Ejercicio 2. Suponga que $a \equiv b \pmod{m}$, para cierto entero m fijo. Probar las siguientes propiedades:

a. $\lambda a \equiv \lambda b \pmod{m}$, para todo $\lambda \in \mathbb{Z}$.

b. $a^n \equiv b^n \pmod{m}$ para todo $n \in \mathbb{N}$. Sugerencia: usar el teorema del binomio.

c. Si $a \equiv 3 \pmod{5}$, hallar el resto de dividir $4a^3$ entre 5.

d. Usando las propiedades anteriores, probar que si $p(x) = \lambda_n x^n + \lambda_{n-1} x^{n-1} + \ldots + \lambda_1 x + \lambda_0$, es un polinomio con coeficientes enteros λ_i, entonces $p(a) \equiv p(b) \pmod{m}$, para todo $a, b \in \mathbb{Z}$.

e. Si $a \equiv 3 \pmod{5}$, hallar el resto de dividir $33a^3 + 3a^2 - 197a + 2$ por 5.

$$a \equiv b \pmod m \Rightarrow \begin{cases} \lambda a \equiv \lambda b \pmod m \\ a^n \equiv b^n \pmod m \end{cases}$$

d) $p(x) = \lambda_n x^n + \lambda_{n-1} x^{n-1} + \ldots + \lambda_1 x + \lambda_0 \quad \lambda_i \in \mathbb{Z}$

$a \equiv b \pmod m \Rightarrow p(a) \equiv p(b) \pmod m$

$a \equiv b \pmod m$

$a \equiv b \pmod m \Rightarrow a^n \equiv b^n \pmod m$

$\Rightarrow \lambda_n a^n \equiv \lambda_n b^n \pmod m$

$\lambda_n a^n + \lambda_{n-1} a^{n-1} + \ldots + \lambda_1 a + \lambda_0 \equiv \lambda_n b^n + \lambda_{n-1} b^{n-1} + \ldots \lambda_1 b + \lambda_0 \pmod m$

$a \equiv b \pmod m \Rightarrow a^i \equiv b^i \pmod m$ para $0 \leq i \leq n$

$\Rightarrow \lambda_i a^i \equiv \lambda_i b^i \pmod m$ porque $\lambda_i \in \mathbb{Z}$

entonces:

$\lambda_n a^n + \lambda_{n-1} a^{n-1} + \ldots + \lambda_1 a + \lambda_0 \equiv \lambda_n b^n + \lambda_{n-1} a^{n-1} + \ldots + \lambda_1 b + \lambda_0 \pmod m$

e) $a \equiv 3 \pmod 5$

buscamos el resto de dividir $33a^3 + 3a^2 - 197a + 2$ por 5

$\underbrace{33a^3 + 3a^2 - 197a + 2}_{p(a)} \equiv r \pmod 5$ con $0 \leq r \leq 4$

r: el resto

$p(x) = 33x^3 + 3x^2 - 197x + 2$

$p(a) \equiv p(3) \pmod 5$

$$P(a) \equiv 33 \cdot 3^3 + 3 \cdot 3^2 - 197 \cdot 3 + 2 \pmod 5$$
$$\equiv 3 \cdot 2 + 3 \cdot 4 - 2 \cdot 3 + 2 \pmod 5$$
$$\equiv 3 \cdot 4 + 2 \pmod 5$$
$$\equiv 14 \pmod 5$$
$$\equiv 4 \pmod 5$$

$P(a) \equiv 4 \pmod 5$ ↝ el resto es 4

$a \equiv b \pmod n$
$c \equiv d \pmod n$
$\Rightarrow ac \equiv bd \pmod n$

$$P(a) \equiv 33 \cdot 3^3 + 3 \cdot 3^2 - 197 \cdot 3 + 2 \pmod 5$$
$$\equiv \underbrace{33 \cdot 27}_{\equiv 3 \cdot 2 \pmod 5} + \underbrace{3 \cdot 9}_{\equiv 3 \cdot 4} - \underbrace{197 \cdot 3}_{\equiv 2 \cdot 3} + 2 \pmod 5$$
$$\equiv 3 \cdot 2 + 3 \cdot 4 - 2 \cdot 3 + 2 \pmod 5$$
$$\equiv 6 + 12 - 6 + 2 \pmod 5$$
$$\equiv 12 + 2 \pmod 5$$
$$\equiv 2 + 2 \pmod 5$$
$$\equiv 4 \pmod 5$$

$33 \cdot 27 \equiv 3 \cdot 2 \pmod 5$
$33 \equiv 3 \pmod 5$
$27 \equiv 2 \pmod 5$

$3 \cdot 9 \equiv 3 \cdot 4 \pmod 5$
$3 \equiv 3 \pmod 5$
$9 \equiv 4 \pmod 5$

Ejercicio 4.

a. Demostrar que $10^n \equiv (-1)^n \pmod{11}$, para todo $n \in \mathbb{N}$.

