Universidad Nacional Autónoma de México
Facultad de Ciencias
Teoría de los Números I

Tarea 4

Ángel Iván Gladín García
No. cuenta: 313112470
angelgladin@ciencias.unam.mx

24 de mayo 2019

Congruencias y Reciprocidad Cuadrática

Los números entre los paréntesis denota el puntaje de ese ejercicio. Hay un total de 70 puntos.

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

a. (1) 3 divide a n si y solamente si la suma de sus dígitos es divisible entre 3.
<u>Solución</u>: Antes de proceder con la demostración, mostraremos que sean dos enteros n y s, donde n es un entero y s es la represtación de la suma de los dígitos de n, de la forma $n = a_0 + a_1 10^1 + \ldots + a_n 10^n$ y $s = a_0 + a_1 + \ldots + a_n$. La resta $n - s$ divisible por 3.

$$\begin{aligned}
n - s &= a_0 + a_1 10^1 + \ldots a_n 10^n - a_0 - a_1 - \ldots - a_n \\
&= (a_0 - a_0) + (a_1 10^1 - a_1) + \ldots + (a_n 10^n - a_n) \\
&= a_1(10^1 - 1) + \ldots + a_n(10^n - 1) \\
&= \sum_{i=1}^{n} a_i b_i && \text{Con } b_i = (10^i - 1)
\end{aligned}$$

Entonces se sigue que $9 \mid b_i$ y en particular $3 \mid b_i$. Ergo $3 \mid n - s$.
$\Longrightarrow$) Por demostrar que la s, suma de los dígitos de n es divisible entre 3.

$$\begin{aligned}
3 &\mid n && \text{Por hipótesis} && (1) \\
3 &\mid n - s && \text{Por análisis previo} && (2) \\
3(r - s) &= s && \text{Aplicando definición de divisibilidad y restando (1) y (2)}
\end{aligned}$$

Por tanto $3 \mid s$.
$\Longleftarrow$) Por demostrar que 3 divide a n.
Análogo al caso anterior.

b. (1) 11 divide a n si y solamente si la suma alternada de sus dígitos es divisible por 11.
<u>Solución</u>: Evidentemente $10 \equiv -1 \mod 11$.

Sea $n = a_k 10^k + a_{k-1}10^{k-1} + \ldots + a_0$ la representación del número en base 10.

$$
\begin{aligned}
& n = a_k 10^k + a_{k-1}10^{k-1} + \ldots + a_0 \equiv 0 \pmod{11} \\
\iff & \begin{cases} a_k 10^k \equiv a_k(-1)^k \pmod{11} \\ a_{k-1}10^{k-1} \equiv a_{k-1}(-1)^{k-1} \pmod{11} \\ \qquad \vdots \\ a_0 \equiv a_0 \pmod{11} \end{cases} \\
\iff & a_k 10^k + a_{k-1}10^{k-1} + \ldots + a_0 \equiv a_k(-1)^k + a_{k-1}(-1)^{k-1} + a_0 \pmod{11}
\end{aligned}
$$

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 $5n^3 + 7n^5 \equiv 0 \pmod{12}$.

a. Por demostrar que la ecuación no tiene $3x^2 + 2 = y^2$ solución en los enteros.
   <u>Solución</u>: Reescribiendo la ecuación se tiene $3x^2 = y^2 - 2$ lo que implica que 3 es un múltiplo de $y^2 - 2$ y por definición de divisibilidad se sigue que $3 \mid y^2 - 2$ que visto como congruencia es $y^2 \equiv 2 \pmod{3}$.
   Por demostrar que todo número perfecto no deja residuo 2 cuando es dividido por 3.
   Sea n^2 modulo 3, se puede expresar n de la forma $3r$,$3r + 1$ y $3r + 2$, entonces $n^2 = 9r^2$, $n^2 = 9r^2 + 6r + 1$ o $n^2 = 9r^2 + 12r + 4 = 9r^2 + 12r + 1$. Mostrando así que todo número perfecto deja de residuo 0 ó 1 módulo 3 y por tanto $y^2 \not\equiv 2 \pmod{3}$.

