Álgebra y Matemática Discreta

Arimética

Grado en Ingeniería Informática - 2019/20

Facultad de Informática

UNIVERSIDAD DE MURCIA

Divisibilidad

- Dados dos números enteros a y $b > 1$ existen valores q y r enteros tales que $a = bq + r$ y $0 \leq r < b$. Estos valores se denominan *cociente* y *resto* de la división, y son únicos.

Divisibilidad

- Dados dos números enteros a y $b > 1$ existen valores q y r enteros tales que $a = bq + r$ y $0 \leq r < b$. Estos valores se denominan *cociente* y *resto* de la división, y son únicos.
- Si $a = -13$ y $b = 4$, ¿ hallar q y r ?.

Divisibilidad

- Dados dos números enteros a y $b > 1$ existen valores q y r enteros tales que $a = bq + r$ y $0 \leq r < b$. Estos valores se denominan *cociente* y *resto* de la división, y son únicos.
- Si $a = -13$ y $b = 4$, ¿ hallar q y r ?.
- Diremos que b divide a a (o que a es múltiplo de b) si existe q tal que $a = bq$. Lo denotaremos $b|a$.

Divisibilidad

- Dados dos números enteros a y $b > 1$ existen valores q y r enteros tales que $a = bq + r$ y $0 \leq r < b$. Estos valores se denominan *cociente* y *resto* de la división, y son únicos.
- Si $a = -13$ y $b = 4$, ¿ hallar q y r ?.
- Diremos que b divide a a (o que a es múltiplo de b) si existe q tal que $a = bq$. Lo denotaremos $b|a$.
- En el caso en que b sea positivo, esto es equivalente a decir que el resto de la división de a entre b es 0.

Divisibilidad: Propiedades

- Si $a|b$ entonces $a|bk$ para todo k.

Divisibilidad: Propiedades

- Si $a|b$ entonces $a|bk$ para todo k.
- Si $a|b$ entonces $-a|b$.

Divisibilidad: Propiedades

- Si $a|b$ entonces $a|bk$ para todo k.
- Si $a|b$ entonces $-a|b$.
- Si $a|b$ y $b|c$ entonces $a|c$.

Divisibilidad: Propiedades

- Si $a|b$ entonces $a|bk$ para todo k.
- Si $a|b$ entonces $-a|b$.
- Si $a|b$ y $b|c$ entonces $a|c$.
- Si $a|b$ y $a|c$ entonces $a|(br + cs)$ para todo $r, s \in \mathbb{Z}$.

Divisores

- Sea a un entero, denotaremos $\mathrm{D}(a)$ al conjunto de divisores positivos de a. Este conjunto siempre tiene a 1 y a $|a|$.

Divisores

- Sea a un entero, denotaremos $\mathrm{D}(a)$ al conjunto de divisores positivos de a. Este conjunto siempre tiene a 1 y a $|a|$.
- Diremos que dos números a y b son coprimos si

$$\mathrm{D}(a) \cap \mathrm{D}(b) = \{1\}$$

Divisores

- Sea a un entero, denotaremos $\mathrm{D}(a)$ al conjunto de divisores positivos de a. Este conjunto siempre tiene a 1 y a $|a|$.
- Diremos que dos números a y b son coprimos si

$$\mathrm{D}(a) \cap \mathrm{D}(b) = \{1\}$$

- El valor más grande del conjunto $\mathrm{D}(a) \cap \mathrm{D}(b)$ se llama máximo común divisor de a y b.

Divisores

- Sea a un entero, denotaremos $\mathrm{D}(a)$ al conjunto de divisores positivos de a. Este conjunto siempre tiene a 1 y a $|a|$.
- Diremos que dos números a y b son coprimos si

$$\mathrm{D}(a) \cap \mathrm{D}(b) = \{1\}$$

- El valor más grande del conjunto $\mathrm{D}(a) \cap \mathrm{D}(b)$ se llama máximo común divisor de a y b.
- Dualmente, el mínimo común múltiplo será el menor de los múltiplos comunes de a y b.