$a \equiv b \pmod m \Rightarrow a^n \equiv b^n \pmod m$

b. Enunciar y probar un criterio de divisibilidad entre 11. Sugerencia: expresar el número en base 10 y usar la parte anterior.

c. Hallar el dígito $d \in \{0, 1, \ldots, 9\}$, de modo que el número $2\mathbf{d}653874$ sea múltiplo de 11.

a) $10^n \equiv (-1)^n \pmod{11}$ para todo $n \in \mathbb{N}$

$10 \equiv -1 \pmod{11}$

↗ $10 - (-1) = 11$ divisible entre 11

↘ $10 \equiv 10 \pmod{11}$
$+ \; 0 \equiv -11 \pmod{11}$
$10 \equiv -1 \pmod{11}$

$10 \equiv -1 \pmod{11} \Rightarrow 10^n \equiv (-1)^n \pmod{11}$

b) $a \in \mathbb{N}$

$a = (a_k \cdots a_1 a_0)_{10}$

$a = a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_1 10 + a_0$

cuando es a divisible entre 11?

$11 \mid a \iff a \equiv 0 \pmod{11}$

$a \equiv a_k 10^k + a_{k-1} 10^{k-1} + \dots + \underbrace{a_2 10^2}_{\equiv a_2} + \underbrace{a_1 10}_{\equiv -a_1} + a_0 \pmod{11}$

$10^n \equiv (-1)^n \pmod{11}$

$10 \equiv -1 \pmod{11}$

$10^2 \equiv 1 \pmod{11}$

$\Rightarrow a_1 10 \equiv -a_1 \pmod{11}$

$a_2 10^2 \equiv a_2 \pmod{11}$

si i es par: $10^i \equiv (-1)^i \pmod{11}$

$10^i \equiv 1 \pmod{11}$

$a_i 10^i \equiv a_i \pmod{11}$

si i es impar: $10^i \equiv (-1)^i \pmod{11}$

$10^i \equiv -1 \pmod{11}$

$a_i 10^i \equiv -a_i \pmod{11}$

$a \equiv a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_2 10^2 + a_1 10 + a_0 \pmod{11}$

$\equiv \underbrace{(a_0 + a_2 + a_4 + \dots)}_{\text{suma de los dígitos en posición par}} - \underbrace{(a_1 + a_3 + a_5 + \dots)}_{\text{suma de los dígitos en posición impar}} \pmod{11}$

a divisible entre 11 $\iff a \equiv 0 \pmod{11}$

$\iff (a_0 + a_2 + \dots) - (a_1 + a_3 + \dots) \equiv 0 \pmod{11}$

$\iff$ la suma de los dígitos en posición par menos la suma de los dígitos en posición impar es múltiplo de 11

Ejercicio 4.

a. Demostrar que $10^n \equiv (-1)^n \pmod{11}$, para todo $n \in \mathbb{N}$.

b. Enunciar y probar un criterio de divisibilidad entre 11. Sugerencia: expresar el número en base 10 y usar la parte anterior.

c. Hallar el dígito $d \in \{0, 1, \ldots, 9\}$, de modo que el número $2\mathbf{d}653874$ sea múltiplo de 11.

buscamos $d \in \{0,1,\ldots,9\}$ tal que $2d653874$ sea multiplo de 11

$2d653874$ es multiplo de 11 $\Leftrightarrow$ $(4+8+5+d)-(7+3+6+2)$ es multiplo de 11

$\Leftrightarrow$ $17+d-18$ es multiplo de 11

$\Leftrightarrow$ $d-1$ es multiplo de 11

$\Leftrightarrow$ $d=1$ porque $d \in \{0,1,\ldots,9\}$

Ejercicio 7. Resolver cada una de las congruencias siguientes:

a. $3x \equiv 7 \pmod{16}$.

b. $2x + 8 \equiv 5 \pmod{33}$.

c. $3x+9 \equiv 8x+61 \pmod{64}$.

d. $6x - 1 \equiv 5 \pmod{12}$.

$6x \equiv 6 \pmod{12}$

a) $3x \equiv 7 \pmod{16}$ $\qquad x \equiv 1 \pmod{2}$

Forma 1 (con ecuaciones diofánticas)

$3x \equiv 7 \pmod{16} \Rightarrow 16 \mid 3x-7$

$\Rightarrow 3x-7 = 16q$ para algún $q \in \mathbb{Z}$

$\Rightarrow 3x-16q = 7$

Vamos a resolver $3x-16q=7$

* $\text{mcd}(3,16)=1 \Rightarrow \text{mcd}(3,16) \mid 7 \Rightarrow$ tiene solución
* solución particular?

