(12) Sean $a, b, n \in \mathbb{Z}$, probar que $a \equiv b(mod\ n)$ si y sólo si $a \equiv b(mod\ -n)$.

(13) Probar que, si $a \equiv b(mod\, n)$, entonces $ac \equiv bc(mod\, n)$.

(14) Probar que, si $a \equiv b(mod\, n)$ y m es un entero no negativo. entonces $a^m \equiv b^m(mod\, n)$.

(15) Sea $n \in \mathbb{Z}$, probar que $n\mathbb{Z} = (-n)\mathbb{Z}$.

(16) Sean $a, b \in \mathbb{Z}$ no ambos cero. Probar que

$$mcd\left(\frac{a}{mcd\,(a,b)}, \frac{b}{mcd\,(a,b)}\right) = 1.$$

(17) Sean $a, b \in \mathbb{Z}$ no ambos cero. Probar que si $mcd\,(a,b) = 1$ y $a \mid bc$, entonces $a \mid c$.

(18) Probar que si $a \equiv b(mod\ m)$, entonces $al \equiv bl(mod\ ml)$.

(19) Probar que si $a \equiv b(mod\ m)$ y $l \mid m$, entonces $a \equiv b(mod\ l)$.

(20) Probar que si $a \equiv b(mod\ m)$ y d es un divisor común de a, b y m, entonces $\frac{a}{d} \equiv \frac{b}{d}(mod\ \frac{m}{d})$.

(21) Probar que si $a \equiv b(mod\ m)$, d es un divisor común de a y b y $mcd(m,d) = 1$, entonces $\frac{a}{d} \equiv \frac{b}{d}(mod\ m)$.

(22) Probar que si $a_1, .., a_k \in \mathbb{Z}$ todos distintos de cero, existen $\alpha, \beta \in \mathbb{N}$ tales que:
   (a) $\alpha \mid a_i$, $a_i \mid \beta$ para todo $i = 1, .., k$
   (b) Si $r \mid a_i$ para todo $i = 1, .., k$, entonces $\alpha \mid r$. Si $a_i \mid s$ para todo $i = 1, .., k$, entonces $s \mid \beta$.

(23) Probar que $10\mathbb{Z} \cap 24\mathbb{Z} = mcm\ (10, 24)\mathbb{Z}$.

(24) Sean $n, m \in \mathbb{Z} \setminus \{0\}$. Probar que $n\mathbb{Z} \cap m\mathbb{Z} = (mcm\ (m,n))\mathbb{Z}$.

(25) Sean $m, n \in \mathbb{Z} \setminus \{0\}$ y suponga que $mcd\ (n,m) = 1$. Probar que $mcm\ (n,m) = |nm|$.

(26) Sean $m, n \in \mathbb{Z} \setminus \{0\}$ y suponga que $mcd\ (n,m) = 1$. Probar que $n\mathbb{Z} \cap m\mathbb{Z} = n.m\mathbb{Z}$.

(27) Sean $m, n \in \mathbb{Z} \setminus \{0\}$. Entonces $mcd\ (m,n) = 1$ si y sólo si $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$.

(28) Sean $m, n \in \mathbb{Z} \setminus \{0\}$. Probar que $n\mathbb{Z} \subset m\mathbb{Z}$ si y sólo si $mcd\ (n,m) = |m|$.

(29) Sean $m, n \in \mathbb{Z} \setminus \{0\}$. Probar que $n\mathbb{Z} \cap m\mathbb{Z} = n\mathbb{Z}$ si y sólo si $mcd(m,n) = |m|$.

(30) Sean p y q números primos diferentes. Probar que $mcd\ (p,q) = 1$.

(31) Sean p y q números primos diferentes. Probar que $p\mathbb{Z} + q\mathbb{Z} = \mathbb{Z}$.

(32) Probar que $x \equiv 3(mod\ n)$ si y sólo si $x = 3 + tn$ con $t \in \mathbb{Z}$.

(33) Si $b, n \in \mathbb{Z}$, definamos $b + n\mathbb{Z} = \{b + nt : t \in \mathbb{Z}\}$. Probar que

$$\mathbb{Z} = 3\mathbb{Z} \cup (1 + 3\mathbb{Z}) \cup (2 + 3\mathbb{Z}).$$

(34) Sea $n \in \mathbb{N}$. Probar que

$$\mathbb{Z} = n\mathbb{Z} \cup (1 + n\mathbb{Z}) \cup (2 + n\mathbb{Z}) \cup ... \cup ((n-1) + n\mathbb{Z}).$$

(35) Sean $b \in \mathbb{Z}$ y $n \in \mathbb{N}$. Probar que $b + n\mathbb{Z} = \{c : c \equiv b(mod\ n)\}$.

(36) Resolver las siguientes congruencias:
(a) $59x \equiv 4\ (mod\ 14)$ (b) $3x \equiv (2\ mod\ 5)$ (c) $2x \equiv 6\ (mod\ 12)$

(37) ¿ Cúales de los enteros positivos

$$101, 10101, 1010101, ...$$

son primos?

(Sugerencia: Sea N cualquiera de los números de la lista, en el cual el numero de $1's$ es k (por ejemplo si $k = 4$, $N = 1010101$). Si M es el número que tiene k dígitos, todos iguales a 1, entonces

$$11 \cdot N = M \cdot (10^k + 1) \tag{7}$$

Muestre que:

(a) Si k es par, M es divisible por 11 y si k es impar, M no es divisible por 11.

(b) Si k es par $10^k + 1$ no es divisible por 11 pero si k es impar, $10^k + 1$ sí es divisible por 11.

(c) Concluya que si $k > 2$, ya sea impar o par, exactamente una de dos M o $10^k + 1$ es divisible por 11. Por la igualdad (7), N es divisible por el otro factor.

(d) ¿Qué pasa si $k = 2$?)

(38) Si m y n son primos relativos ¿ las congruencias simultáneas

$$x \equiv a(mod\ m),\ x \equiv b(mod\ n)$$

tienen siempre solución?

(Sugerencia: La respuesta afirmativa era conocida en China desde hace más de 2000 años. Es un caso particular de un Teorema importante en Teoría de Números, que se conoce como el Teorema Chino del Residuo y que involucra dos o más congruencias. Damos sugerencias para nuestro problema:

Como $1 = mcd(m, n)$, existen $u, v \in \mathbb{Z}$ tales que $1 = mu + nv$. Entonces: $mu = 1 - nv$, luego existe $y_0 \in \mathbb{Z}$ tal que $y_0 \equiv 0(mod\ m)$ y $y_0 \equiv 1(mod\ n)$, por tanto $by_0 \equiv 0(mod\ m)$ y $by_0 \equiv b(mod\ n)$. Por otro lado, $nv = 1 - mu$ implica que existe $z_0 \in \mathbb{Z}$ tal que $z_0 \equiv 0(mod\ n)$ y $z_0 \equiv 1(mod\ m)$, de donde, $az_0 \equiv a(mod\ m)$ y $az_0 \equiv 0(mod\ n)$. Por lo tanto $az_0 + by_0 \equiv a(mod\ m)$ y $az_0 + by_0 \equiv b(mod\ n)$.)