RESUMEN ALGEBRA 1

FINAL

NUMEROS ENTEROS (PARTE 2)

Enteros – Segunda parte.

5.1 Ecuaciones lineales diofánticas.

Proposición 5.1.2. **(Ecuación diofántica y máximo común divisor.)**
Sean $a, b, c \in \mathbb{Z}$ *con* a, b *no nulos. La ecuación diofántica*

$$aX + bY = c$$

admite soluciones enteras si y solo si $(a : b) \mid c$. *Es decir:*

$$\exists\, (x_0, y_0) \in \mathbb{Z}^2 : \; a x_0 + b y_0 = c \iff (a : b) \mid c.$$

Corolario 5.1.3. **(Ecuación diofántica con a y b coprimos.)**
Sean $a, b \in \mathbb{Z}$ *no nulos y* coprimos. *Entonces la ecuación diofántica*

$$aX + bY = c$$

tiene soluciones enteras, para todo $c \in \mathbb{Z}$.

Observación 5.1.5. **(Ecuación diofántica y ecuación "coprimizada".)**
Sean $a, b, c \in \mathbb{Z}$ con a, b no nulos tales que $(a : b) \mid c$.
Definamos $a' = \dfrac{a}{(a : b)}$, $b' = \dfrac{b}{(a : b)}$ y $c' = \dfrac{c}{(a : b)}$. Entonces,

$$a \cdot X + b \cdot Y = c \;\rightsquigarrow\; a' \cdot X + b' \cdot Y = c'.$$

Proposición 5.1.6. **(La ecuación diofántica $a \cdot X + b \cdot Y = 0$.)**
Sean $a, b \in \mathbb{Z}$, *no nulos.*
El conjunto $\mathcal{S}_0$ *de soluciones enteras de la ecuación diofántica* $a \cdot X + b \cdot Y = 0$ *es*

$$\mathcal{S}_0 = \{\, (x, y) : x = b'k,\ y = -a'k,\ k \in \mathbb{Z} \,\},\ \textit{donde}\ a' := \frac{a}{(a : b)}\ y\ b' := \frac{b'}{(a : b)}.$$

Teorema 5.1.7. **(La ecuación diofántica $a \cdot X + b \cdot Y = c$.)**

Sean $a, b, c \in \mathbb{Z}$, con a, b no nulos.

El conjunto $\mathcal{S}$ de soluciones enteras de la ecuación diofántica $a \cdot X + b \cdot Y = c$ es:

- $\mathcal{S} = \emptyset$ *cuando* $(a : b) \nmid c$.
- $\mathcal{S} = \{ (x, y) : x = x_0 + b'k, y = y_0 - a'k;\ k \in \mathbb{Z} \}$, *donde* (x_0, y_0) *es una solución particular cualquiera de la ecuación y* $a' := \dfrac{a}{(a : b)}$, $b' := \dfrac{b}{(a : b)}$ *cuando* $(a : b) \mid c$.

Resolución completa de la ecuación diofántica $aX + bY = c$

1. ¿ Tiene solución la ecuación ?
   (a) **no** cuando $(a : b) \nmid c$. En ese caso $\mathcal{S} = \emptyset$.
   (b) **sí** cuando $(a : b) \mid c$. En ese caso:
2. "Coprimizo" la ecuación:

$$a'X + b'Y = c', \quad \text{con } a' := \frac{a}{(a : b)},\ b' := \frac{b}{(a : b)} \ \text{ y } \ c' := \frac{c}{(a : b)}.$$

3. Busco una solución particular $(x_0, y_0) \in \mathbb{Z}^2$ (a ojo o aplicando el algoritmo de Euclides).
4. Todas las soluciones son:

$$\mathcal{S} = \{ (x, y) : x = x_0 + b'k,\ y = y_0 - a'k;\ k \in \mathbb{Z} \}.$$

5.2 Ecuaciones lineales de congruencia.

Proposición 5.2.2. **(Ecuación de congruencia, mcd y ecuación "coprimizada".)**

Sea $m \in \mathbb{N}$. Dados $a, c \in \mathbb{Z}$, la ecuación de congruencia $aX \equiv c \pmod m$ tiene soluciones enteras si y solo si $(a : m) \mid c$.