$3(-5)-16(-1) = -15+16 = 1$

$3(-5)-16(-1) = 1$

$3(-5)\cdot 7 - 16(-1)\cdot 7 = 7$

solución particular: $\begin{cases} x = -35 \\ q = -7 \end{cases}$

* conjunto de soluciones:

$$3(-35 + \underbrace{16k}_{\mathbb{Z}}) - 16(-7 + \underbrace{3k}_{\mathbb{Z}}) = 7$$

$$\rightarrow x = -35 + 16k \quad k \in \mathbb{Z}$$
$$q = -7 + 3k \quad k \in \mathbb{Z}$$

$3x \equiv 7 \pmod{16} \Rightarrow x = -35 + 16k$ con $k \in \mathbb{Z}$

$\Rightarrow x - (-35) = 16k$

$\Rightarrow x \equiv -35 \pmod{16}$

$\Rightarrow x \equiv -35 + 16 \cdot 3 \pmod{16}$

$\Rightarrow \boxed{x \equiv 13 \pmod{16}}$

Forma 2: usando el inverso 3 modulo 16

$3x \equiv 7 \pmod{16}$

[3 es invertible modulo 16 si existe $y \in \mathbb{Z}$ tal que

$3y \equiv 1 \pmod{16}$]

$3x \equiv 7 \pmod{16} \Rightarrow \underbrace{y3x}_{\equiv 1 \pmod{16}} \equiv y7 \pmod{16}$

$\Rightarrow x \equiv y7 \pmod{16}$

como encontramos el inverso de 3 módulo 16?

identidad de Bezout para 3 y 16

$3(-5) - 16(-1) = 1$

$\boxed{3(-5) + 16 = 1}$ ← lo tenemos porque 3 y 16 son coprimos

$3(-5) = 1 - 16$

inverso de 3 módulo 16

$3(-5) \equiv 1 - \underbrace{16}_{\equiv 0 \pmod{16}} \pmod{16} \Rightarrow \overbrace{3(-5)}^{\text{inverso de 3 módulo 16}} \equiv 1 \pmod{16}$

$3x \equiv 7 \pmod{16} \Rightarrow \underbrace{3(-5)}_{\equiv 1 \pmod{16}} x \equiv 7(-5) \pmod{16}$

$\Rightarrow x \equiv 7(-5) \pmod{16}$

$\Rightarrow x \equiv -35 \pmod{16}$

$\Rightarrow \boxed{x \equiv 13 \pmod{16}}$

b) $2x + 8 \equiv 5 \pmod{33}$

$\Rightarrow 2x \equiv -3 \pmod{33}$

buscamos inverso de 2 modulo 33

el inverso existe porque 2 y 33 son coprimos

$33 + 2(-16) = 33 - 32 = 1$

$\boxed{33 + 2(-16) = 1}$ identidad de Bezout

$\Rightarrow 2(-16) = 1 - 33$

$\Rightarrow 2(-16) \equiv 1 - 33 \pmod{33}$

$\Rightarrow 2(-16) \equiv 1 \pmod{33}$

↑ es inverso de 2 modulo 33

$2x \equiv -3 \pmod{33} \Rightarrow \underbrace{2(-16)}_{\equiv 1 \pmod{33}} x \equiv -3(-16) \pmod{33}$

$\Rightarrow x \equiv 48 \pmod{33}$

$\Rightarrow \boxed{x \equiv 15 \pmod{33}}$

Ejercicio 3. [Pequeño Teorema de Fermat]

a. Probar que si a y b son enteros y p un número primo, entonces: $(a+b)^p \equiv a^p + b^p \pmod{p}$. Sugerencia: usar el teorema del binomio. ¿Vale el resultado si p no es primo?

b. Probar el denominado "pequeño Teorema de Fermat": $a^p \equiv a \pmod{p}$, para todo a entero y p primo. Sugerencia: usar inducción.

c. Calcular el resto de dividir 327^{101} entre 101.

a) a y b enteros, p primo $\Rightarrow (a+b)^p \equiv a^p + b^p \pmod{p}$

tenemos que ver que $p \mid (a+b)^p - (a^p + b^p)$

$$(a+b)^p - (a^p+b^p) = a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \dots + \binom{p}{p-1}ab^{p-1} + b^p - a^p - b^p$$

queremos ver que $p \mid \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \dots \binom{p}{p-1}ab^{p-1}$

veamos que $p \mid \binom{p}{i}$ con $1 \le i \le p-1$

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} \Rightarrow p! = \binom{p}{i} i!(p-i)!$$

$$\Rightarrow p \mid \binom{p}{i} i!(p-i)!$$

p no divide a $i!$

p no divide a $(p-i)!$

p es primo

$\Rightarrow p \mid \binom{p}{i}$

Entonces $p \mid (a+b)^p - (a^p + b^p)$

$\Rightarrow (a+b)^p \equiv a^p + b^p \pmod{p}$

b) pequeño teorema de Fermat:

$a^p \equiv a \pmod{p}$ para todo $a \in \mathbb{Z}$ y p primo

* vamos a probar por inducción que se cumple para $a \in \mathbb{N}$

- caso base: $a = 1$

$1^p \equiv 1 \pmod{p}$ ✓

- paso inductivo: $\boxed{(a+b)^p \equiv a^p + b^p \pmod p}$

  suponemos que $a^p \equiv a \pmod p$

  queremos probar que $(a+1)^p \equiv a+1 \pmod p$

$$\begin{aligned}(a+1)^p &\equiv a^p + 1^p \pmod p \\ &\equiv a + 1^p \pmod p \quad \text{por HI} \\ &\equiv a+1 \pmod p\end{aligned}$$