Divisores

- Sea a un entero, denotaremos $\mathrm{D}(a)$ al conjunto de divisores positivos de a. Este conjunto siempre tiene a 1 y a $|a|$.
- Diremos que dos números a y b son coprimos si

$$\mathrm{D}(a) \cap \mathrm{D}(b) = \{1\}$$

- El valor más grande del conjunto $\mathrm{D}(a) \cap \mathrm{D}(b)$ se llama máximo común divisor de a y b.
- Dualmente, el mínimo común múltiplo será el menor de los múltiplos comunes de a y b.
- Diremos que un número p es primo si $\mathrm{D}(p)$ tiene exactamente dos valores 1 y p.

Teorema Fundamental de la Aritmética

- Todo entero positivo n se puede descomponer de forma única (salvo el orden) como producto de primos

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

Poniendo exponentes 0 para casi todos los primos, podemos poner

$$n = \prod_{p:primo} p^{\alpha_p}$$

Teorema Fundamental de la Aritmética

- Todo entero positivo n se puede descomponer de forma única (salvo el orden) como producto de primos

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

Poniendo exponentes 0 para casi todos los primos, podemos poner

$$n = \prod_{p:primo} p^{\alpha_p}$$

- Si $a = \prod_{p:primo} p^{\alpha_p}$ y $b = \prod_{p:primo} p^{\beta_p}$, entonces
  - $a|b$ si y solo si $\alpha_p \leq \beta_p$ para todo p.
  - $mcd(a,b) = \prod_{p:primo} p^{min(\alpha_p,\beta_p)}$
  - $mcm(a,b) = \prod_{p:primo} p^{max(\alpha_p,\beta_p)}$

Algoritmo de Euclides

- Dados dos números (que podemos suponer positivos), calcular el máximo común divisor factorizando puede ser muy complicado.

Algoritmo de Euclides

- Dados dos números (que podemos suponer positivos), calcular el máximo común divisor factorizando puede ser muy complicado.
- El algoritmo más efectivo es el algoritmo de euclides, que se basa en la propiedad de que si $a = bq + r$ entonces $mcd(a, b) = mcd(b, r)$.

  (Los números a,b y por otro lado los números b,r tienen los mismos divisores. Los divisores comunes de a y b son divisores de r y recíprocamente los divisores comunes de b y r son divisores de a)

Algoritmo de Euclides

- **Ejemplo:** $mcd(125, 35)$

$125 = 3 \cdot 35 + 20$
$35 = 1 \cdot 20 + 15$
$20 = 1 \cdot 15 + 5$
$15 = 3 \cdot 5 + 0$
Tenemos

$$mcd(125, 35) = mcd(35, 20) = mcd(20, 15) = mcd(15, 5) = 5.$$

El máximo común divisor es 5.

Algoritmo de Euclides

- **Algoritmo:**
  Dados $a, b \in \mathbb{Z}$, podemos suponer $a \geq b > 0$ (ya que $mcd(a, b) = mcd(|a|, |b|)$). Entonces

  - Dividimos a entre b tal que $a = b \cdot q_1 + r_1$ $(0 \leq r_1 < b)$
  - Si $r_1 \neq 0$, sustituimos (a, b) por (b, r_1) y repetimos el proceso (dividir b entre r_1) hasta llegar al resto igual a 0.
  - El máximo común divisor será el último resto no nulo.

Algoritmo de Euclides Extendido

- **Teorema de Bezout:** Sean a y b dos enteros y d su máximo común divisor, entonces podemos encontrar valores u y v tales que $d = au + bv$.

Algoritmo de Euclides Extendido

- **Teorema de Bezout:** Sean a y b dos enteros y d su máximo común divisor, entonces podemos encontrar valores u y v tales que $d = au + bv$.
- De hecho el $mcd(a, b)$ es el menor entero positivo que puede expresarse como combinación de a y b.

Algoritmo de Euclides Extendido

- **Teorema de Bezout:** Sean a y b dos enteros y d su máximo común divisor, entonces podemos encontrar valores u y v tales que $d = au + bv$.
- De hecho el $mcd(a, b)$ es el menor entero positivo que puede expresarse como combinación de a y b.
- Para calcular los valores de dicha combinación basta con seguir el camino inverso hecho en el Algoritmo de Euclides.