b. Por demostrar que la ecuación no tiene $7x^3 + 2 = y^3$ solución en los enteros.
   <u>Solución</u>: Reescribiendo se tiene que $7x^2 = y^3 - 2$ lo que significaría que $y^3 \equiv -2 \pmod{7}$.
   Viendo los residuos que deja la congruencia que son:

   - $0^3 = 0 \equiv 0 \pmod{7}$
   - $1^3 = 1 \equiv 1 \pmod{7}$
   - $2^3 = 8 \equiv 1 \pmod{7}$
   - $3^3 = 27 \equiv 6 \pmod{7}$
   - $4^3 = 16 \cdot 4 = 2 \cdot 4 \equiv 1 \pmod{7}$
   - $5^3 = 15 \cdot 5 = 4 \cdot 5 = 20 \equiv 6 \pmod{7}$
   - $6^3 = 36 \cdot 6 = 1 \cdot 6 \equiv 6 \pmod{7}$

   Ergo, viendo los casos exhaustivamente $y^3 \not\equiv -2 \pmod{7}$.

c. Por demostrar que $5n^3 + 7n^5 \equiv 0 \pmod{12}$
   <u>Solución</u>: No supe como hacerlo y opté por hacer un programa en *Python* para ver que $5n^3 + 7n^5 \equiv 0 \pmod{12}$.

```python
# Modulo de la congrunencia
m = 12
# Polinomio que es evaluado en n modulo m
f = lambda n, m: pow(5 * n, 3, m) + pow(7 * n, 5, m)
# Contador de posibles valores que sera congruente
r = 0
```

```
# Correr la x en [0, m)
for x in range(m):
    # Verificar si es congruente
    if f(x, m) %m == 0:
        r += 1
# Numero de veces que la x fue congruente
print(r)
```

Después de ejecutar el programa el, se vio que $r = 12$ lo que significa que evaluado la congruencia todos los valores que puede tomar hace que la congruencia se satisfaga.

Ejercicio 3. (3) Prueba que

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

a. $(n-1)! \equiv -1 \mod n \quad n$ es primo
Solución: Teorema de Wilson. Si $p = 2$ entonces se sigue que $1 \equiv -1 \mod 2$, lo cual es válido para $p = 2$.
Sea $p > 2$. El juego de residos de 1 a $p-1$ son invertibles módulo p por un corolorio que dice que $ax \equiv b \mod m$ tiene solución si y solo sí $(a, m) = 1$ y en particular tomando la congruencia $ax \equiv 1 \mod m$ si y solo si $(a, m) = 1$, pero esta congruencia se satisface si tomamos a $x = a^{-1}$ resultando como $aa^{-1} \equiv 1 \equiv 1 \mod m$. Pero por un lema que dice que un entero positivo a es autoinvertible módulo p si y solo si $a \equiv \pm 1 \mod p$ se sigue que 1 y $p-1$ son sus propios autoinversos.
Sabiendo eso, agrupando los $p-3$ residuos en pares con $\frac{p-3}{2}$ parejas de inversos a y $b = a^{-1}$ tales que $ab \equiv 1 \mod p$ para cada pareja, tenindo así:

$$\begin{aligned} 2 \cdot 3 \cdots (p-2) \equiv & 1 \mod p \\ (p-1)! &= 1 \cdot [2 \cdot 3 \cdots (p-2)] \cdot (p-1) \\ &\equiv 1 \cdot 1 \cdot (p-1) \mod p \\ & -1 \mod p \end{aligned}$$

b. $(n-1)! \equiv 0 \mod n \quad n$ es compuesto
Solución: Suponiendo que n es compuesto, entonces es de la forma $n = ab$ donde hay dos posibles casos; cuando $a \neq b$ y $a = b$.
Si $n = ab$ con $a \neq b$ y $1 < a, b < n$, entonces se tiene que:

$$(n-1)! = 1 \cdot 2 \cdots a \cdots b \cdots (n-1)$$

y por tanto $n = ab \mid (n-1)!$.
En el caso de que $a = b$, ósea $n = a^2$ y como $a > 1$ se sigue que:

$$(n-1)! = 1 \cdot 2 \cdots a \cdot 2a \cdots (a-k)a \cdots (a^2-1)$$

Pero $2a < a^2 = n$, pero ambos a y $2a$ serán factores de $(n-1)!$ y por tanto $n \mid (n-1)!$.

c. $(n-1)! \equiv 2 \mod n \quad n = 4$
Solución: Si $n = 4$, entonces $(n-1)! = 2 \cdot 3 = 6 \equiv 2 \mod 4$.

