1 Números enteros

1.1 Operaciones

Pretendemos precisar nuestro conocimiento intuitivo de los números enteros, lo denotamos por $\mathbf{Z}$ (del alemán *Zahl* número).

Definición 1 *Los números enteros admiten tres operaciones:*
la suma, denotada $x + y$
la resta $x - y$
y el producto xy

Propiedades

1. Propiedades asociativas: $(x + y) + z = x + (y + z)$ y $(xy)z = x(yz)$.
2. Propiedades conmutativas: $x + y = y + x$ y $xy = yx$.
3. Existencia de elementos neutros: $x + 0 = x$ y $x1 = x$
4. Existencia de opuesto: $x + (-x) = 0$.
5. Propiedad distributiva: $x(y + z) = xy + xz$.

Entonces decimos que $\mathbf{Z}$ es un **anillo conmutativo**.

Otras propiedades

1. **Dominio de integridad**: Si a, b son enteros, y $a \neq 0$, $b \neq 0$ entonces $ab \neq 0$.
2. Como consecuencia:

   Propiedad cancelativa: Para cualesquiera $a, b, c \in \mathbf{Z}$ con $c \neq 0$, si $ac = bc$ entonces $a = b$.
3. Multiplicación por a es una aplicación inyectiva:

$$f : \mathbf{Z} \to \mathbf{Z},$$

$$x \to xa$$

1.2 Orden total

Ley de tricotomía. Para dos números enteros cualesquiera x, y se tiene:

$$x < y, x = y \text{ ó } y < x$$

Relación con las operaciones.

1. Si $x_1 \leq x_2$ y $y_1 \leq y_2$, entonces $x_1 + y_1 \leq x_2 + y_2$.
2. Si $x \leq y$ y $z > 0$, entonces $zx \leq zy$.

1.3 Los números naturales

Destacamos el conjunto de los números enteros no negativos

$$\mathbf{N} = \{0, 1, 2, \ldots\}$$

a sus elementos los llamamos **números naturales**.

Principio de buena ordenación. Cada subconjunto no vacío de números naturales tiene un elemento mínimo, i.e. un elemento más pequeño que cualquiera del subconjunto.

Principio de inducción

Teorema 1 *Sea S es un subconjunto del conjunto $\mathbf{N}$ de los números naturales verificando que*
a) $0 \in S$,
b) para todo $n \in \mathbf{N}$, si $n \in S$ entonces $n + 1 \in S$,
(o bien b') para todo $n \in \mathbf{N}$ si $m \in S$ para cada $m < n$, entonces $n \in S$)
necesariamente $S = \mathbf{N}$

Demostración. Sea S' el complementario de S en $\mathbf{N}$. Entonces por el principio de buena ordenación S' tiene un elemento mínimo m. Pero $m \neq 0$ pues $0 \notin S'$ y como $m \notin S$, $m-1 \notin S$, i.e. $m-1 \in S'$ contradicción.

Demostración por inducción

Sea $P(n)$ una proposición relativa a un número natural n. Si queremos demostrar $P(n)$ para todo número natural n bastará:

1. probar $P(0)$,
2. probar que si suponemos que $P(n)$ es cierta entonces $P(n+1)$ es cierta.

   o bien

3. probar que si suponemos que $P(m)$ es cierta para todo $m < n$, entonces $P(n)$ es cierta.

2 Divisibilidad

2.1 Algoritmo de Euclides

Definición 2 *Dados dos números enteros $a, b \in \mathbf{Z}$, decimos que b divide a a, escribiremos $b|a$ si $a = bq$ para algún $q \in \mathbf{Z}$*

Proposición 1 *Divisibilidad en $\mathbf{Z}$ satisface las propiedades siguientes:*

1. *$c|b$ y $b|a$ implica que $c|a$.*
2. *$a|a$ para todo $a \in \mathbf{Z}$.*
3. *Si $a|b$ y $b|a$, entonces $a = \pm b$.*
4. *Si $b|a_1$ y $b|a_2$, entonces $b|a_1 - a_2$.*
5. *Si $b|a$ entonces $b|ac$ para cualquier $c \in \mathbf{Z}$.*

Teorema 2 *(División de enteros) Dados $a, b \in \mathbf{Z}$, si $b > 0$ existen $q, r \in \mathbf{Z}$ tales que*

$$a = bq + r, 0 \leq r < b$$

Demostración. Tomamos q el entero más grande no mayor que a/b, entonces $0 \leq (a/b) - q < 1$ entonces $r = a - bq$ satisface la desigualdad.