Algoritmo de Euclides Extendido

- **Teorema de Bezout:** Sean a y b dos enteros y d su máximo común divisor, entonces podemos encontrar valores u y v tales que $d = au + bv$.
- De hecho el $mcd(a, b)$ es el menor entero positivo que puede expresarse como combinación de a y b.
- Para calcular los valores de dicha combinación basta con seguir el camino inverso hecho en el Algoritmo de Euclides.
- Para el cálculo de $mcd(125, 35)$ tenemos

$$125 = 3 \cdot 35 + 20$$
$$35 = 1 \cdot 20 + 15$$
$$20 = 1 \cdot 15 + 5$$
$$15 = 3 \cdot 5 + 0$$

Algoritmo de Euclides Extendido

- Comenzamos por la expresión donde el máximo común denominador es igual a un resto, a saber $5 = 20 + (-1) \cdot 15$.

Algoritmo de Euclides Extendido

- Comenzamos por la expresión donde el máximo común denominador es igual a un resto, a saber $5 = 20 + (-1) \cdot 15$.
- Iremos sustituyendo todos los restos de uno en uno factorizando los dividendos y divisores. Así

$$5 = 20+(-1)\cdot 15 = 20+(-1)[35+(-1)\cdot 20] = 2\cdot 20+(-1)\cdot 35 =$$

$$= 2 \cdot (125 + (-3) \cdot 35) + (-1) \cdot 35 = 2 \cdot 125 + (-7) \cdot 35.$$

La combinación es $5 = 125 \cdot 2 + 35 \cdot (-7)$.

Descomposición de un número en primos

Sea n un entero ($n > 1$), entonces n no es primo si y sólo si existe un número primo p, con $p \leq \sqrt{n}$, tal que p divide a n.

- Este resultado nos permite ver si un número se factoriza o no, y si se factoriza, encontrar un factor.

Descomposición de un número en primos

Sea n un entero ($n > 1$), entonces n no es primo si y sólo si existe un número primo p, con $p \leq \sqrt{n}$, tal que p divide a n.

- Este resultado nos permite ver si un número se factoriza o no, y si se factoriza, encontrar un factor.
- Sólo tenemos que ver si se factoriza por aquellos primos que son menores o iguales a su raíz cuadrada.
  - $a = 40$. Como $6 < \sqrt{40} < 7$, veamos si se factoriza por el 2, 3 o 5. Es fácil ver que $40 = 2^3 \cdot 5$.
  - $a = 53$. Como $7 < \sqrt{53} < 8$, veamos si se factoriza por el 2, 3, 5 o 7. Observamos que $53 = 2 \cdot 26 + 1$, $53 = 3 \cdot 17 + 2$, $53 = 5 \cdot 10 + 3$, $53 = 7 \cdot 7 + 4$
    con lo que 53 es primo.

Divisores de un número

Dado un número factorizado en primos, podemos calcular todos sus divisores.

- Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, entonces todo divisor d de n es de la forma $d = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ con $0 \leq m_i \leq \alpha_i$.

Divisores de un número

Dado un número factorizado en primos, podemos calcular todos sus divisores.

- Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, entonces todo divisor d de n es de la forma $d = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ con $0 \leq m_i \leq \alpha_i$.
- El número total de divisores es: $(\alpha_1 + 1) \cdot \cdots \cdot (\alpha_k + 1)$.

Divisores de un número

Dado un número factorizado en primos, podemos calcular todos sus divisores.

- Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, entonces todo divisor d de n es de la forma $d = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ con $0 \leq m_i \leq \alpha_i$.
- El número total de divisores es: $(\alpha_1 + 1) \cdot \cdots \cdot (\alpha_k + 1)$.
- Los divisores de $40 = 2^3 \cdot 5$ son:
  - Considerando el primo 2:

    $$2, \quad 10 = 2 \cdot 5, \quad 4 = 2^2, \quad 20 = 2^2 \cdot 5, \quad 8 = 2^3, \quad 40 = 2^3 \cdot 5$$

  - Considerando el primo 5, descartando el 2

    $$5$$

  - No olvidemos el 1

  En total $(3 + 1) \cdot (1 + 1) = 8$ divisores.