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

a. (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 $i = 1, \ldots, s$.
Solución: $\Longrightarrow$) Sea x_0 una solución de $f(x) \equiv 0 \mod m$, tal que $f(x_0) \equiv 0 \mod m$. Como $p_i^{\alpha_i} \mid m$ para toda $i = 1, \ldots, s$, se sigue que $f(x_0) \equiv 0 \mod p_i^{\alpha_i}$ para toda $i = 1, \ldots, s$.
$\Longleftarrow$) Si existe x_i tal que $f(x_i) \equiv 0 \mod p_i^{\alpha_i}$ para $i = 1, \ldots, s$, por el Teorema chino del residuo existe x tal que $x \equiv x_i \mod p_i^{\alpha_i}$ para $i = 1, \ldots, s$, por tanto x es una solución.

b. (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 $\alpha \geq 0$.

- Por demostrar que $N = N_1 N_2 \cdots N_s$.
  Solución: Sea $(b_1, \ldots, b_t)$ una solución al sistema $f(x) \equiv 0 \mod p_i^{\alpha_i}$. Por el teorema chino del residuo, existe un x tal que $x \equiv b_i \mod p_i^{\alpha_i}$. Afirmando que x es solución para $f(x) \equiv 0 \mod n$. En efecto, es lo mismo que decir que que $f(x)$ es divisible por $p_i^{\alpha_i}$ para $i = 1, \ldots, t$. Pero dado que $x \equiv b_i \mod p_i^{\alpha_i}$, y si f es un polinomio, $f(x) \equiv f(b_i) \equiv 0 \mod p_i^{\alpha_i}$, así que $f(x)$ es divisible por $p_i^{\alpha_i}$ para toda i.

  Por tanto, hay una correspondencia biyectiva entre las tuplas $(b_1, \ldots, b_t)$ formando soluciones a $f(x) \equiv 0 \mod p_i^{\alpha_i}$, y siendo x' la solución a $f(x) \equiv 0 \mod n$.
- tiene dos sols alv

c. (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 $\alpha > 0$.
Solución:

d. (1) Junta los resultados anteriores para calcular, en general, cuantas soluciones en $\mathbb{Z}/m\mathbb{Z}$ tiene la congruenca $x^2 \equiv 1 \mod m$.
Solución:

Ejercicio 5. (3) Sea p un primo y $\binom{p}{k}$ el coeficiente binomial. Prueba que para $0 < k < p$, 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.

- Por demostrar que $p \mid \binom{p}{k}$
  Solución: Evidentemente por definición del teorema del binomio se tiene que:

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}$$

  Y reescribiendo se tiene que $p \mid p\frac{(p-1)!}{k!(p-k)!}$ y p divide al numerador y niguno de sus factores del denominador es divisible por p.

- Por demostrar que $(a+b)^p \equiv a^p + b^p \mod p$
  Solución: Usando el teorema del binomio, se tiene que:

$$(a+b)^n = a^n + \sum_{m=1}^{n-1} \binom{n}{m} a^{n-m} b^m + b^n$$

Entonces:

$$\begin{aligned}
(a+b)^p &= a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k + b^p \mod p \\
&\equiv a^p + b^p \mod p \qquad\qquad \text{Porque } p \mid \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k
\end{aligned}$$

- **(Pequeño teorema de Fermat)** Sea p un primo y a cualquier entero tal que $p \nmid a$. Entonces:

  $$a^{p-1} \equiv 1 \mod p$$

  <u>Solución</u>: Sea p un primo y sea cualquier entero a talque $p \nmid a$. Entonces el juego de residos de los enteros $a, 2a, 3a, \ldots, (p-1)a$ módulo p son una permutación de los enteros $1, 2, 3, \ldots, (p-1)$.
  Sabiendo eso, si tomamos el juego de residos $a, 2a, 3a, \ldots, (p-1)a$ módulo p son los mismos como los enteros $1, 2, 3, \ldots, (p-1)$ en el mismo orden, así que su productos son congruentes módulo p, que es, $a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \mod p$. Escrito de otra forma $(p-1)!a^{p-1} \equiv (p-1)! \mod p$.
  Recordando un teorema que dice que si $ac \equiv bc \mod m$ y $(c, m) = 1$, entonces $a \equiv b \mod m$. Usando el teorema se tiene que $((p-1)!, p) = 1$, por tanto $a^{p-1} \equiv 1 \mod p$.