Definición 3 *Un número primo es un entero p mayor que 1 cuyos únicos divisores positivos son 1 y p.*

Definición 4 *Un número entero d es un máximo común divisor de a, b si*

1. *es un divisor común de a y b, i.e. $d|a$ y $d|b$; y*
2. *si e es otro divisor común entonces $e|d$.*

Si d es un máximo común divisor, entonces $-d$ también los es. Por el máximo común divisor entenderemos el positivo.

Definición 5 *Dos números enteros se llaman primos relativos si su máximo comun divisor es uno.*

El algoritmo siguiente ya aparece en el famoso libro de Euclides, Elementos, Libro VII, Proposición 2.

Teorema 3 *(Algoritmo de Euclides.) Dados dos números enteros positivos a y b, aplicamos el algoritmo de la división repetidamente para obtener*

$$\begin{array}{rcl} a & = & bq_1 + r_1 \\ b & = & r_1 q_2 + r_2 \\ r_1 & = & r_2 q_3 + r_3 \\ & \vdots & \\ r_{n-2} & = & r_{n-1} q_n + r_n \\ r_{n-1} & = & r_n q_{n+1} + 0 \end{array}$$

entonces r_n es el máximo común divisor de a y b.

Además se verifica la **identidad de Bezout**

$$mcd(a, b) = ax + by$$

para algunos enteros x, y.

Demostración

Probaremos que r_n es el máximo común divisor y que $r_n = ax + by$ (Identidad de Bezout) para algunos enteros x, y.

Si $n = 0$ entonces $b|a$ y el resultado es trivial.

Si $n = 1$, entonces el algoritmo de Euclides para a y b tiene la forma

$$a = bq_1 + r_1$$
$$b = r_1 q_2 + 0$$

Entonces es fácil ver que r_1 es el máximo común divisor de a y b; también $r_1 = a \cdot 1 + b(-q)$ y la identidad de Bezout se verifica.

Supongamos que el teorema es cierto para $n-1$. Para el caso n el algoritmo toma la forma anterior.

Si eliminamos la primera ecuación, obtendríamos un algoritmo de Euclides para $n-1$, por hipótesis de inducción

$$r_n = (b, r_1)$$

y la identidad de Bezout sería

$$r_n = bu + r_1 v.$$

Ahora $a = bq_1 + r_1$, entonces $(a, b) = (b, r_1) = r_n$.

Como $r_1 = a - bq_1$, sustituyendo en $r_n = bu + r_1 v$

$$r_n = bu + (a - bq_1)v = av + b(u - q_1 v).$$

2.2 Consecuencias de la identidad de Bezout

Corolario 1 *Si $x|a$ y $x|b$, entonces $x|(a, b)$.*

Corolario 2 *Si $a|bc$ y $(a, b) = 1$, entonces $a|c$.*

Demostración. De la identidad de Bezout, sabemos que

$$ar + bs = 1$$

para enteros r, s.

Multiplicando por c,

$$acr + bcs = c.$$

Como $a|bc$ divide a bcs y por tanto $a|c$.

2.3 Ecuaciones de la forma $ax + by = e$

Proposición 2 *Dados enteros a, b, e, existen enteros m y n con $am+bn = e$ si y sólo si (a, b) divide a e.*

Demostración. Si $am + bn = e$ para algunos enteros m, n, entonce el máximo común divisor de a y b divide a e.

Recíprocamente la identidad de Bezout nos da $ar + bs = d$. Si $dm = e$ para algún m, entonces $x = rm$, $y = sm$ resuelve la ecuación $ax + by = e$.

3 Factorización

3.1 Números primos

Definición 6 *Un número primo es un entero p mayor que 1 cuyos únicos divisores positivos son 1 y p.*

Denotaremos por $\pi(x)$ el número de primos menores que x.

