ÁLGEBRA I / MATEMATICA DISCRETA I
PRACTICO 6

(1) a) Calcular el resto de la división de 1599 por 39 sin tener que hacer la división.
b) Lo mismo con el resto de 914 al dividirlo por 31.

Respuestas: a) $1599 = 1600 - 1 = 40^2 - 1 = (39-1)^2 - 1$ Pero $(39-1)^2 - 1 \equiv 1^2 - 1 \equiv 1 - 1 \equiv 0(39)$ y por lo tanto el resto es cero. En efecto, $1599 = 39 * 41$. **b)** $914 = 900 + 14 = 30^2 + 14 = (31-1)^2 + 14$ y por lo tanto $914 \equiv (-1)^2 + 14 \equiv 15(31)$ y el resto es 15. En efecto $914 = 899 + 15 = 29 * 31 + 15$.

(2) Probar que todo número de la forma $4^n - 1$ es siempre divisible por 3.

Respuesta: $4^n - 1 \equiv (3+1)^n - 1 \equiv 1^n - 1 \equiv 1 - 1 \equiv 0\ (3)$.

(3) Probar que el resto de dividir n^2 por 4 es igual a cero si n es par y 1 si n es impar.

Respuesta: Si n es par luego $n = 2k$, $k \in \mathbb{N}$ y $n^2 = 4k^2 \equiv 0\ (4)$ y por lo tanto en este caso el resto es cero. Si n es impar, luego existe $k \in \mathbb{N}$ tal que $n = 2k+1$. En este caso $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 \equiv 1\ (4)$ y por lo tanto el resto es 1.

(4) Probar que si las longitudes de los lados de un triángulo rectángulo son números enteros entonces los catetos no pueden ser ambos impares.

Respuesta: Sean a, b y h las longitudes de los catetos e hipotenusa de un triángulo rectángulo, luego por el teorema de Pitágoras tenemos que $a^2 + b^2 = h^2$ Si suponemos por contradicción que ambos lados son impares y si miramos esta ecuación módulo 4 tenemos que $a^2 + b^2 \equiv 2\ (4)$ [ya que por el ejercicio anterior $a^2 \equiv b^2 \equiv 1(4)$ Pero, también por el ejercicio anterior, $h^2 \equiv 0(4)$ si h es par y $h^2 \equiv 1(4)$ si h es impar. Hemos llegado así a una contradicción $[2 = 0\ (4)$ o $2 = 1\ (4)]$ y por lo tanto ambos lados no pueden ser impares simultáneamente.

(5) Probar las reglas de divisibilidad por 2, 3, 4, 5, 6, 7, 8, 9, 11 que no hayan sido probadas en el teórico.

Respuestas: Veamos algunas; La regla de divisibilidad por 4. Escribiendo el número $m =$ "$a_N a_{N-1} \cdots a_2 a_1 a_0$" como $m = \sum_{i=0}^{N} a_i 10^i$ tenemos que el resto está dado por su equivalencia con 4, es decir, $m \equiv \sum_{i=0}^{N} a_i (8+2)^i \equiv \sum_{i=0}^{N} a_i 2^i\ (4)$. Pero $2^2 = 4 \equiv 0\ (4)$ y por lo tanto la suma termina en el segundo término: $m \equiv a_0 + 2a_1 \equiv 0\ (4)$. La regla es entonces que para que el número $m =$ "$a_N a_{N-1} \cdots a_2 a_1 a_0$" sea divisible por 4, $a_0 + 2a_1$ tiene que ser divisible por 4

La regla de divisibilidad por 9. Escribiendo el número $m =$ "$a_N a_{N-1} \cdots a_2 a_1 a_0$" como $m = \sum_{i=0}^{N} a_i 10^i$ tenemos que el resto está dado por su equivalencia con 9, es decir, $m \equiv \sum_{i=0}^{N} a_i (9+1)^i \equiv \sum_{i=0}^{N} a_i 1^i \equiv \sum_{i=0}^{N} a_i\ (9)$. La regla es entonces que para que el número $m =$ "$a_N a_{N-1} \cdots a_2 a_1 a_0$" sea divisible por 9, la suma de sus cifras tiene que ser divisible por 9. Notar que si el número obtenido en la suma es muy grande uno puede volver a aplicar la regla a este número y reducirlo así a uno menor (donde la divisibilidad sea entonces facil de estableser).