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

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

<u>Solución</u>: Como por hipótesis se tiene que $p - 1 \mid q - 1$, existe una k tal que:

$$(p-1)k = q - 1 \tag{1}$$

Como por hipótesis $(n, pq) = 1$ y en particular se tiene que $(n, p) = (n, q) = 1$, utilizando el pequeño teorema de Fermat se obtienen las siguientes congruencias:

$$n^{q-1} \equiv 1 \mod q \tag{2}$$

$$n^{p-1} \equiv 1 \mod p \tag{3}$$

Por consiguiente, usando (1) se puede escribir (2) de la siguiente manera, obteniendo así siguientes congruencia:

$$n^{q-1} = n^{(p-1)k} = (n^{p-1})^k \equiv 1^k \mod p \tag{4}$$

Por el teorema chino del residuo, existe una x tal que es solución del sistema de congruencias y ésta es a su vez es única.
Considerando el siguiente sistema de congruencias:

$$\begin{aligned}
x &\equiv 1 \mod p \\
x &\equiv 1 \mod q
\end{aligned}$$

Ergo, dicho lo anterior, tomando $x = n^{p-1}$ es una solución del sitema, concluyendo que:

$$n^{q-1} \equiv 1 \mod pq$$

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 $m > 0$.
Solución: Por inducción sobre m:

- Caso base ($m = 3$):
  Entonces la congruencua queda como $x^{\varphi(2^m)/2} \equiv 1 \mod 8$ para un x impar Porque probando los números que son congruentes son $x = 1, 3, 5, 7$ y de hecho todas la x son impares.

- Hipótesis de inducción:
$$x^{\varphi(2^m)/2} = 1 + 2^m t \tag{1}$$

- Paso inductivo ($m + 1$):
  Elevando al cuadrado ambos lados de la ecuación (1) se obtiene:
$$x^{\varphi(2^m)} = 1 + 2^{m+1}t + 2^{2m}t^2 \equiv \quad \mod 2^{m+1}$$

  Este resultado nos dice que no hay raíces primitiva $\mod 2^m$ y que las raíces primitivas módulo 2^m son $\varphi(2^{m-1}) = \varphi(2^{m+1})/2$.

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

a. (1) Prueba que $p > 2$ es primo si y solamente si $\mathrm{ord}_p(\overline{a}) = p - 1$ para alguna $a \in \mathbb{Z}$.
Solución: $\Longrightarrow$) Por definición de raíz primitiva se tiene que:
$$\mathrm{ord}_p(a) = \varphi(p) = p - 1$$
$\Longleftarrow$) Como $\mathrm{ord}_p(a) = p - 1$ entonces $p - 1 = \mathrm{ord}_p(a) \leq \varphi(p) \leq p - 1$, y por la hipótesis eso pasa si p es primo.

b. (1) Sea p un primo de la forma $4k + 3$ y $\overline{a}$ una raíz primitiva. Prueba que $\mathrm{ord}_p(-\overline{a}) = \frac{p-1}{2}$.
Solución:

c. (2) Sean $a, m > 1$ tales que $(a, m) = 1$ y denota $\varepsilon := \mathrm{ord}_m(\overline{a})$. Para $k, k' > 0$ prueba que
$$a^k \equiv a^{k'} \mod m \quad \Longleftrightarrow \quad k \equiv k' \mod \varepsilon$$
Solución:

