MOOC de Criptología Matemática. Aritmética Entera

Leandro Marín

Módulo II. Sesión 1.
Dificultad Baja

Definición

- Llamaremos $\mathbb{Z}$ o conjunto de los números enteros a los números positivos y negativos sin decimales.

$$\{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$$

Definición

- Llamaremos $\mathbb{Z}$ o conjunto de los números enteros a los números positivos y negativos sin decimales.

$$\{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$$

- Este conjunto es infinito tanto por la parte positiva como por la parte negativa.

Definición

- Llamaremos $\mathbb{Z}$ o conjunto de los números enteros a los números positivos y negativos sin decimales.

$$\{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$$

- Este conjunto es infinito tanto por la parte positiva como por la parte negativa.
- Los números enteros se pueden sumar, restar y multiplicar con las reglas habituales.

Definición

- Llamaremos $\mathbb{Z}$ o conjunto de los números enteros a los números positivos y negativos sin decimales.

$$\{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$$

- Este conjunto es infinito tanto por la parte positiva como por la parte negativa.
- Los números enteros se pueden sumar, restar y multiplicar con las reglas habituales.
- Matemáticamente forman lo que se denomina un anillo.

Representación en sage

- El conjunto de los números enteros se representa en sage mediante el símbolo ZZ.

Representación en sage

- El conjunto de los números enteros se representa en sage mediante el símbolo ZZ.
- Si escribimos este símbolo en sage y pulsamos ENTER obtenemos el siguiente resultado:

```
sage: ZZ
Integer Ring
```

Representación en sage

- El conjunto de los números enteros se representa en sage mediante el símbolo ZZ.
- Si escribimos este símbolo en sage y pulsamos ENTER obtenemos el siguiente resultado:

```
sage: ZZ
Integer Ring
```

- Ya lo hemos usado anteriormente para obtener la representación de un número en una base cualquiera o para obtener un número a partir de sus cifras.

```
sage: ZZ(1234).digits(10)
[4, 3, 2, 1]
sage: ZZ([4,3,2,1],10)
1234
```

La División Entera

- Una de las propiedades fundamentales que tiene este conjunto es la de disponer de una división con resto.

La División Entera

- Una de las propiedades fundamentales que tiene este conjunto es la de disponer de una división con resto.
- Es decir, dados dos números enteros a y b con $b > 0$ existen dos valores enteros q y r tales que $a = bq + r$ y $0 \leq r < b$.

La División Entera

- Una de las propiedades fundamentales que tiene este conjunto es la de disponer de una división con resto.
- Es decir, dados dos números enteros a y b con $b > 0$ existen dos valores enteros q y r tales que $a = bq + r$ y $0 \leq r < b$.
- Estos valores q y r son únicos y se denominan cociente y resto de la división.

La División Entera

- Una de las propiedades fundamentales que tiene este conjunto es la de disponer de una división con resto.
- Es decir, dados dos números enteros a y b con $b > 0$ existen dos valores enteros q y r tales que $a = bq + r$ y $0 \leq r < b$.
- Estos valores q y r son únicos y se denominan cociente y resto de la división.
- A los valores a y b se les deomina dividendo y divisor.

La División Entera

- Una de las propiedades fundamentales que tiene este conjunto es la de disponer de una división con resto.
- Es decir, dados dos números enteros a y b con $b > 0$ existen dos valores enteros q y r tales que $a = bq + r$ y $0 \leq r < b$.
- Estos valores q y r son únicos y se denominan cociente y resto de la división.
- A los valores a y b se les deomina dividendo y divisor.
- Cuando el resto r vale 0 diremos que b divide a a o que a es múltiplo de b.

Ejemplo I

- Empecemos con un ejemplo sencillo, vamos a dividir 23 entre 5.