La regla de divisibilidad por 7. Escribiendo el número $m =$ "$a_N a_{N-1} \cdots a_2 a_1 a_0$" como $m = \sum_{i=0}^{N} a_i 10^i$ tenemos que el resto está dado por su equivalencia con 7, es decir, $m \equiv \sum_{i=0}^{N} a_i (7+3)^i \equiv \sum_{i=0}^{N} a_i 3^i\ (7)$. Pero $3^2 = 9 \equiv 2\ (7)$, $3^3 \equiv 3 \cdot 3^2 \equiv 3 \cdot 2 \equiv 6 \equiv -1\ (7)$, $3^4 \equiv 3 \cdot 3^3 \equiv 3 \cdot (-1) \equiv -3\ (7)$, $3^5 \equiv 3 \cdot 3^4 \equiv 3 \cdot -3 \equiv -9 \equiv -2\ (7)$, y $3^6 \equiv 3 \cdot 3^5 \equiv 3 \cdot -2 \equiv -6 \equiv 1\ (7)$ donde vemos que el ciclo comienza a repetirse, luego tenemos que la condición es: $a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + \cdots \equiv 0\ (7)$.

(6) Decir por cuáles de los números del 2 al 11 son divisibles los siguientes números:
a) 12342 b) 5176 c) 314573 d) 899

Respuestas: Aplique las reglas de divisibilidad encontradas en el ejercicio anterior.

(7) Hallar los restos posibles en la división de n^2 por 3.

Respuesta: Todo número entero se puede escribir como $n = 3k + r$, con $0 \leq r < 3$ para algún $k \in \mathbb{N}$. En el primer caso, $r = 0$, tenemos $n^2 = 9k^2 \equiv 0\ (3)$ y por lo tanto el resto es cero. En el segundo caso, $r = 1$, tenemos $n^2 = (3k+1)^2 = 9k^2 + 6k + 1 \equiv 1$ (3) y tenemos resto uno. En el tercer caso, $r = 2$, tenemos $n^2 = (3k+2)^2 = 9k^2 + 12k + 4 \equiv 4 \equiv 1$ (3) y tenemos nuevamente resto uno. Por lo tanto los restos posibles son 0 y 1.

(8) Sean a, b, c números enteros, ninguno divisible por 3. Probar que $a^2 + b^2 + c^2$ es divisible por 3.

Respuesta: Usando el ejercicio anterior tenemos que si ninguno de los tres números es divisible por 3 entonces el resto de sus cuadrados debe ser 1 y por lo tanto $a^2 + b^2 + c^2 \equiv 1 + 1 + 1 \equiv 3 \equiv 0$ (3) o sea que la suma de sus cuadrados es divisible por 3.

(9) Hallar la cifra de las unidades y la de las decenas del número 7^{15}.

Respuesta: Para ello es necesario encontrar el resto de la división de este número por 100. O sea su valor en la congruencia módulo 100. Pero $7^3 = 343 \equiv 43$ (100) y $7^4 = 2401 \equiv 1$ (100) por lo tanto $7^{15} = 7^{4\cdot 3+3} = (7^4)^3 \cdot 7^3 \equiv 1^3 \cdot 43 \equiv 43$ (100) y por lo tanto el resto es 43.

(10) Hallar el resto en la división de x por 5 y por 7 para:

a) $x = 1^8 + 2^8 + 3^8 + 4^8 + 5^8 + 6^8 + 7^8 + 8^8$, b) $x = 3.11.17.71.101$.

