Notas preparatorias: números y divisibilidad

1 Divisivilidad de números enteros

- Dados dos números enteros a y b, decimos que b *divide* a a, o que b es un *divisor de* a, o que a es *múltiplo de* b si existe un número entero c tal que $a = b \cdot c$. Se denota $b|a$.
- Un número entero $p > 1$ se dice *primo* si sus únicos divisores positivos son 1 y p.
- Dados dos números enteros a y $b > 0$, existen dos enteros únicos q y r tales que $0 \leq r < b$ y $a = bq + r$. Los enteros q y r se llaman respectivamente el *cociente* y el *resto* de la división euclídea de a entre b. a es un múltiplo de b si y sólo si $r = 0$.
- Dados dos enteros a y b, su *máximo común divisor* es el mayor entero positivo d que divide a ambos. Se puede calcular mediante el algoritmo de Euclides: comenzamos dividiendo a entre b, obteniendo un cociente q_1 y un resto r_1. Si $r_1 = 0$, el m.c.d. es b. Si no, dividimos b entre r_1, obteniendo un cociente q_2 y un resto r_2. Si $r_2 = 0$, el m.c.d. es r_1. Si no, continuamos hasta que obtengamos resto cero (cosa que ocurre en algún momento, ya que los restos son cada vez menores). El último resto no nulo que hayamos obtenido es el m.c.d. Dos enteros de dicen *primos entre sí* si su m.c.d. es 1 (es decir, si no tienen ningún divisor común mayor que 1).
- Dados dos enteros a y b, su *mínimo común múltiplo* es el menor entero positivo m que es múltiplo de ambos. Si d es el m.c.d. de a y b, se tiene que $|a \cdot b| = d \cdot m$.
- (**Identidad de Bézout**) Dados dos enteros a y b con m.c.d. d, existen enteros x e y tales que $ax + by = d$. Para hallarlos, basta con recorrer hacia atrás el algoritmo de Euclides usado para hallar d.
- Todo número entero positivo se puede expresar, de manera única, como producto de primos: $n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$.
- Si a, b, c son números enteros tales que $a|bc$ y a y b son primos entre sí, entonces $a|c$. En particular, si p es primo y $p|bc$, o bien $p|b$ o bien $p|c$.

2 Congruencias

- Sea m un entero positivo. Dos enteros a, b se dicen *congruentes módulo* m (denotado $a \equiv b \bmod m$) si $m|a - b$.

- Si $a \equiv b$ y $c \equiv d \bmod m$, entonces $a + c \equiv b + d$ y $ac \equiv bd \bmod m$.

- Todo entero a es congruente módulo m a un único entero $\bar{a}$ entre 0 y $m-1$ (que es simplemente el resto de la división de a entre m). $\bar{a}$ se denomina el *residuo* de a módulo m.

- (**Función phi de Euler**) Dado un entero positivo n, denotamos por $\phi(n)$ el número de entero entre 1 y $n-1$ que sean primos con n. Si $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ es su descomposición en factores primos, se tiene que $\phi(n) = p_1^{a_1-1} p_2^{a_2-1} \cdots p_r^{a_r-1}(p_1-1)(p_2-1)\cdots(p_r-1)$. En particular, $\phi(p) = p-1$ si p es primo.

- (**Pequeño teorema de Fermat**) Si a y $n > 0$ son dos entero primos entre sí, se tiene que $a^{\phi(n)} \equiv 1 \bmod n$. En particular, si p es primo, $a^p \equiv a \bmod p$ para todo entero a.

- (**Teorema chino del resto**) Sean $m_1, \ldots, m_r$ enteros positivos primos entre sí dos a dos, y $a_1, \ldots, a_r$ enteros cualesquiera. Entonces, existe un entero a tal que $a \equiv a_i \bmod m_i$ para todo $i = 1, \ldots, r$. Además, cualquier otro entero b que cumpla esta condición es congruente con a módulo $m = m_1 m_2 \cdots m_r$. Por ejemplo, las congruencias

$$a \equiv 1 \bmod 3$$

$$a \equiv 2 \bmod 5$$

$$a \equiv 3 \bmod 4$$

  tienen la solución $a = 7$, y cualquier otra solución es congruente con 7 módulo 60.

- Si p es un primo, un entero $\bar{a}$ entre 1 y $p-1$ se dice un *residuo cuadrático* módulo p si existe un entero b tal que $b^2 \equiv a \bmod p$. Si $p > 2$ exactamente la mitad de los $p-1$ residuos módulo p son residuos cuadráticos.