Ejemplo I

- Empecemos con un ejemplo sencillo, vamos a dividir 23 entre 5.
- En este caso $a = 23$ y $b = 5$, el cociente será 4 y el resto 3 puesto que $23 = 5 \cdot 4 + 3$ y $0 \leq 3 < 5$.

Ejemplo I

- Empecemos con un ejemplo sencillo, vamos a dividir 23 entre 5.
- En este caso $a = 23$ y $b = 5$, el cociente será 4 y el resto 3 puesto que $23 = 5 \cdot 4 + 3$ y $0 \leq 3 < 5$.
- Si lo hacemos en sage obtenemos estos valores:

```
sage: 23//5
4
sage: 23%5
3
```

Ejemplo I

- Empecemos con un ejemplo sencillo, vamos a dividir 23 entre 5.
- En este caso $a = 23$ y $b = 5$, el cociente será 4 y el resto 3 puesto que $23 = 5 \cdot 4 + 3$ y $0 \leq 3 < 5$.
- Si lo hacemos en sage obtenemos estos valores:

```
sage: 23//5
4
sage: 23%5
3
```

- Notemos que el símbolo para calcular el cociente es // (una sola barra representaría la fracción, no la división) y el símbolo % se usa para el resto.

Ejemplo II

- En el caso de b (el divisor), hemos exigido que sea un número mayor que 0, pero no hemos puesto restricciones en a (el dividendo).

Ejemplo II

- En el caso de b (el divisor), hemos exigido que sea un número mayor que 0, pero no hemos puesto restricciones en a (el dividendo).
- Vamos ahora a calcular -23 dividido entre 5. Empecemos viéndolo en `sage`.

```
sage: -23//5
-5
sage: -23%5
2
```

Ejemplo II

- En el caso de b (el divisor), hemos exigido que sea un número mayor que 0, pero no hemos puesto restricciones en a (el dividendo).
- Vamos ahora a calcular -23 dividido entre 5. Empecemos viéndolo en `sage`.

```
sage: -23//5
-5
sage: -23%5
2
```

- Si comprobamos la definición, podemos ver que $-23 = 5(-5) + 2$ y que $0 \leq 2 < 5$, por lo tanto el resultado es correcto.

Ejemplo II

- En el caso de b (el divisor), hemos exigido que sea un número mayor que 0, pero no hemos puesto restricciones en a (el dividendo).
- Vamos ahora a calcular -23 dividido entre 5. Empecemos viéndolo en `sage`.

```
sage: -23//5
-5
sage: -23%5
2
```

- Si comprobamos la definición, podemos ver que $-23 = 5(-5) + 2$ y que $0 \leq 2 < 5$, por lo tanto el resultado es correcto.
- Pero la intuición puede que nos dijera que -23 entre 5 daba cociente -4. Eso no es correcto si exigimos, tal y como lo hemos hecho, que los restos siempre sean mayores o iguales que 0, nunca negativos.

Ejemplo II

- En el caso de b (el divisor), hemos exigido que sea un número mayor que 0, pero no hemos puesto restricciones en a (el dividendo).
- Vamos ahora a calcular -23 dividido entre 5. Empecemos viéndolo en `sage`.

```
sage: -23//5
-5
sage: -23%5
2
```

- Si comprobamos la definición, podemos ver que $-23 = 5(-5) + 2$ y que $0 \leq 2 < 5$, por lo tanto el resultado es correcto.
- Pero la intuición puede que nos dijera que -23 entre 5 daba cociente -4. Eso no es correcto si exigimos, tal y como lo hemos hecho, que los restos siempre sean mayores o iguales que 0, nunca negativos.
- Tengamos esto en cuenta,*cuando dividimos números negativos debemos poner el cociente de forma que el resto obtenido por la fórmula no sea nunca negativo.*

Definición

- Diremos que un número entero b divide a un número entero a si existe un número entero c tal que $bc = a$.