Si ese es el caso, sean $a' := \dfrac{a}{(a : m)}$, $c' := \dfrac{c}{(a : m)}$ y $m' := \dfrac{m}{(a : m)}$. Entonces

$$aX \equiv c \pmod m \iff a'X \equiv c' \pmod{m'}.$$

Observación 5.2.3. **(Simplificando factores comunes en ecuación de congruencia-I.)**

Sean $m' \in \mathbb{N}$ y $a', c', d \in \mathbb{Z}$ no nulos. Entonces,

$$\forall x \in \mathbb{Z}, \quad (d\,a')\,x \equiv d\,c' \pmod{(d\,m')} \iff a'\,x \equiv c' \pmod{m'}.$$

Corolario 5.2.4. **(Ecuación de congruencia con a y m coprimos.)**

Sean $m \in \mathbb{N}$ y $a \in \mathbb{Z}$ tal que a y m son coprimos. *Entonces, la ecuación de congruencia $a\,X \equiv c \pmod{m}$ tiene soluciones enteras, cualquiera sea $c \in \mathbb{Z}$.*

Teorema 5.2.5. **(La ecuación de congruencia $a\,X \equiv c \pmod{m}$.)**

Sea $m \in \mathbb{N}$ y sean $a, c \in \mathbb{Z}$ con $a \neq 0$.

El conjunto $\mathcal{S}$ de soluciones enteras de la ecuación de congruencia

$$a\,X \equiv c \pmod{m}$$

es

- $\mathcal{S} = \emptyset$, *cuando* $(a : m) \nmid c$.
- $\mathcal{S} = \{x \in \mathbb{Z} : \ x \equiv x_0 \pmod{m'}\}$ *donde* $x_0 \in \mathbb{Z}$ *es una solución particular cualquiera de la ecuación* $a\,X \equiv c \pmod{m}$ *o de la ecuación equivalente* $a'\,X \equiv c' \pmod{m'}$ *donde* $a' = \dfrac{a}{(a : m)}$, $c' = \dfrac{c}{(a : m)}$ *y* $m' = \dfrac{m}{(a : m)}$, *cuando* $(a : m) \mid c$, *ya que*

  $$a\,X \equiv c \pmod{m} \quad \rightsquigarrow \quad X \equiv x_0 \pmod{m'}.$$

  Más aún, existe una única solución $x_0 \in \mathbb{Z}$ que satisface $0 \leq x_0 < m'$.

Observación 5.2.6. **(Simplificando factores comunes en ecuación de congruencia-II.)**

Sean $m \in \mathbb{N}$ y $a, c, d \in \mathbb{Z}$, con a, d no nulos.

Si d y m son *coprimos*, entonces se tiene la siguiente equivalencia de ecuaciones de congruencia:

$$(d\,a)\,X \equiv d\,c \pmod{m} \quad \rightsquigarrow \quad a\,X \equiv c \pmod{m}.$$

Resolución completa de la ecuación de congruencia $aX \equiv c \pmod{m}$

1. Antes que nada reemplazo, si es necesario, a por $r_m(a)$ y c por $r_m(c)$ sin cambiar las soluciones, ya que $a \equiv r_m(a) \pmod{m}$ y $c \equiv r_m(c) \pmod{m}$, o por algún otro número conveniente que sea congruente, por ejemplo -1. Así, de entrada se tiene que los coeficientes de la ecuación de congruencia son los más simples posibles.

2. ¿ Tiene solución la ecuación ?

   (a) **no** si $(a : m) \nmid c$.

   (b) **sí** si $(a : m) \mid c$. En ese caso:

3. "Coprimizo" la ecuación:

$$a'X \equiv c' \pmod{m'}, \quad \text{con } a' := \frac{a}{(a:m)},\ c' := \frac{c}{(a:m)} \text{ y } m' := \frac{m}{(a:m)}.$$

4. Si es necesario, ahora que $a' \perp m'$, simplifico todos los factores comunes entre a' y c' aplicando la Observación 5.2.6. Esto me simplifica la búsqueda de la solución particular.

5. Busco una solución particular $x_0 \in \mathbb{Z}$ que satisface que $a'x_0 \equiv c' \pmod{m'}$ (a ojo o encontrando una solución particular de la ecuación diofántica $a'X - m'Y = c'$ asociada).

6. Se concluye que

$$aX \equiv c \pmod{m} \quad \rightsquigarrow \quad X \equiv x_0 \pmod{m'}.$$

O sea, el conjunto de soluciones de la ecuación de congruencia es el conjunto

$$\mathcal{S} = \{\, x \in \mathbb{Z} :\ x \equiv x_0 \pmod{m'} \,\}.$$

5.3 Teorema chino del resto (TCR).

Proposición 5.3.1. (Sistemas equivalentes.)

