Máximo común divisor, parte 1

Algebra Superior 2

Facultad de Ciencias, UNAM

marzo de 2020

Definiciones I y II

Antes de la contingencia habíamos visto tres formas de ver al máximo común divisor, dos de ellas eran definiciones:

Definiciones I y II

Antes de la contingencia habíamos visto tres formas de ver al máximo común divisor, dos de ellas eran definiciones:

Definición (I)

Sean $a, b \in \mathbb{Z}$ *con* $a \neq 0$ *o* $b \neq 0$. *Definimos* $mcd(a, b) = máx\big[D(a) \cap D(b)\big]$.

Definiciones I y II

Antes de la contingencia habíamos visto tres formas de ver al máximo común divisor, dos de ellas eran definiciones:

Definición (I)

Sean $a, b \in \mathbb{Z}$ *con* $a \neq 0$ *o* $b \neq 0$*. Definimos* $mcd(a,b) = máx\big[D(a) \cap D(b)\big]$.

Definición (II)

Sean $a, b, d \in \mathbb{Z}$ *con* $a \neq 0$ *o* $b \neq 0$*. Decimos que* $d = mcd(a,b)$ *si se cumplen las siguientes condiciones:*
(i) $d|a$ *y* $d|b$
(ii) $\forall d' \in \mathbb{Z}$ *se tiene:*

$$d'|a \text{ y } d'|b \;\Rightarrow\; d' \leq d.$$

El Teorema III

La tercera forma de ver al máximo común divisor la vimos en un teorema, el sábado antes de la contingencia:

El Teorema III

La tercera forma de ver al máximo común divisor la vimos en un teorema, el sábado antes de la contingencia:

Teorema (III)

Sean $a, b, d \in \mathbb{Z}$ *con* $a \neq 0$ *o* $b \neq 0$*. Si* d *es la mínima combinación lineal positiva de* a *y* b*, entonces* $d = mcd(a, b)$

El Teorema III

La tercera forma de ver al máximo común divisor la vimos en un teorema, el sábado antes de la contingencia:

Teorema (III)

Sean $a, b, d \in \mathbb{Z}$ *con* $a \neq 0$ *o* $b \neq 0$*. Si* d *es la mínima combinación lineal positiva de* a *y* b*, entonces* $d = mcd(a, b)$

Lo que ya no vimos fue la definición de *primos relativos*, que veremos a continuación:

Los primos relativos

Definición

Sean $a, b, d \in \mathbb{Z}$ *con* $a \neq 0$ *o* $b \neq 0$. *Decimos que* a *y* b *son primos relativos si* $mcd(a, b) = 1$.

Los primos relativos

Definición

Sean $a, b, d \in \mathbb{Z}$ *con* $a \neq 0$ *o* $b \neq 0$. *Decimos que a y b son primos relativos si* $mcd(a, b) = 1$.

En principio esta definición **no** tiene que ver con el hecho de que a o b sean primos. Por ejemplo, 8 y 9 son primos relativos, ya que $mcd(8, 9) = 1$. Nota que 8 **no** es primo y 9 tampoco lo es.

Los primos relativos

Definición

Sean $a, b, d \in \mathbb{Z}$ *con* $a \neq 0$ *o* $b \neq 0$*. Decimos que* a *y* b *son primos relativos si* $mcd(a, b) = 1$*.*

En principio esta definición **no** tiene que ver con el hecho de que a o b sean primos. Por ejemplo, 8 y 9 son primos relativos, ya que $mcd(8, 9) = 1$. Nota que 8 **no** es primo y 9 tampoco lo es.

Más ejemplos:

Los primos relativos

Definición

Sean $a, b, d \in \mathbb{Z}$ *con* $a \neq 0$ *o* $b \neq 0$. *Decimos que* a *y* b *son primos relativos si* $mcd(a, b) = 1$.

En principio esta definición **no** tiene que ver con el hecho de que a o b sean primos. Por ejemplo, 8 y 9 son primos relativos, ya que $mcd(8, 9) = 1$. Nota que 8 **no** es primo y 9 tampoco lo es.