Teorema 4 *(J. Hadamard y Ch. J. de la Vallé Poussin)*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/lnx} = 1$$

3.1.1 Algunas conjeturas

Muchos primos aparecen por parejas: 3 y 5, 17 y 19, 29 y 31. Se denominan **primos gemelos**.

Conjetura 1 *¿Existen infinitas parejas de primos gemelos, i.e. de la forma n y $n + 2$?*

Conjetura 2 *(C.H. Goldbach, 1742) Cada número par es suma de dos números primos.*

Teorema 5 *(I.M. Vinogradov, 1937) Los números impares suficientes grandes pueden escribirse como suma de tres primos.*

Para más infomación http://primes.utm.edu/

3.2 Factorización

Lema 1 *Cada entero positivo puede escribirse como producto de primos.*

Demostración. Lo demostraremos por inducción.

Primero, 2 es primo.

Supongamos que el resultado es cierto para para cada entero positivo menor que n.

Si n es primo entonces hemos terminado. En caso contrario, $n = xy$ con $x, y < n$ por la hipótesis de inducción x e y se escriben como producto de primos.

Así n también es producto de primos.

Unicidad

Lema 2 *Si p es un número primo y $a_1, a_2, \ldots, a_n \in \mathbf{Z}$ tales que*

$$p | a_1 a_2 \cdots a_n,$$

entonces $p | a_i$ para algún $i = 1, \ldots n$.

Demostración. Probaremos el contrarecíproco de esta afirmación,i.e. si $p \not| a_i$ para todo $i = 1, \ldots n$ entonces $p \not| a_1 a_2 \ldots a_n$.

Para el caso $n = 1$ no hay que probar.

Supongamos $n = 2$. Debemos probar si $p \not| a$, $p \not| b$ entonces $p \not| ab$.

Como p es primo, a, p son primos relativos, entonces la identidad de Bezout nos dice que $ax + py = 1$ para algunos $x, y \in \mathbf{Z}$, análogamente $bu + pv = 1$.

Multiplicando ambas igualdades

$$1 = (ax + py)(bu + vp) = abxu + p(ybu + axv + ypv)$$

y esto demuestra que ab y p son primos relativos, por tanto $p \not| ab$.

Supongamos que $n > 2$ y el resultado cierto para valores menores que n.

Dado un primo p tal que $p \not| a_i$ para todo $i = 1, \ldots n$, usando la hipótesis de inducción $p \not| a_1 \cdots a_{n-1}$.

Como también $p \not| a_n$, el caso n=2 nos demuestra que $p \not| a_1 \cdots a_n$.

Teorema 6 *Cada entero positivo a puede escribirse como producto de números primos* $a = p_1 p_2 \ldots p_r$.

Además, si tenemos otra factorización $a = q_1 q_2 \ldots q_s$, *entonces*
$r = s$
y reordenando convenientemente los q_i *se tiene que* $p_i = q_i$.

Demostración Si tenemos

$$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

Entonces $p_1 | q_1 \cdots q_s$, por el lema anterior $p_1 | q_i$ para algún i.
Renumerando podemos suponer que $p_1 | q_1$. Como q_1 es primo, $p_1 = q_1$.
Simplificamos p_1

$$p_2 \cdots p_r = q_2 \cdots q_s$$

Aplicando inducción sobre r se sigue que $r - 1 = s - 1$ y reordenando $p_i = q_i$ para $i = 2 \ldots n$. Así $r = s$ y $p_i = q_i$ para $i = 1, \ldots, n$.

Teorema 7 *(Teorema de Euclides) Existen infinitos números primos*

Demostración. Supongamos que existieran sólo un número finito, digamos que $p_1, p_2, \ldots, p_r$ son todos los que hay.

Consideremos el número $m = p_1 p_2 \cdots p_r + 1$.

Tendrá que tener un divisor primo, q. Entonces q será uno de los que existen $p_1, p_2, \ldots, p_r$, por tanto divide a $p_1 p_2 \cdots p_r$ y como dividía a m dividirá a 1.

Pero esto es una contradicción.

4 Congruencias

4.1 Propiedades elementales

Introducidas por Gauss en su libro *Disquisitiones Arithmeticae* (1801).