3 Polinomios

- Dados dos polinomios $a(x)$ y $b(x)$, decimos que $b(x)$ *divide a* $a(x)$, o que $b(x)$ es un *divisor de* $a(x)$, o que $a(x)$ es *múltiplo de* $b(x)$ si existe un polinomio $c(x)$ tal que $a(x) = b(x) \cdot c(x)$. Se denota $b(x)|a(x)$.

- Un polinomio $p(x)$ no constante se dice *irreducible* si no se puede expresar como producto de dos polinomios de menos grado.

- Dados dos polinomios $a(x)$ y $b(x)$, existen únicos polinomios $q(x)$ y $r(x)$ tales que el grado de $r(x)$ es menor que el de $b(x)$ y $a(x) = b(x)q(x) + r(x)$. Los polinomios $q(x)$ y $r(x)$ se llaman respectivamente el *cociente* y el *resto* de la división euclídea de $a(x)$ entre $b(x)$. $a(x)$ es un múltiplo de $b(x)$ si y sólo si $r(x) = 0$.

4 Progresiones

- Una *progresión aritmética* es una sucesión infinita de números $a_1, a_2, \ldots, a_n, \ldots$ tales que la diferencia entre dos términos consecutivos es constante: $a_{n+1} - a_n = r$ para todo n. Entonces se tienen las fórmulas $a_n = a_1 + r(n-1)$ y $a_1 + \cdots + a_n = na_1 + \frac{rn(n-1)}{2}$.
- Una *progresión geométrica* es una sucesión infinita de números $a_1, a_2, \ldots, a_n, \ldots$ no nulos tales que el cociente entre dos términos consecutivos es constante: $a_{n+1}/a_n = r$ para todo n. Entonces se tienen las fórmulas $a_n = a_1 \cdot r^{n-1}$ y, si $r \neq 1$, $a_1 + \cdots + a_n = a_1 \frac{r^n - 1}{r-1}$.

5 Principio de inducción

El principio de inducción es un método para probar que una propiedad se verifica para todo número natural n. Supongamos que la propiedad se verifica para $n = 1$, y que, a partir de la hipótesis de que se verifica para un cierto n podemos deducir que se verifica también para $n + 1$. Entonces la propiedad se verifica para todo número natural n (porque a partir de la propiedad para $n = 1$ se verificaría para $n = 2$, de ahí para $n = 3$, y así sucesivamente). Veamos, por ejemplo, cómo probar de esta forma que $1 + r + \cdots + r^n = \frac{r^{n+1}-1}{r-1}$ para todo número real r y para todo número natural n:

- Para $n = 1$ es cierto, ya que $1 + r = \frac{r^2-1}{r-1}$.
- Partiendo de la hipótesis de que $1 + r + \cdots + r^n = \frac{r^{n+1}-1}{r-1}$ para un cierto n, sumando r^{n+1} en ambos lados obtenemos que

  $$1+r+\cdots+r^n+r^{n+1} = \frac{r^{n+1}-1}{r-1} + r^{n+1} = \frac{r^{n+1} - 1 + r^{n+1}(r-1)}{r-1} = \frac{r^{n+2}-1}{r-1}$$

  que es justamente la propiedad buscada para $n + 1$. Por tanto dicha propiedad se verifica para todo n.

6 Algunas fórmulas útiles

Sea n un entero positivo, y $n = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ su descomposición en factores primos.

- El número de divisores positivos de n es $(a_1 + 1)(a_2 + 1) \cdots (a_n + 1)$.
- La suma de los divisores positivos de n es

  $$\frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{a_r+1} - 1}{p_r - 1}$$

- El producto de los divisores positivos de n es $n^{\tau(n)/2}$, donde $\tau(n) = (a_1 + 1)(a_2 + 1) \cdots (a_n + 1)$ es el número de divisores positivos de n.

- Para todo entero $n > 0$,

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1})$$

En particular,

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$$

- Si n es impar,

$$x^n + y^n = (x+y)(x^{n-1} - x^{n-2}y + \cdots - xy^{n-2} + y^{n-1})$$

En particular,

$$x^n + 1 = (x+1)(x^{n-1} - x^{n-2} + \cdots - x + 1)$$

- (**Binomio de Newton**) Para todo entero $n > 0$,

$$(x+y)^n = x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n-2}x^2y^{n-2} + \binom{n}{n-1}xy^{n-1} + y^n$$

donde

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

son los números combinatorios. En particular, haciendo $x = y = 1$ obtenemos

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-2} + \binom{n}{n-1} + \binom{n}{n} = 2^n$$