Definición

- Diremos que un número entero b divide a un número entero a si existe un número entero c tal que $bc = a$.
- Utilizando esta definición, si b divide a a entonces $-b$ también divide a a porque $a = bc = (-b)(-c)$.

Definición

- Diremos que un número entero b divide a un número entero a si existe un número entero c tal que $bc = a$.
- Utilizando esta definición, si b divide a a entonces $-b$ también divide a a porque $a = bc = (-b)(-c)$.
- Podemos por tanto considerar sólo los divisores positivos, para evitar contar los divisores dos veces.

Definición

- Diremos que un número entero b divide a un número entero a si existe un número entero c tal que $bc = a$.
- Utilizando esta definición, si b divide a a entonces $-b$ también divide a a porque $a = bc = (-b)(-c)$.
- Podemos por tanto considerar sólo los divisores positivos, para evitar contar los divisores dos veces.
- Un número estrictamente mayor que 1 diremos que es un número primo cuando sus únicos divisores sean él mismo y 1.

Definición

- Diremos que un número entero b divide a un número entero a si existe un número entero c tal que $bc = a$.
- Utilizando esta definición, si b divide a a entonces $-b$ también divide a a porque $a = bc = (-b)(-c)$.
- Podemos por tanto considerar sólo los divisores positivos, para evitar contar los divisores dos veces.
- Un número estrictamente mayor que 1 diremos que es un número primo cuando sus únicos divisores sean él mismo y 1.
- Por definición 1 no es un número primo, por tanto los números primos siempre tendrán dos divisores positivos distintos.

Infinitud de los Números Primos

- Existe una cantidad de números primos infinita.

Infinitud de los Números Primos

- Existe una cantidad de números primos infinita.
- En criptografía a veces es necesario encontrar números primos muy grandes.

Infinitud de los Números Primos

- Existe una cantidad de números primos infinita.
- En criptografía a veces es necesario encontrar números primos muy grandes.
- Eso es posible utilizando algoritmos especiales que no explicaremos en este curso.

Infinitud de los Números Primos

- Existe una cantidad de números primos infinita.
- En criptografía a veces es necesario encontrar números primos muy grandes.
- Eso es posible utilizando algoritmos especiales que no explicaremos en este curso.
- Lo que es importante saber en este momento es que si los necesitamos, los podemos encontrar.

Infinitud de los Números Primos

- Existe una cantidad de números primos infinita.
- En criptografía a veces es necesario encontrar números primos muy grandes.
- Eso es posible utilizando algoritmos especiales que no explicaremos en este curso.
- Lo que es importante saber en este momento es que si los necesitamos, los podemos encontrar.
- El comando que nos dice si un número (incluso muy grande) es primo, es `is_prime`. Podemos encontrar un número primo mayor que n con este ejemplo:

```
n = 2^100
while not is_prime(n):
  n = n+1
print n
```

nos dará 1267650600228229401496703205653.

Conjunto de Divisores

- El conjunto de divisores positivos de un número se puede calcular en sage mediante:

```
sage: divisors(45)
[1, 3, 5, 9, 15, 45]
```

Conjunto de Divisores

- El conjunto de divisores positivos de un número se puede calcular en sage mediante:

```
sage: divisors(45)
[1, 3, 5, 9, 15, 45]
```

- Siempre nos dará los positivos, aunque el argumento sea negativo:

```
sage: divisors(-45)
[1, 3, 5, 9, 15, 45]
```

Conjunto de Divisores

- El conjunto de divisores positivos de un número se puede calcular en sage mediante:

```
sage: divisors(45)
[1, 3, 5, 9, 15, 45]
```

- Siempre nos dará los positivos, aunque el argumento sea negativo:

```
sage: divisors(-45)
[1, 3, 5, 9, 15, 45]
```

- Como podemos ver, 1 y n siempre son divisores de n cuando $n > 0$.