Respuestas:

a)

$$
\begin{aligned}
x &\equiv 1 + 4^4 + (5-2)^8 + (5-1)^8 + 0 + (5+1)^8 + (5+2)^8 + (5+3)^8 \ (5) \\
&\equiv 1 + (-1)^4 + (-2)^8 + (-1)^8 + 1^8 + 2^8 + (-2)^8 \ (5) \\
&\equiv 1 + 1 + 4^4 + 1 + 1 + 4^4 + 4^4 \ (5) \\
&\equiv 7 \ (5) \\
&\equiv 2 \ (5),
\end{aligned}
$$

y el resto es 2. Similarmente para 7.

b) $x = 3.11.17.71.101 \equiv 3\cdot(10+1)\cdot(15+2)\cdot(70+1)\cdot(100+1) \equiv 3\cdot 1\cdot 2\cdot 1\cdot 1 \equiv 6 \equiv 1$ (5). y el resto es 1. Similarmente para 7.

(11) Sean $a, b, m \in \mathbb{Z}$, $d > 0$, $d|a$, $d|b$, $d|m$. Probar que la ecuación

$$(1) \qquad ax \equiv b \mod (m)$$

tiene solución si y sólo si la ecuación:

$$(2) \qquad \frac{a}{d}x \equiv \frac{b}{d} \mod (\frac{m}{d})$$

tiene solución. Más aún si x_0 es solución de (1), entonces $x_0 + km$, $k \in \mathbb{Z}$ es también solución de (1). ¿Cuales son entonces las soluciones de (2)?.

(12) Resolver las siguientes ecuaciones:

$$a)\, 2x \equiv -21 \mod (8), \ b)\, 2x \equiv -12 \mod (7), \ c)\, 3x \equiv 5 \mod (4).$$

Respuestas:

a) Tenemos $(2, 8) = 2$ pero 2 no divide a -21 y por lo tanto no hay solución.

b) $(2, 7) = 1$ y por lo tanto siempre hay solución. En este caso planteamos que $1 = s \cdot 2 + t \cdot 7$ y por lo tanto que $s \cdot 2 \equiv 1$ (7), con solución $s = 4$, $t = -1$. Por lo tanto multiplicando ambos miembros de la ecuación por $s = 4$ obtenemos, $4 \cdot 2x \equiv x \equiv -48 \equiv -49 + 1 \equiv 1$ (7) con lo que una solución es $x = 1$. En efecto $2 \cdot 1 + 12 = 14 \equiv 0$ (7). Las otras soluciones será $x_m = 1 + 7m$.

c) $(3, 4) = 1$ y por lo tanto hay solución. En este caso $1 = s \cdot 3 + t \cdot 4$ con $s = -1$, $t = 1$ y por lo tanto $(-1) \cdot 3x \equiv x \equiv (-1) \cdot 5 \equiv -5 \equiv 8 - 5 \equiv 3$ y por lo tanto la solución entre cero y cinco es $x = 3$. Las restantes soluciones son $3 + 4m$ con $m \in \mathbb{N}$.

(13) Resolver la ecuación $221x \equiv 85 \mod (340)$. Hallar todas las soluciones x tales que $0 \le x < 340$.

Respuesta: En este caso $(221, 340) = 17$ y $85 = 17 \cdot 5$ por lo tanto $17|85$ y hay solución. La ecuación reducida (obtenida dividiendo todo por 17) es: $13x \equiv 5 \mod (20)$ En este caso tenemos $1 = s \cdot 13 + t \cdot 20$ con $s = -3$, $t = 2$. Y por lo tanto tenemos: $(-3) \cdot 13x \equiv x \equiv (-3) \cdot 5 \equiv -15 \equiv 5 \mod (20)$ y por lo tanto una solución es $x = 5$. Toda otra solución será de la forma $x_k = 5 + 20k$ y tomando todos los $0 \leq k < 17$ obtenemos todas las soluciones buscadas.

