lo elementos de $(\mathbb{Z}_p)^\times = \{, 1, 2, ..., p-1\}$, recordamos que es un cuerpo por lo que podemos particionarlo usando la siguiente clase de equivalencia

$$\{x, -x, x^{-1}, -x^{-1}\}$$

Esta clase de equivalencia es de a lo más 4 elementos, veamos los siguientes casos

- Si $x \equiv -x \mod p \implies 2x \equiv 0 \mod p \implies 2 \equiv 0 \mod p \vee x \equiv 0 \mod p$, pero $p \neq 2$, y $x \not\equiv 0 \mod p$, por lo que este caso no pasa.
- Si $x \equiv x^{-1} \mod p \implies x^2 \equiv 1 \mod p \implies (x-1)(x+1) \equiv 0 \mod p$, por lo que $x = 1$ o $x = p-1$, esta partición es $\{1, p-1\}$
- Si $x \equiv -x^{-1} \mod p \implies x^2 \equiv -1 \mod p$, dado esto, podemos tener cero o dos soluciones $(x, p-x)$. Asumamos que existe $x_0 \in \mathbb{Z}_p$ tal que $x_0^2 \equiv -1 \mod p$, y que además existe $y_0 \in \mathbb{Z}_p$ tal que $y_0^2 \equiv -1 \mod p$. Luego $x_0^2 - y_0^2 \equiv 0 \mod p \implies x_0 \equiv y_0 \mod p \vee x_0 \equiv -y_0 \mod p$, una impica que $x_0 = y_0$ y el otro implica que $y_0 = p - x_0$, ambas son contradicciones, por lo tanto solo hay dos soluciones de la equivalencia dado un p, por lo que solo hay una clase de equivalencia de la forma $\{x_0, p - x_0\}$

Fuera de estos todas las clases son de tamaño 4, si $p = 4k+1$, hay $4k$ elementos en $(\mathbb{Z}_p)^\times$, luego recordamos que esta $\{1, p-1\}$, por lo que nos quedan $4k-2$ elementos, como todas las clases de equivalencia son de tamaño 4 o son la única clase de la forma $\{x_0, p-x_0\}$, esta clase tiene que existir por conteo. Es decir $p \equiv 1 \mod 4 \implies \exists x_0 \in \mathbb{Z}_p : x_0^2 \equiv -1 \mod p$ Si $p = 4k+3$, $(\mathbb{Z}_p)^\times$ tiene $4k+2$ elementos, por lo que nos queda $\{1, p-1\}$ y las particiones de tamaño 4, por lo que $x^2 \equiv -1 \mod p$ no tiene soluciones Con esto se concluye que $\exists x_0 : x_0^2 \equiv -1 \mod p \implies p \equiv 1 \mod 4$

■

Problema 3 (3 pts c/u)**.** Dada una finita lista finita de primos distintos $p_1, ..., p_l$ uno puede escribir los enteros $4(p_1 \cdot ... \cdot p_l)^2 + 1$ y $4p_1 \cdot ... \cdot p_l - 1$. Usando esta idea y adaptando la demostración de Euclides, demuestre lo siguiente:

I) Existen infinitos primos $p \equiv 1 \mod 4$

II) Existen infinitos primos $p \equiv 3 \mod 4$

Solución problema 3:

I) Asumamos que existen finitos primos de la forma $p \equiv 1 \mod 4$, luego sea $n = 4\left(p_1 \cdot ... \cdot p_l\right)^2 + 1$, donde $p_j \equiv 1 \mod 4$.

$$\begin{aligned} n &\equiv 1 \mod 4 \\ \left(2p_1 \cdot ... \cdot p_l\right)^2 + 1 &\equiv 1 \mod 4 \end{aligned}$$

Si n es primo tenemos una contradicción inmediata, ya que $p_j \nmid n$. Ahora, notamos que por ejercicio 2, la ecuación $a^2 \equiv -1 \mod p$ solo tiene solución para $p \equiv 1 \mod 4$, por lo que existe $p \mid n$, tal que $p \equiv 1 \mod 4$, lo que también es una contradicción. Por lo que hay infinitos primos de esta forma.

