Tarea IV: Congruencias y Reciprocidad Cuadrática
Teoría de los números I
Fecha de entrega: viernes, 24/mayo/2019

Los números entre los paréntesis denota el puntaje de ese ejercicio. Hay un total de puntos.

Ejercicio 1. (2) Criterios de divisibilidad. Prueba que:

1. (1) 3 divide a n si y solamente si la suma de sus dígitos es divisible entre 3.
2. (1) 11 divide a n si y solamente si la suma alternada de sus dígitos es divisible por 11.

Ejercicio 2. (2) Prueba que las ecuaciones $3x^2 + 2 = y^2$ y $7x^3 + 2 = y^3$ no tienen solución en los enteros. También prueba que$5n^3 + 7n^5 \equiv 0 \mod 12$.

Ejercicio 3. (3) Prueba que

$$(n-1)! \equiv \begin{cases} -1 \mod n & n \text{ es primo} \\ 0 \mod n & n \text{ es compuesto} \\ 2 \mod n & n = 4 \end{cases}$$

Ejercicio 4. (6) Ecuaciones polinomiales módulo un número compuesto.

1. (1) Sea $f(x)$ un polinomio con coeficientes enteros y $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$. Prueba que $f(x) \equiv 0 \mod m$ tiene solución si y solamente si $f(x) \equiv 0 \mod p_i^{\alpha_i}$ tiene solución para toda $i = 1, \ldots, s$.
2. (2) Define N como la cantidad de soluciones en $\mathbb{Z}/m\mathbb{Z}$ de $f(x) \equiv 0 \mod m$ y N_i como la cantidad de soluciones en $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ de $f(x) \equiv 0 \mod p_i^{\alpha_i}$ para toda $i = 1, \ldots, s$. Prueba que $N = N_1 N_2 \cdots N_s$. También calcula N para $f(x) = x^2 - 1$ y $m = 2^\alpha$ para cualquier exponent $\alpha \geq 0$.
3. (2) Ahora fija $f(x) = x^2 - 1$ y definimos $S_m \subseteq \mathbb{Z}/m\mathbb{Z}$ como las soluciones de la ecuación $x^2 \equiv 1 \mod m$. Prueba que $S_{p^\alpha} = \{\overline{1}, \overline{-1}\}$ para todo primo $p > 2$ y exponente $\alpha > 0$.
4. (1) Junta los resultados anteriores para calcular, en general, cuantas soluciones en $\mathbb{Z}/m\mathbb{Z}$ tiene la congruenca $x^2 \equiv 1 \mod m$.

Ejercicio 5. (3) Sea p un primo y $\binom{p}{k}$ el coeficiente binomial. Prueba que para $0 < k < n$, se tiene que $p \mid \binom{p}{k}$. Concluye que $(a+b)^p \equiv a^p + b^p \mod p$ para toda $a, b \in \mathbb{Z}$. Enuncia y prueba el pequeño teorema de Fermat con este hecho.

Ejercicio 6. (1) Sean $p \neq q$ primos distintos tales que $p - 1 \mid q - 1$. Prueba que

$$(n, pq) = 1 \Longrightarrow n^{q-1} \equiv 1 \mod pq$$

Ejercicio 7. (2) Prueba que $a^{\varphi(2^m)/2} \equiv 1 \mod 2^m$ para toda $a \in \mathbb{Z}$ y $m > 2$. ¿Qué dice este resultado sobre la existencia de raices primitivas módulo 2^m? Calcula las raices primitivas módulo 2^m para toda $m > 0$.

Ejercicio 8. (5) Propiedades de $\operatorname{ord}_m(\overline{a})$.