(14) Hallar todos los x que satisfacen:

a) $x^2 \equiv 1 \mod (4)$	*b)* $x^2 \equiv x \mod (12)$	*c)* $x^2 \equiv 2 \mod (3)$
d) $x^2 \equiv 0 \mod (12)$	*e)* $x^4 \equiv 1 \mod (16)$	*f)* $3x \equiv 1 \mod (5)$
g) $2x \equiv 5 \mod (6)$	*h)* $3x^2 \equiv 20 \mod (8)$	

Respuestas: a) $x^2 \equiv 1 \mod (4)$ es equivalente a $x^2 - 1 \equiv (x+1)(x-1) \equiv 0 \mod (4)$. Estos números ($x+1$ y $x-1$) son los dos pares o los dos impares, en el primer caso cada uno de ellos es divisible por dos y por lo tanto en conjunto son divisibles por 4. Si ambos son impares el resultado es impar y por lo tanto no hay solución. Por lo tanto las soluciones son todos los números pares o sea todos los x impares. Entre el 0 y el 3 las soluciones son 1 y 3. En efecto $1^2 = 1 \equiv 1 \mod (4)$, $3^2 = 9 = 8 + 1 \equiv 1 \mod (4)$.

d) $x^2 \equiv 0 \mod (12)$. Como $12 = 2^2 \cdot 3$ debemos tener que $2|x$ y $3|x$ [ya que 2 y 3 son primos y debe ser que $2|x^2$ y $3|x^2$]. Por lo tanto $x = m \cdot 2 \cdot 3 = 6m$. La únicas soluciones entre 0 y 11 son por lo tanto $x_0 = 0$ y $x_1 = 6$.

e) $x^4 \equiv 1 \mod (16)$. Esta ecuación es equivalente a $x^4 - 1 = (x^2-1)(x^2+1) \equiv 0 \mod (16)$. Ya que si x es solución $x + 16m$, $m \in \mathbb{N}$, es también solución, solo debemos buscar soluciones con $0 \leq x < 16$. Note que o ambos números son pares o ambos impares, en el caso impar el resultado del producto es impar y por lo tanto no hay solución. Por lo tanto estos debes ser par y x debe ser impar. Pero si $x = 2k+1$, luego $x^2 - 1 = (2k+1)^2 - 1 = 4k^2 + 4k + 1 - 1 = 4k(k+1) \equiv 0 \mod (0)$ ya que $k(k+1)$ es par. Y por lo tanto la equación original se satisface para todo x impar. Ver ejercicio 17.

h) $3x^3 \equiv 20 \equiv 4 \mod (8)$. Cláramente x tiene que ser par y solo debemos buscar entre los números del cero al ocho. $x = 0$ no es solución, $x = 2$ si, ya que $3 \cdot 2^2 = 12 = 8 + 4 \equiv 4 \mod (8)$. $x = 4$ no lo es, ya que $4^2 = 16 \equiv 0 \mod (8)$. $x = 6$ si, ya que $6^2 = 36 \equiv 4 \mod (8)$. Si agregamos un término $8m$ a cualquiera de estas soluciones también obtenemos otra solución.

(15) Dado $t \in \mathbb{Z}$, decimos que t es *inversible módulo* m si existe $h \in \mathbb{Z}$ tal que $th \equiv 1 \mod (m)$.
(a) ¿Es 5 inversible módulo 17?.
(b) ¿Existe algún m tal que m sea inversible módulo m?
(c) Probar que t es inversible módulo m si y sólo si $(t, m) = 1$.
(d) Determinar los inversibles módulo m para m= 11, 12, 16.

Respuestas: a) Si, la equación es $h5 \equiv 1 \mod (17)$ y esta tiene solución ya que $(5, 17) = 1$. Una solución es: $h = 7$ ($7 \cdot 5 = 35 = 34 + 1 \equiv 1 \mod (17)$).

b) Solo $m = 1$ y $m = -1$ ya que si $m \neq \pm 1$ $(m, m) = |m| > 1$ y por lo tanto $|m|$ no dividira a 1 y no habra solución a la ecuación definiendo la inversa.

c) La ecuación que la inversa debe satisfacer es $ht \equiv 1 \mod (m)$ y esta tiene solución si y solo si $(t, m) = 1$.

d) Caso $m = 11$. Debemos tener que $(t, 11) = 1$ y por lo tanto que en la descomposición en primos de t no puede haber ningún 11. O sea son todos los números que no tienen 11 en su decomposición en primos. Caso $m = 12 = 2^2 \cdot 3$. En este caso el conjunto de los números invertibles es el conjunto de aquellos enteros cuya decomposición prima no contiene ningún 2 ni ningún 3.