Teorema Fundamental de la Aritmética

- Sea $n > 1$ un número entero. Entonces existen números primos distintos $p_1, p_2, \cdots, p_k$ y exponentes enteros positivos $\alpha_1, \alpha_2, \cdots, \alpha_k$ tales que $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.

Teorema Fundamental de la Aritmética

- Sea $n > 1$ un número entero. Entonces existen números primos distintos $p_1, p_2, \cdots, p_k$ y exponentes enteros positivos $\alpha_1, \alpha_2, \cdots, \alpha_k$ tales que $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.
- Estos números primos y exponentes son únicos salvo el orden.

Teorema Fundamental de la Aritmética

- Sea $n > 1$ un número entero. Entonces existen números primos distintos $p_1, p_2, \cdots, p_k$ y exponentes enteros positivos $\alpha_1, \alpha_2, \cdots, \alpha_k$ tales que $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.
- Estos números primos y exponentes son únicos salvo el orden.
- Encontrar la descomposición se conoce como factorización de n. Es computacionalmente muy compleja cuando n es muy grande y sus factores son a su vez grandes.

Teorema Fundamental de la Aritmética

- Sea $n > 1$ un número entero. Entonces existen números primos distintos $p_1, p_2, \cdots, p_k$ y exponentes enteros positivos $\alpha_1, \alpha_2, \cdots, \alpha_k$ tales que $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.
- Estos números primos y exponentes son únicos salvo el orden.
- Encontrar la descomposición se conoce como factorización de n. Es computacionalmente muy compleja cuando n es muy grande y sus factores son a su vez grandes.
- Como podemos ver 1 no puede ser primo, porque si no haría que la unicidad de la descomposición dada en este teorema fuera falsa.

Factorización en sage

Podemos factorizar con el comando `factor` del siguiente modo:

```
sage: factor(3^10-1)
2^3 * 11^2 * 61
```

Máximo Común Divisor

- Sean a y b dos números enteros y $D(a), D(b)$ los divisores positivos de cada uno de ellos.

Máximo Común Divisor

- Sean a y b dos números enteros y $D(a), D(b)$ los divisores positivos de cada uno de ellos.
- Llamaremos máximo común divisor al más grande de los elementos comunes a ambos conjuntos, o lo que es lo mismo, al elemento más grande de $D(a) \cap D(b)$.

Máximo Común Divisor

- Sean a y b dos números enteros y $D(a), D(b)$ los divisores positivos de cada uno de ellos.
- Llamaremos máximo común divisor al más grande de los elementos comunes a ambos conjuntos, o lo que es lo mismo, al elemento más grande de $D(a) \cap D(b)$.
- Por ejemplo, los divisores de 24 son $[1, 2, 3, 4, 6, 8, 12, 24]$ y los de 16 son $[1, 2, 4, 8, 16]$. El máximo común divisor de ambos es 8.

Números Coprimos

- Como el 1 divide a cualquier número, sabemos que 1 siempre es divisor común de a y b.

Números Coprimos

- Como el 1 divide a cualquier número, sabemos que 1 siempre es divisor común de a y b.
- En algunos casos, 1 es el único divisor común de dichos números, en ese caso diremos que a y b son números comprimos.

Números Coprimos

- Como el 1 divide a cualquier número, sabemos que 1 siempre es divisor común de a y b.
- En algunos casos, 1 es el único divisor común de dichos números, en ese caso diremos que a y b son números comprimos.
- Esto puede suceder aunque ninguno de los dos números sea primo.

Números Coprimos

- Como el 1 divide a cualquier número, sabemos que 1 siempre es divisor común de a y b.
- En algunos casos, 1 es el único divisor común de dichos números, en ese caso diremos que a y b son números comprimos.
- Esto puede suceder aunque ninguno de los dos números sea primo.
- Por ejemplo, los divisores de 15 son $[1, 3, 5, 15]$ y los de 16 son $[1, 2, 4, 8, 16]$ y como podemos ver, el 1 es el único elemento común a ambos conjuntos.