Ecuaciones diofánticas

- Una **ecuación diofántica** es una ecuación con coeficientes enteros de la que tenemos que encontrar las soluciones enteras.

Ecuaciones diofánticas

- Una **ecuación diofántica** es una ecuación con coeficientes enteros de la que tenemos que encontrar las soluciones enteras.
- Por ejemplo, de $7x + 5y = 3$ sabemos que $x = (3 - 5y)/7$, pero ésta puede no ser una solución válida.

Ecuaciones diofánticas

- Una **ecuación diofántica** es una ecuación con coeficientes enteros de la que tenemos que encontrar las soluciones enteras.
- Por ejemplo, de $7x + 5y = 3$ sabemos que $x = (3 - 5y)/7$, pero ésta puede no ser una solución válida.
- Imaginemos que x e y representan objetos indivisibles y no podemos decidir tomar $3/7$ de persona, por ejemplo. La resolución de multitud de pasatiempos aritméticos se basan en este tipo de ecuaciones.

Ecuaciones diofánticas

- Una **ecuación diofántica** es una ecuación con coeficientes enteros de la que tenemos que encontrar las soluciones enteras.
- Por ejemplo, de $7x + 5y = 3$ sabemos que $x = (3 - 5y)/7$, pero ésta puede no ser una solución válida.
- Imaginemos que x e y representan objetos indivisibles y no podemos decidir tomar $3/7$ de persona, por ejemplo. La resolución de multitud de pasatiempos aritméticos se basan en este tipo de ecuaciones.
- Una solución es $x = -6$ e $y = 9$, pero existen muchas otras.

Ecuaciones diofánticas

- Una **ecuación diofántica** es una ecuación con coeficientes enteros de la que tenemos que encontrar las soluciones enteras.
- Por ejemplo, de $7x + 5y = 3$ sabemos que $x = (3 - 5y)/7$, pero ésta puede no ser una solución válida.
- Imaginemos que x e y representan objetos indivisibles y no podemos decidir tomar $3/7$ de persona, por ejemplo. La resolución de multitud de pasatiempos aritméticos se basan en este tipo de ecuaciones.
- Una solución es $x = -6$ e $y = 9$, pero existen muchas otras.
- Vamos a aprender a encontrar las soluciones de este tipo de ecuaciones, y a saber cuando existen.

Ecuaciones diofánticas

- Una **ecuación diofántica** es una ecuación con coeficientes enteros de la que tenemos que encontrar las soluciones enteras.
- Por ejemplo, de $7x + 5y = 3$ sabemos que $x = (3 - 5y)/7$, pero ésta puede no ser una solución válida.
- Imaginemos que x e y representan objetos indivisibles y no podemos decidir tomar $3/7$ de persona, por ejemplo. La resolución de multitud de pasatiempos aritméticos se basan en este tipo de ecuaciones.
- Una solución es $x = -6$ e $y = 9$, pero existen muchas otras.
- Vamos a aprender a encontrar las soluciones de este tipo de ecuaciones, y a saber cuando existen.
- Si las ecuaciones son no lineales, el problema se puede complicar enormemente y sobrepasa con mucho lo que vamos a ver en este curso. Hay muchos problemas abiertos relacionados con ecuacones diofánticas no lineales.

Condición para la Existencia de Solución

- No todas las ecuaciones diofánticas lineales tienen solución. Pensemos por ejemplo, en $8x - 6y = 1$, sean cuales sean los valores de x y de y, sabemos que $8x$ es un número par y que $6y$ también. Su diferencia será siempre un número par, nunca puede ser 1.

Condición para la Existencia de Solución

- No todas las ecuaciones diofánticas lineales tienen solución. Pensemos por ejemplo, en $8x - 6y = 1$, sean cuales sean los valores de x y de y, sabemos que $8x$ es un número par y que $6y$ también. Su diferencia será siempre un número par, nunca puede ser 1.
- **Existencia de Soluciones de una Ecuación Diofántica:** Una ecuación diofántica lineal del tipo $ax + by = c$ tendrá solución si y sólo si el máximo común divisor de a y b divide a c.