Más ejemplos:

(i) -10 y 21 son primos relativos, pues $mcd(-10, 21) = 1$,

Los primos relativos

Definición

Sean $a, b, d \in \mathbb{Z}$ con $a \neq 0$ o $b \neq 0$. Decimos que a y b son primos relativos si $mcd(a, b) = 1$.

En principio esta definición **no** tiene que ver con el hecho de que *a* o *b* sean primos. Por ejemplo, 8 y 9 son primos relativos, ya que $mcd(8, 9) = 1$. Nota que 8 **no** es primo y 9 tampoco lo es.

Más ejemplos:

(i) -10 y 21 son primos relativos, pues $mcd(-10, 21) = 1$,

(ii) -14 y 21 **no** son primos relativos, pues $mcd(-14, 21) = 7 \neq 1$,

Los primos relativos

Definición

Sean $a, b, d \in \mathbb{Z}$ *con* $a \neq 0$ *o* $b \neq 0$*. Decimos que* a *y* b *son primos relativos si* $mcd(a, b) = 1$*.*

En principio esta definición **no** tiene que ver con el hecho de que a o b sean primos. Por ejemplo, 8 y 9 son primos relativos, ya que $mcd(8, 9) = 1$. Nota que 8 **no** es primo y 9 tampoco lo es.

Más ejemplos:

(i) -10 y 21 son primos relativos, pues $mcd(-10, 21) = 1$,

(ii) -14 y 21 **no** son primos relativos, pues $mcd(-14, 21) = 7 \neq 1$,

(iii) -25 y 21 son primos relativos, pues $mcd(-25, 21) = 1$.

Los primos relativos

Pregunta

¿Existe $b \in \mathbb{Z}$ *tal que* 0 *y* b *sean primos relativos? ¿Qué posibilidades podría tener* b*?*

Los primos relativos

Pregunta

¿Existe $b \in \mathbb{Z}$ *tal que* 0 *y* b *sean primos relativos? ¿Qué posibilidades podría tener* b*?*

Por favor piénsalo...

Los primos relativos

Pregunta

¿Existe $b \in \mathbb{Z}$ *tal que* 0 *y* b *sean primos relativos? ¿Qué posibilidades podría tener* b*?*

Por favor piénsalo...

Recuerda ahora lo que decía el Teorema III. Veremos cómo usarlo para probar algunos resultados relacionados con primos relativos.

Usando el Teorema III

Considera primero la siguiente pregunta:

Usando el Teorema III

Considera primero la siguiente pregunta:

Pregunta (2)

Si $a|bc$, *es cierto que entonces* $a|b$ *o* $a|c$*?*

Usando el Teorema III

Considera primero la siguiente pregunta:

Pregunta (2)

Si $a|bc$, es cierto que entonces $a|b$ o $a|c$?

Piénsalo un momento...

Usando el Teorema III

Tal vez hayas visto que la respuesta es: no. Por ejemplo, si $a = 4$, $b = 2 = c$, entonces se tiene que $a|bc$, pero a no divide a b ni a c.

Usando el Teorema III

Tal vez hayas visto que la respuesta es: no. Por ejemplo, si $a = 4$, $b = 2 = c$, entonces se tiene que $a|bc$, pero a no divide a b ni a c.

Por cierto, busca tú tres ejemplos más que muestren que la respuesta a la Pregunta (2) es negativa.

Usando el Teorema III

Tal vez hayas visto que la respuesta es: no. Por ejemplo, si $a = 4$, $b = 2 = c$, entonces se tiene que $a|bc$, pero a no divide a b ni a c.

Por cierto, busca tú tres ejemplos más que muestren que la respuesta a la Pregunta (2) es negativa.

Ahora observa otra cosa: si $a = 4$ y $b = 2 = c$, entonces a y b no son primos relativos (a y c tampoco lo son).

Tal vez hayas visto que la respuesta es: no. Por ejemplo, si $a = 4$, $b = 2 = c$, entonces se tiene que $a|bc$, pero a no divide a b ni a c.

Por cierto, busca tú tres ejemplos más que muestren que la respuesta a la Pregunta (2) es negativa.

Ahora observa otra cosa: si $a = 4$ y $b = 2 = c$, entonces a y b no son primos relativos (a y c tampoco lo son).