Cálculo del Máximo Común Divisor

- El algoritmo que sirve para calcular el máximo común divisor de dos números se denomina Algoritmo de Euclides.

Cálculo del Máximo Común Divisor

- El algoritmo que sirve para calcular el máximo común divisor de dos números se denomina Algoritmo de Euclides.
- No lo vamos a ver, pero es muy sencillo de programar y muy eficiente.

Cálculo del Máximo Común Divisor

- El algoritmo que sirve para calcular el máximo común divisor de dos números se denomina Algoritmo de Euclides.
- No lo vamos a ver, pero es muy sencillo de programar y muy eficiente.
- Nosotros simplemente usaremos el comando `sage` que nos da el resultado. Este comando es `gcd`

```
sage: gcd(3885,630)
105
```

Algoritmo de Euclides Extendido

- Sean a y b dos números enteros y d su máximo común divisor, entonces existen valores enteros u y v tales que

$$d = au + bv$$

Algoritmo de Euclides Extendido

- Sean a y b dos números enteros y d su máximo común divisor, entonces existen valores enteros u y v tales que

$$d = au + bv$$

- El cálculo de estos valores se puede hacer con el algoritmo de Euclides extendido.

Algoritmo de Euclides Extendido

- Sean a y b dos números enteros y d su máximo común divisor, entonces existen valores enteros u y v tales que

$$d = au + bv$$

- El cálculo de estos valores se puede hacer con el algoritmo de Euclides extendido.
- En sage se pueden obtener estos valores con el comando `xgcd`

```
sage: xgcd(3885,630)
(105, 1, -6)
```

Algoritmo de Euclides Extendido

- Sean a y b dos números enteros y d su máximo común divisor, entonces existen valores enteros u y v tales que

$$d = au + bv$$

- El cálculo de estos valores se puede hacer con el algoritmo de Euclides extendido.
- En sage se pueden obtener estos valores con el comando `xgcd`

```
sage: xgcd(3885,630)
(105, 1, -6)
```

- Este comando nos devuelve tres valores, el primero es el máximo común divisor, el segundo es el coeficiente u y el tercero el coeficiente v.

Algoritmo de Euclides Extendido

- Sean a y b dos números enteros y d su máximo común divisor, entonces existen valores enteros u y v tales que

$$d = au + bv$$

- El cálculo de estos valores se puede hacer con el algoritmo de Euclides extendido.
- En sage se pueden obtener estos valores con el comando `xgcd`

```
sage: xgcd(3885,630)
(105, 1, -6)
```

- Este comando nos devuelve tres valores, el primero es el máximo común divisor, el segundo es el coeficiente u y el tercero el coeficiente v.
- Podemos comprobar que $105 = 3885 \cdot 1 + 630 \cdot (-6)$

Teorema de Bezout

- Esta propiedad del máximo común divisor la usaremos casi siempre para el caso de números coprimos.

Teorema de Bezout

- Esta propiedad del máximo común divisor la usaremos casi siempre para el caso de números coprimos.
- En el caso de números coprimos la propiedad es incluso más fuerte y se conoce como Teorema de Bezout.

Teorema de Bezout

- Esta propiedad del máximo común divisor la usaremos casi siempre para el caso de números coprimos.
- En el caso de números coprimos la propiedad es incluso más fuerte y se conoce como Teorema de Bezout.
- El teorema dice que dos números a y b son coprimos si y sólo si existen valores u y v tales que $1 = au + bv$.

Teorema de Bezout

- Esta propiedad del máximo común divisor la usaremos casi siempre para el caso de números coprimos.
- En el caso de números coprimos la propiedad es incluso más fuerte y se conoce como Teorema de Bezout.
- El teorema dice que dos números a y b son coprimos si y sólo si existen valores u y v tales que $1 = au + bv$.
- El cálculo lo haremos con `xgcd`.