1. (1) Prueba que $p > 2$ es primo si y solamente si $\operatorname{ord}_p(\overline{a}) = p - 1$ para alguna $a \in \mathbb{Z}$.
2. (1) Sea p un primo de la forma $4k + 3$ y $\overline{a}$ una raíz primitiva. Prueba que $\operatorname{ord}_p(-\overline{a}) = \frac{p-1}{2}$.
3. (2) Sean $a, m > 1$ tales que $(a, m) = 1$ y denota $\varepsilon := \operatorname{ord}_m(\overline{a})$. Para $k, k' > 0$ prueba que

$$a^k \equiv a^{k'} \mod m \iff k \equiv k' \mod \varepsilon$$

4. (1) Sean $a, b \in \mathbb{Z}$ y $m > 1$ tales que $(a, m) = 1 = (b, m)$ y $\big(\operatorname{ord}_m(\overline{a}), \operatorname{ord}_m(\overline{b})\big) = 1$. Prueba que $\operatorname{ord}_m(\overline{a}\overline{b}) = \operatorname{ord}_m(\overline{a}) \cdot \operatorname{ord}_m \overline{b}$.

Tarea IV: Congruencias y Reciprocidad Cuadrática
Teoría de los números I
Fecha de entrega: viernes, 24/mayo/2019

Ejercicio 9. (1) Sea $\overline{a}$ una raíz primitiva módulo $p > 2$. Prueba que $\{a^2, a^4, \ldots, a^{p-1}\}$ son los residuos cuadráticos módulo p y $\{a, a^3, \ldots, a^{p-2}\}$ son los residuos no-cuadráticos.

Ejercicio 10. (1) Demuestra que hay una infinidad de primos de la forma $6k + 1$.

Ejercicio 11. (3) Sea $p > 2$ un primo y $U(\mathbb{Z}/p\mathbb{Z}) = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$. Sean $S, T \subseteq U(\mathbb{Z}/p\mathbb{Z})$ subconjuntos y define $S \cdot T := \{\overline{s}\overline{t} \mid \overline{s} \in S, \overline{t} \in T\}$; también define $T \cdot T = T^2$ y $S \cdot S = S^2$ de manera análoga (observa que $S \cdot T = T \cdot S$). Si $S, T \subseteq U(\mathbb{Z}/p\mathbb{Z})$ cumplen las siguientes propiedades:

- $S \neq T$
- $S \cup T = U(\mathbb{Z}/p\mathbb{Z})$
- $S \cdot T \subseteq T$
- $S^2, T^2 \subseteq S$

Prueba que S es el conjunto de residuos cuadráticos módulo p y T es el conjunto de residuos no-cuadráticos módulo p.

Ejercicio 12. (1) Sean $a \in \mathbb{Z}$ y $p > 2$ pimos tales que $p \nmid a$. Prueba que la ecuación general $ax^2 + bx + c \equiv 0 \mod p$ tiene $1 + \left(\frac{b^2-4ac}{p}\right)$ soluciones.

Ejercicio 13. (5) Identidades del símbolo de Legendre.

1. (1) Prueba que para todo primo $p > 2$ se cumple:
$$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = 0$$
2. (2) Toma $a, b \in \mathbb{Z}$ tal que $p \nmid a$. Prueba que
$$\sum_{k=1}^{p-1} \left(\frac{ak+b}{p}\right) = 0$$
3. (2) Ahora sea p de la forma $4k + 1$, prueba que
$$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) k = 0$$

Ejercicio 14. (18) Ejercicios numéricos:

1. (1) Resuelve $256x \equiv 179 \mod 337$.
2. (2) Resuelve los siguientes sistemas de congruencias:
$$\begin{aligned} x &\equiv 3 \mod 8 \\ x &\equiv 11 \mod 20 \\ x &\equiv 1 \mod 15 \end{aligned} \qquad \begin{aligned} y &\equiv 1 \mod 7 \\ y &\equiv 4 \mod 9 \\ y &\equiv 3 \mod 5 \end{aligned}$$
3. (3) Calcula todas las raices primitivas de $11, 13$ y 17.
4. (3) Encuentra la soluciones de las siguientes ecuaciones:
$$x^8 \equiv 17 \mod 43 \quad , \quad 8^x \equiv 3 \mod 43 \quad , \quad 1 + x + \cdots + x^6 \equiv 0 \mod 29$$