(16) Encontrar los enteros cuyos cuadrados divididos por 19 dan resto 9.

Respuesta: Eso es $x^2 = 9 \mod (19)$ o lo que es equivalente $(x+3)(x-3) = 0 \mod (19)$ Como 19 es primo o bien $19|(x+3)$ o $19|(x-3)$. Por lo tanto todas las soluciones son de la forma $x_m^+ = 3 + 19m$, $x_m^- = -3 + 19m$.

(17) Probar que todo número entero impar satisface: $a^4 \equiv 1(16)$, $a^8 \equiv 1(32)$, $a^{16} \equiv 1(64)$. ¿Se puede asegurar que $a^{2^n} \equiv 1(2^{2n+2})$?

Respuesta: Si a es impar entonces es de la forma $a = 2k+1$ y por lo tanto $a^4 = (2k+1)^4 = 16k^4 + 32k^3 + 16k^2 + 8k^2 + 8k + 1 \equiv 8k^2 + 8k + 1 \equiv 8k(k+1) + 1 \equiv 1 \mod (16)$, donde en la última equivalencia hemos usado que $k(k+1)$ es par (y por lo tanto de la forma $2m$ para algún m). El resultado general es que $a^{2^n} \equiv 1(2^{n+2})$ y se puede probar por inducción en n.

(18) Encuentre el resto en la división de a por b en los siguientes casos:

$$i)\ a = 11^{13}.13^8,\ b = 12, \quad ii)\ a = 4^{1000},\ b = 7$$
$$iii)\ a = 123^{456},\ b = 31, \quad iv)\ a = 7^{83},\ b = 10$$

Respuestas:

i) $a = 11^{13} \cdot 13^8$, $b = 12$ $a = (12-1)^13 \cdot (12+1)^8 \equiv (-1)^13 + 1^8 \equiv -1 + 1 \equiv 0 \mod (12)$ y por lo tanto el resto es cero.

ii) $a = 4^{1000}$, $b = 7$ $a = (7-3)^{1000} \equiv (-3)^1000 \equiv 3^{1000} \equiv 3 \cdot 3^{333 \cdot 3} \equiv 3 \cdot (3^3)^{333} \equiv 3 \cdot 27^{333} \equiv 3 \cdot (28-1)^{333} \equiv 3 \cdot (-1)^{333} \equiv -3 \equiv 4$ y el resto es 4.

(19) Obtenga el resto en la división de

$$i)\, 2^{21} \ \text{ por } \ 13, \quad ii)\, 3^8 \ \text{ por } \ 5, \quad iii)\, 8^{25} \ \text{ por } \ 127.$$

(20) Probar que si $(a, 1001) = 1$ entonces 1001 divide a $a^{720} - 1$.

(21) Decir si existe $x \in \mathbb{N}$ tal que se satisfacen simultáneamente las siguientes ecuaciones:

$$a)\, x \equiv 1 \mod (3), \quad x \equiv 1 \mod (5), \quad x \equiv 1 \mod (7)$$
$$b)\, x \equiv 2 \mod (3), \quad x \equiv 3 \mod (5), \quad x \equiv 5 \mod (2)$$
$$c)\, x \equiv 5 \mod (2), \quad x \equiv 2 \mod (4)$$

Respuestas: La primera y la segunda si tienen solución pues los números de las congruencias son co-primos entre si (de hecho son primos). La tercera no pues no son co-primos. De hecho la primera ecuación del tercer sistema requiere que x sea impar, mientras que la segunda que sea par.

(22) Hallar cuatro enteros consecutivos divisibles por 5, 7, 9 y 11 respectivamente.

Respuesta: Sea N el último de estos números. Luego se debe cumplir que

$$\begin{aligned} N-3 &\equiv 0 \mod (5) \\ N-2 &\equiv 0 \mod (7) \\ N-1 &\equiv 0 \mod (9) \\ N &\equiv 0 \mod (11) \end{aligned}$$

Este sistema tiene solución pues son congruencias co-primas entre sí. Usando el teorema Chino del resto sabemos que la solución es $N = n'_0 y_0 + n'_1 y_1 + n'_2 y_2 + n'_3 y_3$ donde si $n_0 = 11$, $n_1 = 9$, $n_2 = 7$, $n_3 = 5$ definimos $n'_i = n_0 n_1 n_2 n_3 / n_i$ y las y_i satisfacen las ecuaciones. $n'_i y_i = i \mod (n_i)$.