Resulta que si se pide una condición de primos relativos, entonces ¡la respuesta a la Pregunta (2) es afirmativa! Y lo probaremos en el siguiente lema.

El Lema(*)

Lema (*)

Sean $a, b, c \in \mathbb{Z}$ *con* $a \neq 0$ *o* $b \neq 0$. *Si* $a|bc$ *y* $mcd(a, b) = 1$, *entonces* $a|c$.

El Lema(*)

Lema (*)

Sean $a, b, c \in \mathbb{Z}$ *con* $a \neq 0$ *o* $b \neq 0$. *Si* $a|bc$ *y* $mcd(a, b) = 1$, *entonces* $a|c$.

Demostración: Tenemos dos hipótesis. Por un lado $a|bc$, así que existe $k \in \mathbb{Z}$ tal que

$$ak = bc. \tag{1}$$

El Lema(*)

Lema (*)

Sean $a, b, c \in \mathbb{Z}$ *con* $a \neq 0$ *o* $b \neq 0$. *Si* $a|bc$ *y* $mcd(a, b) = 1$, *entonces* $a|c$.

Demostración: Tenemos dos hipótesis. Por un lado $a|bc$, así que existe $k \in \mathbb{Z}$ tal que

$$ak = bc. \tag{1}$$

La segunda hipótesis que tenemos es que $mcd(a, b) = 1$. Podríamos usar la Definición I o la Definición II para usar esta hipótesis, pero nos conviene **mucho** más usar el Teorema III. Veamos:

El Lema(*)

Lema (*)

Sean $a, b, c \in \mathbb{Z}$ con $a \neq 0$ o $b \neq 0$. Si $a|bc$ y $mcd(a, b) = 1$, entonces $a|c$.

Demostración: Tenemos dos hipótesis. Por un lado $a|bc$, así que existe $k \in \mathbb{Z}$ tal que

$$ak = bc. \tag{1}$$

La segunda hipótesis que tenemos es que $mcd(a, b) = 1$. Podríamos usar la Definición I o la Definición II para usar esta hipótesis, pero nos conviene **mucho** más usar el Teorema III. Veamos:

El Teorema III dice varias cosas, entre ellas que 1 es combinación lineal de a y b. En otras palabras, existen $\alpha, \beta \in \mathbb{Z}$ tales que

$$1 = \alpha a + \beta b.$$

Prueba del Lema(*)

De esta manera,

$$\begin{aligned} c &= (\alpha a + \beta b)c \qquad (2) \\ &= \alpha ac + \beta bc. \qquad (3) \end{aligned}$$

Prueba del Lema(*)

De esta manera,

$$\begin{aligned} c &= (\alpha a + \beta b)c && (2) \\ &= \alpha ac + \beta bc. && (3) \end{aligned}$$

Usando la ecuación (1) obtenemos que

$$\begin{aligned} c &= \alpha ac + \beta ak && (4) \\ &= a(\alpha c + \beta k). && (5) \end{aligned}$$

Prueba del Lema(*)

De esta manera,

$$
\begin{aligned}
c &= (\alpha a + \beta b)c && (2)\\
&= \alpha ac + \beta bc. && (3)
\end{aligned}
$$

Usando la ecuación (1) obtenemos que

$$
\begin{aligned}
c &= \alpha ac + \beta ak && (4)\\
&= a(\alpha c + \beta k). && (5)
\end{aligned}
$$

Por lo tanto, $a|c$. $\square$

El Lema(**)

Veamos otro lema.

El Lema(**)

Veamos otro lema.

Lema (**)

Sean $a, b, c \in \mathbb{Z} \setminus \{0\}$. *Si* $mcd(a, c) = 1 = mcd(b, c)$, *entonces* $mcd(ab, c) = 1$.

El Lema(**)

Veamos otro lema.

Lema (**)

Sean $a, b, c \in \mathbb{Z} \setminus \{0\}$. *Si* $mcd(a, c) = 1 = mcd(b, c)$, *entonces* $mcd(ab, c) = 1$.