Definición 7 *Dos enteros* a, b *son congruentes módulo* m, *escribimos*

$$a \equiv b \ (mod\ m)$$

si m *divide a* $a - b$, *o equivalentemente* $a = b + km$ *para algún* $k \in \mathbf{Z}$.

Proposición 3 *Sea m un número natural > 1. Cada número entero es congruente con m exactamente a un número del conjunto $\{0, 1, \ldots, m-1\}$*

Teorema 8 *Sea m un entero positivo. Entonces la relación de congruencia mod m es una relación de equivalencia en $\mathbf{Z}$. Además*
1) si $a \equiv b$ and $a' \equiv b'$ (mod m) entonces $a + a' \equiv b + b'$ (mod m),
2) si $a \equiv b$ and $a' \equiv b'$ (mod m) entonces $aa' \equiv bb'$ (mod m),
3) si $ca \equiv cb$ (mod m) y c es primo con m, entonces $a \equiv b$ (mod m),
4) si $a \equiv b$ (mod km) y $k \neq 0$, entonces $a \equiv b$ (mod m).

Demostración 3) Supongamos $ca \equiv cb \pmod{m}$, como c y m son primos relativos, por la identidad de Bezout $uc + vm = 1$ con u, v números enteros, i.e. $uc \equiv 1 \pmod{m}$.

Entonces $auc \equiv a$, $buc \equiv b \pmod{m}$. Multiplicando la equivalencia dada por u se sigue que $uca \equiv ucb \pmod{m}$. Por tanto $a \equiv auc \equiv buc \equiv b$ (mod m).

Proposición 4 *Sean a y b dos números naturales entonces a es congruente a b módulo m si ambos dan el mismo resto al dividirlos por m*

Demostración. Si $a = q_1 m + r$ y $b = q_2 m + r$, entonces $a - b = (q_1 - q_2)m$, así $a \equiv b \pmod{m}$.

Recíprocamente si $a \equiv b \pmod{m}$, entonces $a = b + km$. Si $b = qm + r$, se sigue que $a = qm + r + km = (q + k)m + r$ y ambos dan el mismo resto al dividirlos por m.

Prueba de los nueves

Apareció en Europa en el libro Liber Abaci (1202) de Fibonacci

Lema 3 *Sea x un entero positivo, 9 divide a x si y sólo si x divide a las suma de las cifras de x.*

Demostración. Observamos que $10^r \equiv 1 \pmod{9}$ para todo $r > 0$. Entonces

$$x = x_n 10^n + x_{n-1} 10^{n-1} + \ldots + x_2 10^2 + x_1 10 + x_0$$

$$\equiv x_n + x_{n-1} + \ldots + x_2 + x_1 + x_0$$

Proposición 5 *La ecuación $ax \equiv 1 \pmod m$ tiene solución si y sólo si a y m son primos relativos.*

Demostración. La ecuación es equivalente a $ax = 1+km$, o $ax-km = 1$ y aplicamos la Proposición 2 de la lección 7.

4.2 Clases de restos

La relación de congruencia módulo m es una relación de equivalencia, sus clases de equivalencia son la clases de restos módulo m, las denotamos $\overline{a}$. Entonces el conjunto cociente lo denotamos

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

En este conjunto cociente se pueden definir las operaciones suma y producto.

$$\overline{a} + \overline{b} = \overline{a+b}$$

$$\overline{a} \cdot \overline{b} = \overline{ab}.$$

Supongamos que $\overline{a} = \overline{a}'$, $\overline{b} = \overline{a}'$, entonces $a \equiv a'$ y $b \equiv b' \pmod m$. Se sigue que $a + b \equiv a' + b'$, i.e. $\overline{a+b} = \overline{a' + b'}$.

Análogamente para el producto.

El conjunto $\mathbf{Z}$/m$\mathbf{Z}$ se denomina el **anillo de enteros módulo** m.

Definición 8 *Un elemento de un anillo u se dice que es una* **unidad** *si existe un elemento v tal que $uv = vu = 1$, a v se le denomina el inverso de u y se denota u^{-1}.*

Teorema 9 *En $\mathbf{Z}/m\mathbf{Z}$, $\overline{a}$ es una una unidad si y sólo si a y m son primos relativos.*

Demostración. $\overline{a}\overline{b} = 1$ es equivalente a $uv \equiv 1 \pmod m$.