II) Supongamos que existen finitos primos de la forma $p \equiv 3 \mod 4$, luego sea $n = 4(p_1 \cdot ... \cdot p_l) - 1$, donde $p_j \equiv 3 \mod 4$, notamos que $p_j \nmid n$, por lo que

$$p \mid n \implies p \equiv 1 \mod 4$$

Luego $n = p_1^{\alpha_1} \cdot ... \cdot p_k^{\alpha_k}$, donde son primos de la forma $p_i \equiv 1 \mod 4$, por lo que

$$\begin{aligned} n &\equiv \prod_i p_i^{\alpha_i} \mod 4 \\ &\equiv \prod_i 1^{\alpha_i} \mod 4 \\ &\equiv 1 \mod 4 \end{aligned}$$

Pero recordamos que $n \equiv 3 \mod 4$, por lo que hay infinitos primos de la forma $p \equiv 3 \mod 4$

■

Problema 4 (4 pts.)**.** Sea χ es carácter de Dirichlet módulo 4 no trivial. Demuestre que

$$L(1, \chi) = \frac{\pi}{4}$$

Solución problema 4: Se puede notar que el carácter no trivial es el siguiente:

$$\chi(n) = \begin{cases} 1 & n \equiv 1 \mod 4 \\ -1 & n \equiv 3 \mod 4 \\ 0 & \text{en otro caso} \end{cases}$$

Por lo que se sabe que

$$L(1, chi) = \sum_{n \geq 1} \frac{\chi(n)}{n} = \sum_{k \geq 0} \left(\frac{1}{4k+1} - \frac{1}{4k+3} \right)$$

Por otro lado

$$\begin{aligned} \arctan(1) &= \int_0^1 \frac{1}{1+x^2} \, \mathrm{d}x \\ &= \int_0^1 (1 - x^2 + x^4 - x^6 + ...) \, \mathrm{d}x \\ &= x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + ... \Big|_0^1 \\ &= 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + ... \\ &= \sum_{k \geq 0} \frac{1}{4k+1} - \frac{1}{4k+3} \end{aligned}$$

Usando la identidad de la progresión geométrica

$$\frac{1}{1-r} = 1 + r + r^2 + r^3 + ...$$

Y tomamos $r = -x^2$, lo cual es menor igual a uno, por lo que se cumple. Con esto se ve que

$$L(1, \chi) = \arctan(1) = \frac{\pi}{4}$$

■

Problema 5 (4 pts.)**.** Sea $f(t) \in \mathbb{Z}[t]$ un polinomio no constante. Demuestre que existen infinitos primos p tales que la congruencia

$$f(x) \equiv 0 \mod p$$

tiene solución $x \in \mathbb{Z}$

Solución problema 5: Sea $p(x) \in \mathbb{Z}[x]$ tal que la siguiente congruencia solo tenga solución en finitos primos $A = \{p_1, ..., p_l\}$

$$f(x) \equiv 0 \mod p$$

Luego nos tomamos $n \in \mathbb{Z}$ tal que $p(n) = a \neq 0$ y construimos el polinomio

$$q(x) = a^{-1}p(n + x \cdot p_1 \cdot ... \cdot p_l \cdot a)$$

Notamos que este polinomio pertenece a $\mathbb{Z}[x]$.

$$\therefore q(x) \equiv 1 \mod p_i \quad \text{donde } p_i \in A$$

Por lo que existe $p \notin A : p \mid q(x)$ para algún x, luego si $p \mid q(x) \implies p \mid p(n+x\cdot p_1 \cdot ... \cdot p_l \cdot a \implies \exists \alpha : p(\alpha) \equiv 0 \mod p$, pero $p \notin A$ lo que es una contradicción. Tienen que haber infinitos primos tal que tenga solucón.

■