Demostración: Aplicando el Teorema III a nuestra primera hipótesis obtenemos que existen $\alpha, \beta \in \mathbb{Z}$ tales que

$$1 = \alpha a + \beta c. \tag{6}$$

El Lema(**)

Veamos otro lema.

Lema (**)

Sean $a, b, c \in \mathbb{Z} \setminus \{0\}$. *Si* $mcd(a, c) = 1 = mcd(b, c)$, *entonces* $mcd(ab, c) = 1$.

Demostración: Aplicando el Teorema III a nuestra primera hipótesis obtenemos que existen $\alpha, \beta \in \mathbb{Z}$ tales que

$$1 = \alpha a + \beta c. \tag{6}$$

Si ahora aplicamos el Teorema III a nuestra segunda hipótesis resulta que existen $\gamma, \eta \in \mathbb{Z}$ tales que

$$1 = \gamma b + \eta c. \tag{7}$$

El Lema(**)

Veamos otro lema.

Lema (**)

Sean $a, b, c \in \mathbb{Z} \setminus \{0\}$. *Si* $mcd(a, c) = 1 = mcd(b, c)$, *entonces* $mcd(ab, c) = 1$.

Demostración: Aplicando el Teorema III a nuestra primera hipótesis obtenemos que existen $\alpha, \beta \in \mathbb{Z}$ tales que

$$1 = \alpha a + \beta c. \tag{6}$$

Si ahora aplicamos el Teorema III a nuestra segunda hipótesis resulta que existen $\gamma, \eta \in \mathbb{Z}$ tales que

$$1 = \gamma b + \eta c. \tag{7}$$

Queremos probar que $mcd(ab, c) = 1$, así que sería bueno que escribiéramos a 1 como combinación lineal de ab y c.

El Lema(**)

Veamos otro lema.

Lema (**)

Sean $a, b, c \in \mathbb{Z} \setminus \{0\}$. *Si* $mcd(a, c) = 1 = mcd(b, c)$, *entonces* $mcd(ab, c) = 1$.

Demostración: Aplicando el Teorema III a nuestra primera hipótesis obtenemos que existen $\alpha, \beta \in \mathbb{Z}$ tales que

$$1 = \alpha a + \beta c. \tag{6}$$

Si ahora aplicamos el Teorema III a nuestra segunda hipótesis resulta que existen $\gamma, \eta \in \mathbb{Z}$ tales que

$$1 = \gamma b + \eta c. \tag{7}$$

Queremos probar que $mcd(ab, c) = 1$, así que sería bueno que escribiéramos a 1 como combinación lineal de ab y c.
Para eso podemos usar (6) y (7). Multiplicando deducimos que:

Prueba del Lema(**)

$$\begin{aligned}
1 &= (\alpha a + \beta c)(\gamma b + \eta c) && (8)\\
&= \alpha a \gamma b + \alpha a \eta c + \beta c \gamma b + \beta c \eta c && (9)\\
&= (\alpha\gamma) ab + (\alpha a \eta + \beta \gamma b + \beta c \eta) c && (10)
\end{aligned}$$

Prueba del Lema(**)

$$
\begin{aligned}
1 &= (\alpha a + \beta c)(\gamma b + \eta c) && (8)\\
&= \alpha a \gamma b + \alpha a \eta c + \beta c \gamma b + \beta c \eta c && (9)\\
&= (\alpha\gamma) ab + (\alpha a \eta + \beta \gamma b + \beta c \eta) c && (10)
\end{aligned}
$$

Así, hemos visto que 1 en efecto es combinación lineal de ab y c.

Prueba del Lema(**)

$$
\begin{aligned}
1 &= (\alpha a + \beta c)(\gamma b + \eta c) && (8)\\
&= \alpha a \gamma b + \alpha a \eta c + \beta c \gamma b + \beta c \eta c && (9)\\
&= (\alpha\gamma) ab + (\alpha a \eta + \beta \gamma b + \beta c \eta) c && (10)
\end{aligned}
$$

Así, hemos visto que 1 en efecto es combinación lineal de ab y c.

Notemos que no hay números enteros positivos menores que 1, así que 1 es la combinación lineal más pequeña positiva de ab y c.