Condición para la Existencia de Solución

- No todas las ecuaciones diofánticas lineales tienen solución. Pensemos por ejemplo, en $8x - 6y = 1$, sean cuales sean los valores de x y de y, sabemos que $8x$ es un número par y que $6y$ también. Su diferencia será siempre un número par, nunca puede ser 1.
- **Existencia de Soluciones de una Ecuación Diofántica:** Una ecuación diofántica lineal del tipo $ax + by = c$ tendrá solución si y sólo si el máximo común divisor de a y b divide a c.
- Cualquier divisor común de a y b dividirá a ax y a bx y por lo tanto a su suma $ax + by = c$. Si eso es cierto para todoss los divisores, en particular es cierto para el máximo común divisor.

Condición para la Existencia de Solución

- No todas las ecuaciones diofánticas lineales tienen solución. Pensemos por ejemplo, en $8x - 6y = 1$, sean cuales sean los valores de x y de y, sabemos que $8x$ es un número par y que $6y$ también. Su diferencia será siempre un número par, nunca puede ser 1.
- **Existencia de Soluciones de una Ecuación Diofántica:** Una ecuación diofántica lineal del tipo $ax + by = c$ tendrá solución si y sólo si el máximo común divisor de a y b divide a c.
- Cualquier divisor común de a y b dividirá a ax y a bx y por lo tanto a su suma $ax + by = c$. Si eso es cierto para todoss los divisores, en particular es cierto para el máximo común divisor.
- Por otro lado, supongamos que el máximo común divisor d divide a c, es decir, $c = dk$ para algún k. Entonces como por el algoritmo de euclides extendido podemos encontrar soluciones u y v tales que $d = au + bv$ podemos poner $c = dk = auk + bvk$ y entoncces $x_0 = uk$, $y_0 = vk$ es solución.

Si Hay una Solución, Hay Infinitas

- Una ecuación diofántica lineal, o bien no tiene solución, o si las tiene, tiene que tener una cantidad infinita.

Si Hay una Solución, Hay Infinitas

- Una ecuación diofántica lineal, o bien no tiene solución, o si las tiene, tiene que tener una cantidad infinita.
- Vamos a ver cómo se generan todas las soluciones. Ya hemos visto que podemos encontrar una, que llamaremos (x_0, y_0) (una solución particular). A partir de ella se pueden encontrar las demás:

Si Hay una Solución, Hay Infinitas

- Una ecuación diofántica lineal, o bien no tiene solución, o si las tiene, tiene que tener una cantidad infinita.
- Vamos a ver cómo se generan todas las soluciones. Ya hemos visto que podemos encontrar una, que llamaremos (x_0, y_0) (una solución particular). A partir de ella se pueden encontrar las demás:
- $$x = x_0 - \frac{b}{d}t, \quad y = y_0 + \frac{a}{d}t \qquad \forall t \in \mathbb{Z}$$

  Son todas las soluciones de la ecuación.

Si Hay una Solución, Hay Infinitas

- Una ecuación diofántica lineal, o bien no tiene solución, o si las tiene, tiene que tener una cantidad infinita.
- Vamos a ver cómo se generan todas las soluciones. Ya hemos visto que podemos encontrar una, que llamaremos (x_0, y_0) (una solución particular). A partir de ella se pueden encontrar las demás:
- $$x = x_0 - \frac{b}{d}t, \quad y = y_0 + \frac{a}{d}t \qquad \forall t \in \mathbb{Z}$$

  Son todas las soluciones de la ecuación.
- Si sustituimos, vemos que

$$ax + by = a(x_0 - \frac{b}{d}t) + b(y_0 + \frac{a}{d}t) = ax_0 + by_0 - \frac{ab}{d}t + \frac{ab}{d}t = c$$

Ejemplo: Método I

Encuentra las soluciones enteras de la ecuación $42x + 32y = 14$

- Paso 1: Calculamos el $mcd(42, 32)$

$$42 = 32 \cdot 1 + 10, \quad 32 = 10 \cdot 3 + 2, \quad 10 = 2 \cdot 5$$

  El máximo común divisor es 2.