1. *Sean* $m_1, \ldots, m_n \in \mathbb{N}$ coprimos dos a dos, *es decir* $m_i \perp m_j$ *para* $i \neq j$. *Entonces,* $\forall\, c \in \mathbb{Z}$,

$$\begin{cases} X \equiv c \pmod{m_1} \\ X \equiv c \pmod{m_2} \\ \quad\vdots \\ X \equiv c \pmod{m_n} \end{cases} \rightsquigarrow \quad X \equiv c \pmod{m_1 \cdot m_2 \cdots m_n}.$$

2. *Sean* $m, m' \in \mathbb{N}$ *tales que* $m' \mid m$. *Entonces,* $\forall\, c, c' \in \mathbb{Z}$,

- *Si* $c \not\equiv c' \pmod{m'}$, $\begin{cases} X \equiv c' \pmod{m'} \\ X \equiv c \pmod{m} \end{cases}$ *es incompatible,*

- *Si* $c \equiv c' \pmod{m'}$, $\begin{cases} X \equiv c' \pmod{m'} \\ X \equiv c \pmod{m} \end{cases} \rightsquigarrow X \equiv c \pmod{m}.$

Teorema 5.3.2. **(Teorema chino del resto.)**

Sean $m_1, \dots, m_n \in \mathbb{N}$ coprimos dos a dos, *es decir* $m_i \perp m_j$ *para* $i \neq j$. *Entonces,* $\forall\, c_1, \dots, c_n \in \mathbb{Z}$, *el sistema de ecuaciones de congruencia*

$$\begin{cases} X \equiv c_1 \pmod{m_1} \\ \quad \vdots \\ X \equiv c_n \pmod{m_n} \end{cases}$$

tiene soluciones enteras.
Más aún,

$$\begin{cases} X \equiv c_1 \pmod{m_1} \\ \quad \vdots \\ X \equiv c_n \pmod{m_n} \end{cases} \quad \leftrightsquigarrow \quad X \equiv x_0 \pmod{m_1 \cdots m_n}\ ,$$

donde $x_0 \in \mathbb{Z}$ *es una solución particular cualquiera del sistema, y se tiene*

$$\mathcal{S} = \{x \in \mathbb{Z} :\ x \equiv x_0 \pmod{m_1 \cdots m_n}\}.$$

En particular, existe una única solución $x_0 \in \mathbb{Z}$ *que satisface* $0 \leq x_0 < m_1 \cdots m_n$.

5.4 El Pequeño Teorema de Fermat (PTF)

Teorema 5.4.1. **(Pequeño Teorema de Fermat - PTF.)**

Sea p *un* primo *positivo. Entonces,* $\forall\, a \in \mathbb{Z}$,

1. $a^p \equiv a \pmod{p}$
2. $p \nmid a \implies a^{p-1} \equiv 1 \pmod{p}$

Observación 5.4.2.

El teorema es falso en general si p no es primo: por ejemplo $3^4 = 81 \not\equiv 3 \pmod 4$. Sin embargo existen números n no primos para los cuales vale el enunciado del PTF: $a^n \equiv a \pmod{n}$ para todo $a \in \mathbb{Z}$.

Corolario 5.4.4. **(Congruencia y potencias.)**

Sea p *un primo positivo. Entonces* $\forall\, a \in \mathbb{Z}$ tal que $p \nmid a$ *y* $n \in \mathbb{N}$, *se tiene*

$$n \equiv r \pmod{(p-1)} \implies a^n \equiv a^r \pmod{p}.$$

En particular,

$$p \nmid a \implies a^n \equiv a^{r_{p-1}(n)} \pmod{p}.$$

Proposición 5.5.1. **(PTF para pq.)**

Sean p, q dos primos positivos distintos, y sea $a \in \mathbb{Z}$ coprimo con pq. Entonces

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

Y por lo tanto, $\forall m \in \mathbb{N}$,

$$m \equiv r \left(\mathrm{mod}\,(p-1)(q-1)\right) \implies a^m \equiv a^r \pmod{pq}.$$

Observación 5.5.2. **(Propiedad clave por la cual funciona el algoritmo RSA.)**

Sean $n = p \cdot q$, d, e como arriba. Sea $a \in \mathbb{N}$ con $1 \leq a < n$. Entonces

$$a^{ed} \equiv a \pmod{n}.$$

5.6 El anillo $\mathbb{Z}/m\mathbb{Z}$ y el cuerpo $\mathbb{Z}/p\mathbb{Z}$.

5.6.1 El anillo $\mathbb{Z}/m\mathbb{Z}$.

Teorema 5.6.1. **(El anillo $\mathbb{Z}/m\mathbb{Z}$.)**

Sea $m \in \mathbb{N}$ y consideremos en $\mathbb{Z}$ la relación de equivalencia congruencia módulo m. *Entonces*

1. *Sea $0 \leq r < m$. La clase de equivalencia $\overline{r}$ de r es*

$$\overline{r} = \{a \in \mathbb{Z} : \ a \equiv r \pmod{m}\}$$

y

$$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \cdots \cup \overline{m-1}$$

es la partición de $\mathbb{Z}$ asociada a esta relación de equivalencia.