Corolario 3 *El número de unidades de $\mathbf{Z}/m\mathbf{Z}$ es igual al número de enteros x, $1 \leq x \leq a$ que son primos relativos con m.*

El número de enteros x, $1 \leq x \leq a$ que son primos relativos con m se denota $\phi(x)$, la función fi de Euler.

Corolario 4 *Si p es primo, todos los elementos no cero de $\mathbf{Z}/p\mathbf{Z}$ son unidades, i.e. es un cuerpo.*

En particular $\phi(p) = p - 1$.
No es dificil ver que

$$\phi(p^r) = p^r - p^{r-1} = p^r(1 - \frac{1}{p}).$$

5 Teoremas de Fermat y Euler

5.1 Ordenes de elementos

Proposición 6 *Si a y m son primos relativos, entonces $a^t \equiv 1$ para algún t, $1 \leq t < m$.*

Demostración. Como a y m son primos relativos, m no divide a a^s para cualquier s. Así los números

$$1, a, a^2, \ldots, a^{m-1}$$

pertenecen a clases de restos distintos de la $\overline{0}$. Por tanto dos de ellos deben de estar en la misma clase, i.e.

$$a^s \equiv a^{s+t}$$

donde $s \geq 0$ y $0 \leq t < m - 1$. Ahora como a y m son primos relativos, podemos simplificar a^s de ambos términos de la igualdad, se obtiene

$$1 \equiv a^t \ (mod\ m).$$

Definición 9 *Sea $m \geq 2$ and a un entero primo relativo con m. El* **orden** *de a módulo m es el menor entero positivo e tal que $a^e \equiv 1$ (mod m).*

Proposición 7 *Si e es el orden de un módulo m, y $a^f \equiv 1$ (mod m), entonces e divide f.*

Demostración. Tenemos $a^e \equiv 1$ y $a^f \equiv 1 \pmod{m}$. Dividimos f entre e, i.e. $f = eq + r$ con $0 \leq r < e$. Entonces

$$1 \equiv a^f \equiv (a^e)^q a^r \equiv a^r,$$

por tanto $a^r \equiv 1$, pero e era el menor natural tal que $a^e \equiv 1 \pmod{m}$, por tanto $r = 0$ y e divide a f.

5.2 Teorema de Fermat

Fue descubierto por P. Fermat en 1640.

Teorema 10 *Si p es un primo y a es un entero no divisible por p, entonces*

$$a^{p-1} \equiv 1 \ (mod\ p).$$

Demostración. Sea $\overline{a} \neq \overline{0}$ la clase de restos de a módulo p. Multiplicación por $\overline{a}$ es una aplicación inyectiva de $\mathbf{Z}/p\mathbf{Z}$, i.e. la aplicación $\mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$, enviando $\overline{x} \to \overline{ax}$ es inyectiva. Como son conjuntos finitos la aplicación tiene que ser biyectiva, es decir,

$$\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\} = \{\overline{a} \times \overline{1}, \overline{a} \times \overline{2}, \ldots, \overline{a} \times \overline{p-1}\}.$$

Al multiplicar ambos conjuntos tendremos el mismo resultado

$$\overline{1} \times \overline{2} \times \cdots \times \overline{p-1} = \overline{a} \times \overline{1} \times \overline{a} \times \overline{2} \times \cdots \times \overline{a} \times \overline{p-1}.$$

Podemos simplificar $\overline{1} \times \overline{2} \times \cdots \times \overline{p-1}$ para obtener

$$\overline{1} = (\overline{a})^{p-1}$$

si se translada esta acuación a congruencias obtenemos el resultado del teorema.

5.3 Teorema de Euler

Una función definida sobre $\mathbf{Z}$ se denomina una **función aritmética**. Como por ejemplo ϕ.

Una función aritmética f se llama **multiplicativa** si

$$f(mn) = f(m)f(n)$$

cuando $(m, n) = 1$.