Estas ecuaciones independientes dan:

$$\begin{aligned} 9 \cdot 7 \cdot 11 y_3 &\equiv 4 \cdot 2 \cdot 1 y_3 \equiv 3y_3 \equiv 3 \mod (5) \\ 5 \cdot 9 \cdot 11 y_2 &\equiv (-2) \cdot 2 \cdot (-3) y_2 \equiv -2y_2 \equiv 2 \mod (7) \\ 5 \cdot 7 \cdot 11 y_1 &\equiv (-4) \cdot (-2) \cdot 2 y_1 \equiv -2y_1 \equiv 1 \mod (9) \\ 5 \cdot 7 \cdot 9 y_0 &\equiv 0 \mod (11) \end{aligned} \tag{1}$$

Con lo que podemos tomar las siguientes soluciones: $y_0 = 0$, $y_1 = -5$, $y_2 = -1$ $y_3 = 1$ La solución general es entonces: $N = 385 \cdot (-5) + 495 \cdot (-1) + 693 \cdot 1 = -1727$ Toda otra solución es de la forma $N + n_0 n_1 n_2 n_3 m = -1727 + 3465m$. En particular $m = 1$ nos da el primer natural con estas propiedades, $n = 1738$.

(23) a) Probar que no existen enteros no nulos tales que $x^2 + y^2 = 3z^2$.

b) Probar que no existen números racionales no nulos a, b, r tales que $3(a^2+b^2) = 7r^2$.

(24) Cinco hombres recogieron en una isla un cierto número de cocos y resolvieron repartirlos al día siguiente. Durante la noche uno de ellos decidió separar una parte y para ello dividió el total en cinco partes y dio un coco que sobraba a un mono y se fue a dormir. En seguida otro de los hombres hizo lo mismo, dividiendo lo que había quedado por cinco, dando un coco que sobraba a un mono y retirando su parte, se fue a dormir. Uno tras otro los tres restantes hicieron lo mismo, dándole a un mono el coco que sobraba. A la mañana siguiente repartieron los cocos restantes, dándole a un mono el coco sobrante. ¿Cuál es el número mínimo de cocos que se recogieron?

(25) La producción diaria de huevos en una granja es inferior a 75. Cierto día el recolector informó que la cantidad de huevos recogida es tal que contando de a 3 sobran 2, contando de a 5 sobran 4 y contando de a 7 sobran 5. el capataz dijo que eso era imposible. ¿Quién tenía razón?

Respuesta: Las tres condiciones de divisibilidad se pueden expresar como un sistema de ecuaciones en congruencia. Si N es el número total de huevos recogidos diariamente. Tenemos que:

$$\begin{aligned} N &\equiv 2 \mod (3) \\ N &\equiv 4 \mod (5) \\ N &\equiv 5 \mod (7) \end{aligned}$$

Como los números de las tres congruencias son co-primos entre si (en realidad son primos) luego habrá una solución módulo $M = 3 \cdot 5 \cdot 7 = 105$ y la pregunta es entonces si hay alguna solución con $N < 75$. Usando el teorema Chino del resto la solución se obtiene resolviendo las siguientes ecuaciones, (ver ejercicio 22 para entender la notación):

$$\begin{aligned} y_1 \cdot 35 &\equiv 2 \mod (3) \\ y_2 \cdot 21 &\equiv 4 \mod (5) \\ y_3 \cdot 15 &\equiv 5 \mod (7), \end{aligned}$$

que tiene como soluciones: $y_1 = 1$, $y_2 = 4$, $y_3 = 5$. Por lo tanto $n = 35{\cdot}1 + 21{\cdot}4 + 15{\cdot}5 = 194$ es solución del problema original. Restando M obtenemos que la única solución positiva menor que 105 es $89 > 75$ y por lo tanto vemos que el capataz tenía razón.