2. *Notemos*

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\},$$

y sean $+$ y $\cdot$ las operaciones en $\mathbb{Z}/m\mathbb{Z}$ definidas por

$$\overline{r}_1 + \overline{r}_2 = \overline{r_1 + r_2} \quad \text{y} \quad \overline{r}_1 \cdot \overline{r}_2 = \overline{r_1 \cdot r_2}, \quad \text{para } 0 \leq r_1, r_2 < m.$$

Entonces $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ es un anillo conmutativo.

5.6.2 El cuerpo $\mathbb{Z}/p\mathbb{Z}$.

Proposición 5.6.2. **(La ecuación de congruencia $a \cdot X \equiv 1 \pmod{m}$.)**

Sea $m \in \mathbb{N}$ y sea $a \in \mathbb{Z}$. Entonces la ecuación de congruencia $a \cdot X \equiv 1 \pmod{m}$ tiene soluciones si y solo si $a \perp m$. En ese caso, hay una única solución x_0 con $1 \leq x_0 < m$.

Corolario 5.6.3. **(La ecuación de congruencia $a \cdot X \equiv 1 \pmod{p}$.)**

Sea p un primo positivo y sea $a \in \mathbb{N}$ tal que $p \nmid a$. Entonces la ecuación de congruencia $a \cdot X \equiv 1 \pmod{p}$ tiene una única solución x_0 con $1 \leq x_0 < p$.

Corolario 5.6.4. **(Los elementos inversibles de $\mathbb{Z}/m\mathbb{Z}$.)**

Sea $m \in \mathbb{N}$, y sea $\overline{r} \in \mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$.

Entonces, $\overline{r}$ es inversible en $\mathbb{Z}/m\mathbb{Z}$ si y solo si $r \perp m$.

Teorema 5.6.5. **($\mathbb{Z}/p\mathbb{Z}$ es un cuerpo.)**

Sea p un primo positivo. Entonces $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ es un cuerpo.

Es decir, además de ser un anillo conmutativo con la suma y el producto definidos en el Teorema 5.6.1, se satisface que todo elemento no nulo de $\mathbb{Z}/p\mathbb{Z}$ es inversible.

EJERCICIOS DE PARCIAL

13/8/22

3. Hallar todos los $a, b \in \mathbb{N}$ que verifican simuitáneamente:

- $12a - 7b = 5$,
- $2^b \equiv a \ (13)$.

20/7/22

3. Para cada $k \in \mathbb{N}$, hallar el resto de

$$2^{3^{k!}}$$

en la división por 23.

27/7/22

2. Hallar todos los $a, b \in \mathbb{Z}$ que verifican simultáneamente:

- $16a + 22b = 162$,
- $a - 2b$ tiene exactamente 5 divisores positivos.

17/6/22

2. Pruebe que si a es impar y $7 \nmid a$, entonces $(3a^4 - a^3 : a + 7) \in \{2, 22\}$.

27/5/22

2. Encuentre todos los $a \in \mathbb{Z}$ tales que

$$3a \equiv 7 \pmod{23} \quad y \quad (2a + 5 : 13a - 2) \neq 1.$$

29/4/22

2. Encuentre todos los $a \in \mathbb{Z}$ tales que

$$\frac{3a^{18}}{5} - \frac{5a^{86}}{43} + \frac{12a}{215} \in \mathbb{Z}.$$

4/3/22

2. Determinar todos los valores de $n \in \mathbb{N}$ para los cuales $n^{1021} \equiv 22 \pmod{55}$ y $5 \mid n2^n - 3n^5$.

25/2/22

3. Hallar el menor número natural a que satisface

$$\begin{cases} 3 \cdot 7^{15} a \equiv -15 \pmod{36}, \\ (a : 425) = 5. \end{cases}$$

18/2/22

2. Determinar todos los primos $p \in \mathbb{N}$ para los cuales la ecuación de congruencia

$$pX \equiv 2 \cdot 3^{p^2+4} \pmod{35p^2}$$

tiene solución y para cada primo hallado, resolverla.

22/12/21

Ejercicio 2

Sea $a \in \mathbb{Z}$ tal que $a \equiv 2 \pmod{28}$. Clasificar los valores que toma

$$(3a + 196^n : 2a - 196^n)$$

según los distintos valores de a, descritos en la forma $a \equiv r \pmod{m}$ para $r, m \in \mathbb{N}$ adecuados, y de $n \in \mathbb{N}$.

10/12/21

2. Determinar los posibles restos al dividir por 252 de todos los $a \in \mathbb{Z}$ que satisfacen que

$$(a^{225} + 10a + 1 : 252) = 14.$$

21/10/21

3. Determinar todos los $a, b \in \mathbb{N}$ que satisfacen simutáneamente que

$$(a : b) = -2a + b \quad \text{y} \quad [a : b] = 83a.$$