Tarea IV: Congruencias y Reciprocidad Cuadrática
Teoría de los números I
Fecha de entrega: viernes, 24/mayo/2019

5. (2) Usa el lema de Gauss para calcular $\left(\frac{5}{7}\right)$ y $\left(\frac{3}{11}\right)$
6. (3) Calcula $\left(\frac{61}{233}\right)$ y $\left(\frac{113}{997}\right)$. Además calcula $\left(\frac{-1}{m}\right)$ para $m > 1$ impar.
7. (2) Encuentra todos los primos tales que $\left(\frac{-3}{p}\right) = 1$ y $\left(\frac{7}{p}\right) = 1$
8. (2) ¿Tiene solución de ecuación $x^2 + 5x \equiv 12 \mod 31$? Exhibe las soluciones o prueba que no tiene solución. Haz lo mismo para la ecuación $x^2 \equiv 19 \mod 30$.

Ejercicio 15. (11) Propiedades de raices primitivas.

1. (1) Sea $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ una raíz primitiva módulo m. Prueba que $\overline{b}$ es una raíz primitiva si y solamente si $\overline{b}$ es de la forma $\overline{b} = \overline{a}^n$ donde $(n, \varphi(m)) = 1$ y $1 \leq n \leq \varphi(m)$.
2. (1) Sea $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ con $(a, m) = 1$. Prueba $\overline{a}$ es una raíz primitiva módulo m si y solamente si $\overline{a}^{-1}$ es una raíz primitiva.
3. (1) Sea $\overline{a}$ una raíz primitiva módulo p^α para alguna $\alpha > 0$. Prueba que $\overline{a}$ también es raíz primitiva módulo p.
4. (1) Sea p un primo de la forma $4k+1$. Prueba que $\overline{a}$ es raíz primitiva módulo p si y solamente si $-\overline{a}$ es una raíz primitiva.
5. (3) Para $\overline{a}$ una raíz primitiva módulo un primo p, verifica que

$$\sum_{\substack{k=1 \\ (\varphi(m),k)=1}}^{\varphi(m)} a^k \equiv \mu(p-1) \mod p$$

6. (2) Sea X el conjunto de raices primitivas módulo p.

$$\prod_{\overline{a} \in X} a \equiv 1 \mod p$$

7. (2) Sea $(a, m) = 1$ y $\varphi(m) = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$. Prueba que

$$\overline{a} \text{ es raíz primitiva} \iff a^{\frac{\varphi(m)}{p_i}} \not\equiv 1 \mod m \quad \forall i \in \{1, \ldots, s\}$$

Ejercicio 16. (6) Los primos impares de la forma $4k + 1$ son los únicos primos impares que son suma de dos cuadrados.

1. (2) Sea m un entero libre de cuadrados. Demuestra que, si $a \in \mathbb{Z}$ es primo relativo con m, entonces existen $x, y \in \mathbb{Z}$ tales que $ax \equiv y \mod m$, $0 < x < \sqrt{n}$ y $0 < |y| < \sqrt{n}$.
2. (2) Sea $p > 2$ un primo y define $q := \frac{p-1}{2}$ y $a = q!$. Prueba que $a^2 + (-1)^q \equiv 0 \mod p$.
3. (1) Ahora restringe al caso $p \equiv 1 \mod 4$. Prueba que existen enteros positivos n y m donde $0 < n, m < \sqrt{p}$ tales que satisfacen la ecuación $a^2n^2 - m^2 \equiv 0 \mod p$. Concluye que $p = n^2 + m^2$.
4. (1) Si $p \equiv 3 \mod 4$, prueba que p no puede ser descompuesto en suma de dos cuadrados.

En resumen un primo $p > 2$ es suma de dos cuadrados si y solamente si $p \equiv 1 \mod 4$.