Prueba del Lema(**)

$$
\begin{aligned}
1 &= (\alpha a + \beta c)(\gamma b + \eta c) && (8)\\
&= \alpha a \gamma b + \alpha a \eta c + \beta c \gamma b + \beta c \eta c && (9)\\
&= (\alpha\gamma) ab + (\alpha a \eta + \beta \gamma b + \beta c \eta) c && (10)
\end{aligned}
$$

Así, hemos visto que 1 en efecto es combinación lineal de ab y c.

Notemos que no hay números enteros positivos menores que 1, así que 1 es la combinación lineal más pequeña positiva de ab y c.

En consecuencia, por el Teorema III, podemos concluir que $mcd(ab, c) = 1$. $\square$

Otra pregunta

Es momento de considerar otra pregunta:

Pregunta

Si $a|c$ *y* $b|c$, *¿es cierto que* $ab|c$*?*

Otra pregunta

Es momento de considerar otra pregunta:

Pregunta

Si $a|c$ y $b|c$, ¿es cierto que $ab|c$?

Piénsalo un momento...

Un comentario

Tal vez hayas notado que la respuesta a esta pregunta es negativa (¡busca tres ejemplos distintos!).

Un comentario

Tal vez hayas notado que la respuesta a esta pregunta es negativa (¡busca tres ejemplos distintos!).

Una vez más, la respuesta a la pregunta se vuelve afirmativa si añadimos una hipótesis sobre primos relativos, y lo probaremos en el siguiente lema.

El Lema(***)

Lema (***)

Sean $a, b, c \in \mathbb{Z}$ *con* $a \neq 0$ *o* $b \neq 0$. *Si* $a|c$, $b|c$ *y* $mcd(a, b) = 1$, *entonces* $ab|c$.

El Lema(***)

Lema (***)

Sean $a, b, c \in \mathbb{Z}$ *con* $a \neq 0$ *o* $b \neq 0$. *Si* $a|c$, $b|c$ *y* $mcd(a, b) = 1$, *entonces* $ab|c$.

Demostración: En esta ocasión tenemos tres hipótesis.

El Lema(***)

Lema (***)

Sean $a, b, c \in \mathbb{Z}$ *con* $a \neq 0$ *o* $b \neq 0$. *Si* $a|c$, $b|c$ *y* $mcd(a, b) = 1$, *entonces* $ab|c$.

Demostración: En esta ocasión tenemos tres hipótesis.
Por un lado, como $a|c$, existe $k \in \mathbb{Z}$ tal que

$$ak = c. \tag{11}$$

El Lema(***)

Lema (***)

Sean $a, b, c \in \mathbb{Z}$ *con* $a \neq 0$ *o* $b \neq 0$. *Si* $a|c$, $b|c$ *y* $mcd(a, b) = 1$, *entonces* $ab|c$.

Demostración: En esta ocasión tenemos tres hipótesis.
Por un lado, como $a|c$, existe $k \in \mathbb{Z}$ tal que

$$ak = c. \tag{11}$$

Por otro lado, como $b|c$, existe $m \in Z$ tal que

$$bm = c. \tag{12}$$

Prueba del Lema(***)

Nuestra tercera hipótesis es que $mcd(a, b) = 1$.

Prueba del Lema(***)

Nuestra tercera hipótesis es que $mcd(a, b) = 1$. Por el Teorema III existen $\alpha, \beta \in \mathbb{Z}$ tales que

$$1 = \alpha a + \beta b. \tag{13}$$

Prueba del Lema(***)

Nuestra tercera hipótesis es que $mcd(a, b) = 1$. Por el Teorema III existen $\alpha, \beta \in \mathbb{Z}$ tales que

$$1 = \alpha a + \beta b. \tag{13}$$

Multiplicando por c se sigue que

$$c = \alpha ac + \beta bc. \tag{14}$$

Prueba del Lema(***)

Nuestra tercera hipótesis es que $mcd(a, b) = 1$. Por el Teorema III existen $\alpha, \beta \in \mathbb{Z}$ tales que

$$1 = \alpha a + \beta b. \tag{13}$$

Multiplicando por c se sigue que

$$c = \alpha ac + \beta bc. \tag{14}$$

Vamos ahora a sustituir (11) y (12) en (14), pero lo haremos con cuidado para que quede de la siguiente forma:

$$c = (\alpha a)(bm) + (\beta b)(ak). \tag{15}$$

Prueba del Lema(***)