d. (1) Sean $a, b \in \mathbb{Z}$ y $m > 1$ tales que $(a, m) = 1 = (b, m)$ y $\big(\mathrm{ord}_m(\overline{a}), \mathrm{ord}_m(\overline{b})\big) = 1$. Prueba que $\mathrm{ord}_m(\overline{a}\overline{b}) = \mathrm{ord}_m(\overline{a}) \cdot \mathrm{ord}_m\overline{b}$.
Solución: Sea $x = \mathrm{ord}_m(a)$ y $y = \mathrm{ord}_m(b)$, usando la definición de raíz primitiva se sigue la siguiente congruencia:
$$(ab)^{xy} \equiv (a^x)^y (a^y)^x \equiv 1 \mod m$$
Sea $k = \mathrm{ord}_m(ab)$ y suponiendo que $k \mid xy$, se tiene:
$$a^{ky} \equiv (ab)^{ky} \equiv 1 \mod m$$
Lo significa que $x \mid ky$, como $(x, y) = 1$ nos lleva a que $x \mid ky$. Como por hipótesis $(a, m) = 1 = (b, m)$ entonces se tiene que $x \mid k$ y $y \mid k$, se sigue que $xy \mid k$. Ergo $k = xy$, lo que significa que $\mathrm{ord}_m(\overline{a}\overline{b}) = \mathrm{ord}_m(\overline{a}) \cdot \mathrm{ord}_m\overline{b}$.

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.
<u>Solución</u>: Si n es par, digamos $n = 2m$ entonces $a^n = (a^m)^2$ así que

$$a^n \equiv x^2 \mod p \qquad \text{Donde } x = a^m$$

Por consiguiente $a^n Rp$. Pero hay $\frac{p-1}{2}$ distintas potencias pares $a^2, \ldots, a^{p-1}$ módulo p y el mismo números de residuos cuadráticos módulo p. Por tanto las potencias pares son los residuos cuadráticos y las potencias impares son los residuos no-cuadráticos.

Ejercicio 10. (1) Demuestra que hay una infinidad de primos de la forma $6k + 1$.
<u>Solución</u>: Sea P el conjunto finito de número primos de la forma $6k + 1$, y sea N un número que es divisible por cada número en P. Suponiendo que N es también por 6. Sea p un primo divisor de $N^2 - N + 1$.

Teniendo en cuenta que $(N^2 - N + 1)(N + 1) = N^3 + 1$, así p divide a $N^3 + 1$, o en otras palabras $N^3 \equiv -1 \mod p$ y así $N^6 \equiv 1 \mod p$.

Recordando que el orden de N módulo p es el menor entero positivo k tal que $N^k \equiv 1 \mod p$. El orden debe dividir a 6, tal que $k = 1, 2, 3$ ó 6. Pero $N^3 \equiv -1 \mod p$, por lo que el orden no puede ser 1 ó 3.

El orden no puede ser 2 porque si $N^2 \equiv 1 \mod p$ y $N^3 \equiv -1 \mod p$ entonces $N \equiv -1 \mod p$. Lo que no se podría porque entonces p dividiría a ambos $N + 1$ y $N^2 - N + 1$, pero el $(N + 1.N^2 - N + 1) = (N + 1, 3) < p$ lo cual es una contradicción.

Por consiguiente, N tiene orden 6 módulo p y el grupo de las unidades módulo p tiene orden $p - 1$, de esta manera 6 divide a $p - 1$, lo que significa que p es de la forma $6k + 1$. Por tanto, P no contiene a todos los primos de la forma $6k + 1$, concluyendo que el conjuto de primo de esa forma es infinito.

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:

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

Prueba que S es el conjunto de residuos cuadráticos módulo p y T es el conjunto de residuos no-cuadráticos módulo p.
<u>Solución</u>:

Ejercicio 12. (1) Sean $a \in \mathbb{Z}$ y $p > 2$ primos 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.
<u>Solución</u>:

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

a. (1) Prueba que para todo primo $p > 2$ se cumple:

$$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = 0$$

Solución: Como hay exactamente tantos residuos cuadráticos como no residuo cuadráticos y para los residuos $\left(\frac{k}{p}\right) = 0$ y para los no residuos es igual a -1, entonces la suma da 0.

b. (2) Toma $a, b \in \mathbb{Z}$ tal que $p \nmid a$. Prueba que

$$\sum_{k=1}^{p-1} \left(\frac{ak+b}{p}\right) = 0$$

Solución: Como $p \nmid a$ entonces $\{a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)\}$ es el juego completo de residuos módulo p y por lo tanto también es $\{a \cdot 1 + b, a \cdot 2 + b, \ldots, a \cdot (p-1) + b\}$ y utilizando el ejercicio anterior se sigue que la suma da 0.