Teorema 11 *La función ϕ es multiplicativa.*

Demostración. Como $\phi(1) = 1$ la ecuación es cierta para $n = 1$ o $m = 1$. Podemos suponer que $n > 1$ y $m > 1$. Escribimos los restos módulo nm en una tabla de la forma siguiente

$$\begin{array}{ccccc}
0 & 1 & 2 & \dots & m-1 \\
m & m+1 & m+2 & \dots & m+(m-1) \\
2m & 2m+1 & 2m+2 & \dots & 2m+(m-1) \\
 & & \vdots & & \\
(n-1)m & (n-1)m+1 & (n-1)m+2 & \dots & (n-1)m+(m-1)
\end{array}$$

La primera fila incluye todos los posibles restos módulo m. Habrá $\phi(m)$ elementos primos con m. Por otro lado una fila arbitraria de la tabla anterior es congruente con la primera módulo m. Por tanto cada fila contiene $\phi(m)$ elementos primos con m. Habrá $\phi(m)$ columnas formadas completamente por enteros primos con m.

Una columna arbitraria es de la forma

$$b, m + b, 2m + b, \dots, (n - 1)m + b.$$

Claramente estos forman un conjunto con todos los restos posibles módulo n. Efectivamente hay $n - 1$ números positivos y dos de ellos no pueden dar el mismo resto módulo n pues si

$$im + b \equiv jm + b\,(mod\,n)$$

se tendría

$$im \equiv jm\,(mod\,n)$$

y como m es primo con n se puede simplificar dando $i = j$, pues ambos son menores que n. Así en cada columna hay $\phi(n)$ números primos con n. En total tendremos en la tabla $\phi(n)\phi(m)$ números que son primos con n y con m. Pero como n y m son primos relativos, esto es lo mismo que decir que esos números son primos con nm. Se tiene

$$\phi(n)\phi(m) = \phi(nm).$$

Teorema 12 *Para cada $n > 1$ se tiene que*

$$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p})$$

donde el producto significa que multiplicamos sobre todos los primos que dividen a n.

bf Demostración. Sea $n = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_k^{a_k}$ aplicando ϕ y teniendo en cuenta que ϕ es multiplicativa

$$\phi(n) = \phi(p_1^{a_1}) \times \phi(p_2^{a_2}) \times \cdots \times \phi(p_k^{a_k})$$

Ahora bien como hemos visto

$$\phi(p^r) = p^r(1 - \frac{1}{p})$$

así se obtiene que

$$\phi(n) = p^{a_1}(1 - \frac{1}{p_1}) \times p^{a_2}(1 - \frac{1}{p_2}) \times \cdots \times p^{a_r}(1 - \frac{1}{p_r})$$

Agrupando términos se tiene

$$\phi(n) = (p^{a_1} \times p^{a_2} \times \cdots \times p^{a_r}) \times (1 - \frac{1}{p_1}) \times (1 - \frac{1}{p_2}) \times \cdots \times (1 - \frac{1}{p_r})$$

la fórmula buscada.

Teorema 13 *Teorema de Euler Si $(a, m) = 1$, entonces*

$$a^{\phi(m)} \equiv 1 \, (mod \, m).$$

Demostración. La idea es similar a la demostración del teorema de Fermat. En esta ocasión tenemos que tomar el conjunto de las unidades de $\mathbf{Z}/m\mathbf{Z}$. Sabemos que hay sólo $\phi(m)$ de tales unidades, i.e

$$U = \{\overline{u_1}, \ldots, \overline{u_{\phi(m)}}\}.$$

Por la misma razón que en el teorema de Fermat si multiplicamos por $\overline{a}$. Entonces

$$U = \{\overline{au_1}, \ldots, \overline{au_{\phi(m)}}\}.$$

Si multiplicamos los elementos de ambos conjuntos

$$\overline{u_1} \times \cdots \times \overline{u_{\phi(m)}} = \overline{au_1} \times \cdots \times \overline{au_{\phi(m)}}.$$

Simplificando de nuevo por $\overline{u_1} \times \cdots \times \overline{u_{\phi(m)}}$, esto se puede hacer pues es una unidad, se sigue que

$$\overline{1} = \overline{a}^{\phi(m)}.$$

Esta igualdad es equivalente a la igualdad de congruencias que establece el enunciado.