Esto último se puede reescribir de una manera más adecuada:

$$c = ab(\alpha m + \beta k), \tag{16}$$

Esto último se puede reescribir de una manera más adecuada:

$$c = ab(\alpha m + \beta k), \tag{16}$$

con lo cual podemos concluir que $ab|c$. $\square$

Una propiedad más

Ahora que estamos estudiando al máximo común divisor, sería bueno saber qué propiedades interesantes tiene. También sería bueno encontrar propiedades que fueran particularmente útiles.

Una propiedad más

Ahora que estamos estudiando al máximo común divisor, sería bueno saber qué propiedades interesantes tiene. También sería bueno encontrar propiedades que fueran particularmente útiles.

Por ejemplo, sería bueno saber si el máximo común divisor "saca escalares".

Una propiedad más

Ahora que estamos estudiando al máximo común divisor, sería bueno saber qué propiedades interesantes tiene. También sería bueno encontrar propiedades que fueran particularmente útiles.

Por ejemplo, sería bueno saber si el máximo común divisor "saca escalares".

La pregunta concreta sería:

Pregunta

¿Es cierto que $mcd(ac, bc) = c \cdot mcd(a, b)$*?*

Una propiedad más

Ahora que estamos estudiando al máximo común divisor, sería bueno saber qué propiedades interesantes tiene. También sería bueno encontrar propiedades que fueran particularmente útiles.

Por ejemplo, sería bueno saber si el máximo común divisor "saca escalares".

La pregunta concreta sería:

Pregunta

¿Es cierto que $mcd(ac, bc) = c \cdot mcd(a, b)$*?*

Desde luego, c no podría ser cero (¿por qué?)

Una propiedad más

En principio la respuesta es negativa, porque $mcd(ac, bc)$ **siempre** es mayor o igual que 1 (¿te acuerdas?). Por otro lado, si $c < 0$, entonces queda que $c \cdot mcd(a, b) < 0$.

Una propiedad más

En principio la respuesta es negativa, porque $mcd(ac, bc)$ **siempre** es mayor o igual que 1 (¿te acuerdas?). Por otro lado, si $c < 0$, entonces queda que $c \cdot mcd(a, b) < 0$.

Tomando en cuenta esta observación, lo que tendría sentido sería preguntar lo siguiente:

Una propiedad más

En principio la respuesta es negativa, porque $mcd(ac, bc)$ **siempre** es mayor o igual que 1 (¿te acuerdas?). Por otro lado, si $c < 0$, entonces queda que $c \cdot mcd(a, b) < 0$.

Tomando en cuenta esta observación, lo que tendría sentido sería preguntar lo siguiente:

Pregunta

¿Es cierto que $mcd(ac, bc) = |c| mcd(a, b)$*?*

Una nueva propiedad

Resulta que la respuesta ¡es afirmativa! y lo probaremos en la siguiente presentación.

Aquí incluimos el enunciado preciso de lo que se probará la próxima ocasión.

Una nueva propiedad

Resulta que la respuesta ¡es afirmativa! y lo probaremos en la siguiente presentación.

Aquí incluimos el enunciado preciso de lo que se probará la próxima ocasión.

Teorema

Sean $a, b \in \mathbb{Z}$ *con* $a \neq 0$ *o* $b \neq 0$. *Si* $c \in \mathbb{Z} \setminus \{0\}$, *entonces* $mcd(ac, bc) = |c| mcd(a, b)$.

Una nueva propiedad

Resulta que la respuesta ¡es afirmativa! y lo probaremos en la siguiente presentación.

Aquí incluimos el enunciado preciso de lo que se probará la próxima ocasión.

Teorema

Sean $a, b \in \mathbb{Z}$ con $a \neq 0$ o $b \neq 0$. Si $c \in \mathbb{Z} \setminus \{0\}$, entonces $mcd(ac, bc) = |c| mcd(a, b)$.

Si tienes alguna duda sobre este material, me puedes escribir a paty ciencias.unam.mx