c. (2) Ahora sea p de la forma $4k + 1$, prueba que

$$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) k = 0$$

Solución:

Ejercicio 14. (18) Ejercicios numéricos:

a. (1) Resuelve $256x \equiv 179 \mod 337$.
Solución: Verificando primero que $(256, 337) = 1$ y como $1 \mid 179$ entonces sí tiene solución y tiene 1 solución incongruente. Las soluciones están dadas por $x = x_0 + (\frac{m}{d})t = x_0 + (\frac{337}{1})t = x_0 + 337t$, donde x_0 es una solución particular. Ahora por *prueba y error* se tiene que $x_0 = 81$ es una solución.
Ergo la solución general es de la forma $x = 81 + 337t$.

b. (2) Resuelve los siguientes sistemas de congruencias:

$$\begin{aligned} x &\equiv 3 \mod 8 \\ x &\equiv 11 \mod 20 \\ x &\equiv 1 \mod 15 \end{aligned}$$

Solución: Como soy pésimo haciendo cuentas y sé programar, use un programa en **Python**[1] que por medio del Teorema Chino del residuo primero dice si tiene solución el sistema y si existe, calcula x.

```
from functools import reduce


def chinese_remainder(n, a):
```

[1] Para usarlo con la terminal poner `$ python3 chinese_remainder_theorem.py`

```python
    sum = 0
    prod = reduce(lambda a, b: a * b, n)
    for n_i, a_i in zip(n, a):
        p = prod // n_i
        sum += a_i * mul_inv(p, n_i) * p
    return sum % prod


def mul_inv(a, b):
    b0 = b
    x0, x1 = 0, 1
    if b == 1:
        return 1
    while a > 1:
        q = a // b
        a, b = b, a % b
        x0, x1 = x1 - q * x0, x0
    if x1 < 0:
        x1 += b0
    return x1

# Numero de congruencias
# Ejemplo: 3
x = int(input())
# x \equiv a_i \mod m_i
# Lista que tendra los a_i y la otra que tendra los m_i
n, m = [], []

for _ in range(x):
    # Entrada: a_i m_i
    # Ejemplo: 1 2
    a, b = map(int, input().split())
    n.append(a)
    m.append(b)

print(chinese_remainder(n, m))
```

En este caso la congruencia tiene solución y es $x = 20$.

$$\begin{aligned} y &\equiv 1 \mod 7 \\ y &\equiv 4 \mod 9 \\ y &\equiv 3 \mod 5 \end{aligned}$$

<u>Solución</u>: Usando el programa de arriba se tiene que que la solución es $x = 5$.

c. (3) Calcula todas las raices primitivas de $11, 13$ y 17.
Igual como soy malo haciendo cuentas y esas cosas, use *Python* para calcularlas[2].

[2]Teniendo instalado `sympy==1.3` en Python 3.7, abrir el interprete y primero im-

- Las raíces primitivas de 11 son: $\{2, 6, 7, 8\}$.
- Las raíces primitivas de 13 son: $\{2, 6, 7, 11\}$.
- Las raíces primitivas de 17 son: $\{3, 5, 6, 7, 10, 11, 12, 14\}$.

d. (3) Encuentra la soluciones de las siguientes ecuaciones:

$$x^8 \equiv 17 \mod 43 \quad , \quad 8^x \equiv 3 \mod 43 \quad , \quad 1 + x + \cdots + x^6 \equiv 0 \mod 29$$

Solución:

e. (2) Usa el lema de Gauss para calcular $\left(\frac{5}{7}\right)$ y $\left(\frac{3}{11}\right)$
Solución:

- $\left(\frac{5}{7}\right)$: $\frac{7-1}{2} = 3$, y así los residuos de $1 \cdot 5, 2 \cdot 5, 3 \cdot 5$ son $-2, 3, 1$ respectivamente, así $\mu = 1$ y $\left(\frac{5}{7}\right) = (-1)^\mu = -1$.
- $\left(\frac{3}{11}\right)$: $\frac{11-1}{2} = 5$, y así los residuos de $1 \cdot 3, 2 \cdot 3, 3 \cdot 3, 3 \cdot 4, 4 \cdot 3, 5 \cdot 3$ son $3, -1, -2, 1, 4$ respectivamente, así $\mu = 2$ y $\left(\frac{3}{13}\right) = (-1)^\mu = 1$.

f. (3) Calcula $\left(\frac{61}{233}\right)$ y $\left(\frac{113}{997}\right)$. Además calcula $\left(\frac{-1}{m}\right)$ para $m > 1$ impar.