- Paso 2: Comprobamos que el máximo común divisor divide al término independiente y dividimos la ecuación por dicho valor, nos queda la euación ya normalizada $21x + 16y = 7$.
- Paso 3: Utilizando el algoritmo de Euclides extendido, calculamos coeficientes u y v tales que $1 = 21u + 16v$. Eso lo podemos hacerde varias formas, por ejemplo usando las divisiones que hemos hecho en el Paso 1, o de cualquier otra forma explicada en clase. Por ejemplo $21 \cdot (-3) + 16 \cdot 4 = 1$.

Ejemplo: Método I

- La solución particular se obtiene multiplicando el término independiente de la ecuación normalizada por esta combinación

$$21 \cdot [(-3) \cdot 7] + 16 \cdot [4 \cdot 7] = 7$$

Ejemplo: Método I

- La solución particular se obtiene multiplicando el término independiente de la ecuación normalizada por esta combinación

$$21 \cdot [(-3) \cdot 7] + 16 \cdot [4 \cdot 7] = 7$$

- La solución particular es $(x_0, y_0) = ((-3) \cdot 7, 4 \cdot 7) = (-21, 28)$, siendo la solución general

$$x = -21 - 16t, \quad y = 28 + 21t$$

donde t es un entero cualquiera.

Ejemplo: Método I (Variante)

Encuentra las soluciones enteras de la ecuación $42x + 32y = 14$

- Paso 1: Calculamos el $mcd(42, 32)$

$$42 = 32 \cdot 1 + 10, \quad 32 = 10 \cdot 3 + 2, \quad 10 = 2 \cdot 5$$

El máximo común divisor es 2 y la combinación de 42 y 32 que nos da el máximo común divisor es $2 = 42 \cdot (-3) + 32 \cdot 4$.

Ejemplo: Método I (Variante)

Encuentra las soluciones enteras de la ecuación $42x + 32y = 14$

- Paso 1: Calculamos el $mcd(42, 32)$

$$42 = 32 \cdot 1 + 10, \quad 32 = 10 \cdot 3 + 2, \quad 10 = 2 \cdot 5$$

El máximo común divisor es 2 y la combinación de 42 y 32 que nos da el máximo común divisor es $2 = 42 \cdot (-3) + 32 \cdot 4$.

- Comprobamos que el máximo común divisor divide al término independiente

Ejemplo: Método I (Variante)

Encuentra las soluciones enteras de la ecuación $42x + 32y = 14$

- Paso 1: Calculamos el $mcd(42, 32)$

$$42 = 32 \cdot 1 + 10, \quad 32 = 10 \cdot 3 + 2, \quad 10 = 2 \cdot 5$$

El máximo común divisor es 2 y la combinación de 42 y 32 que nos da el máximo común divisor es $2 = 42 \cdot (-3) + 32 \cdot 4$.

- Comprobamos que el máximo común divisor divide al término independiente
- La solución particular se obtiene multiplicando el término independiente dividido por el máximo común divisor d

$$42 \cdot [(-3) \cdot 7] + 32 \cdot [4 \cdot 7] = 14$$

Ejemplo: Método I (Variante)

Encuentra las soluciones enteras de la ecuación $42x + 32y = 14$

- Paso 1: Calculamos el $mcd(42, 32)$

$$42 = 32 \cdot 1 + 10, \quad 32 = 10 \cdot 3 + 2, \quad 10 = 2 \cdot 5$$

El máximo común divisor es 2 y la combinación de 42 y 32 que nos da el máximo común divisor es $2 = 42 \cdot (-3) + 32 \cdot 4$.

- Comprobamos que el máximo común divisor divide al término independiente
- La solución particular se obtiene multiplicando el término independiente dividido por el máximo común divisor d

$$42 \cdot [(-3) \cdot 7] + 32 \cdot [4 \cdot 7] = 14$$

- La solución general es $x = x_0 - \frac{32}{d}t = -21 - 16t$, $y = y_0 + \frac{42}{d}t = 28 + 21t$, donde t es un entero cualquiera.

Método II

Una vez estudiado en aritmética modular los enteros congruentes módulo un natural n, estudiaremos un segundo método basado en convertir la ecuación diofántica (una vez normalizada) en una ecuación modular.