- $\left(\frac{113}{997}\right)$.
Solución: Usando el símbolo de Jacobbi se tiene:

$$\left(\frac{113}{997}\right)\left(\frac{997}{113}\right) = (-1)^{\frac{113-1}{2}\frac{997-1}{2}} = (-1)^{56 \cdot 498} = 1$$

Así, $\left(\frac{113}{997}\right) = \left(\frac{997}{113}\right) = \left(\frac{93}{113}\right)$. Aplicando reciprocidad cuadrática de nuevo se tiene

$$\left(\frac{93}{113}\right)\left(\frac{113}{93}\right) = (-1)^{\frac{93-1}{2}\frac{113-1}{2}} = (-1)^{46 \cdot 56} = 1$$

Así, $\left(\frac{93}{113}\right) = \left(\frac{113}{93}\right) = \left(\frac{20}{93}\right) = \left(\frac{4}{93}\right) \cdot \left(\frac{5}{93}\right)$, como 4 siempre es residuo cuadrático, se tiene:

$$\left(\frac{5}{93}\right)\left(\frac{93}{5}\right) = (-1)^{\frac{93-1}{2}\frac{5-1}{2}} = (-1)^{46 \cdot 2} = 1$$

Y entonces $\left(\frac{5}{93}\right) = \left(\frac{93}{5}\right) = \left(\frac{3}{5}\right) = -1$ y como 1, 4 son los únicos residuos cuadráticos módulo 5.
- $\left(\frac{-1}{m}\right)$ para $m > 1$ impar.
Solución: $\left(\frac{-1}{m}\right)$: son los residuos del los primeros $\frac{m-1}{2}$ mútiplos de -1 todos negativos, así $\left(\frac{-1}{m}\right) = (-1)^\mu = (-1)^{(p-1)/2}$.

portar `sympy` para poder usarlo (con `import sympy`) y despues la siguiente función `list(sympy.ntheory.residue_ntheory._primitive_root_prime_iter(n))` donde en la `n` ponemos el número y nos regresará una lista con las raíces primitivas del número dado.

g. (2) Encuentra todos los primos tales que $\left(\frac{-3}{p}\right) = 1$ y $\left(\frac{7}{p}\right) = 1$
Solución:

h. (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 $x^2 \equiv 19 \mod 30$.
Solución:

Ejercicio 15. (11) Propiedades de raices primitivas.
Quiero tomar este ejercicio gratis

a. (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 $1 \leq n \leq \varphi(m)$.
Solución:

b. (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.
Solución:

c. (1) Sea $\overline{a}$ una raíz primitiva módulo p^α para alguna $\alpha > 0$. Prueba que $\overline{a}$ también es raíz primitiva módulo p.
Solución:

d. (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.
Solución:

e. (3) Para $\overline{a}$ una raíz primitiva módulo un primo p, verifica que

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

Solución:

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

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

Solución:

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

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

Solución:

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

a. (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 $0 < |y| < \sqrt{n}$.
Solución:

b. (2) Sea $p > 2$ un primo y define $q := \frac{p-1}{2}$ y $a = q!$. Prueba que $a^2 + (-1)^q \equiv 0 \mod p$.
Solución:

c. (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 $p = n^2 + m^2$.
Solución:

d. (1) Si $p \equiv 3 \mod 4$, prueba que p no puede ser descompuesto en suma de dos cuadrados.
Solución:

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

Referencias

[1] Thomas Koshy. *Elementary Number Theory with Applications. 2nd Edition.* Addison-Wesley, Reading, Massachusetts, 1993. Academic Press. 8th May 2007.

[2] Apostol, Tom M. *Introduction to Analytic Number Theory.* Springer-Verlag, New York, 1976.

[3] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory (Graduate Texts in Mathematics)* Springer, Springer; 2nd edition (August 1, 1998).