Práctico 4
Matemática Discreta I – Año 2021/1
FAMAF

Antes de resolver los ejercicios, recordemos una propiedad muy útil que cumple las *congruencias*. Si k, m son enteros, con $m \geq 2$, entonces por la definición de congruencia se cumple que: $km \equiv 0 \pmod{m}$, ya que $m \mid km$. De donde, si $a = b \cdot q + r$, con $a, q \in \mathbb{Z}$, $b \geq 2$ y $0 \leq r < b$, por las propiedades de las congruencias (*Teorema 4.1.3 del Apunte*) y teniendo en mente que "$\equiv$" es una *relación de equivalencia*, obtenemos

$$a \equiv b \cdot q + r \equiv 0 + r \equiv r \pmod{b}. \qquad (*)$$

De otro lado, si existen números naturales c, d tales que $b = c + d$ (esto implica que $c < b$ y $d < b$), entonces

$$c + d \equiv b \equiv 0 \pmod{b} \quad \Leftrightarrow \quad c \equiv -d \pmod{b} \quad \Leftrightarrow \quad d \equiv -c \pmod{b}. \qquad (**)$$

En lo que sigue, aplicaremos (*) y (**), indicando cual de las igualdades se cumple: $a = b \cdot q + r$ o $b = c + d$, al trabajar módulo b.

Ejercicios resueltos

(1) *a)* Calcular el resto de la división de 1599 por 39, sin tener que hacer la división.
Rta: Como $40 = 39 + 1$, se sigue que:

$$40 \equiv 1\ (39) \ \Rightarrow\ 40^2 \equiv 1\ (39) \ \Rightarrow\ 40^2 - 1 \equiv 0\ (39)$$
$$\Rightarrow\ 1599 \equiv 0\ (39)\,,$$

por lo tanto el resto es 0.

b) Lo mismo con el resto de 914 al dividirlo por 31.
Rta: Como $31 = 30 + 1$, tenemos que $30 \equiv -1\ (31)$. Luego,

$$914 \equiv 30^2 + 14 \equiv (-1)^2 + 14 \equiv 15\ (31)\,,$$

por lo tanto el resto es 15.

(2) Sea $n \in \mathbb{N}$. Probar que todo número de la forma $4^n - 1$ es divisible por 3.
Rta: Como $4 = 3 + 1$, entonces:

$$4 \equiv 1\ (3) \ \Rightarrow\ 4^n \equiv 1^n = 1\ (3)\,,\ \forall n \in \mathbb{N} \ \Rightarrow\ 4^n - 1 \equiv 0\ (3)\,,\ \forall n \in \mathbb{N}$$

por lo tanto, $3 \mid (4^n - 1)$ para cada $n \in \mathbb{N}$.

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

a) $x = 1^8 + 2^8 + 3^8 + 4^8 + 5^8 + 6^8 + 7^8 + 8^8$;
Rta: Para módulo 5: Como $2^4 = 16 = 3 \cdot 5 + 1$, se cumple que:

$$2^4 \equiv 1\ (5) \ \Rightarrow\ 2^8 \equiv 1\ (5)\,.$$

Además,

$$\begin{aligned}
3^8 &\equiv (-2)^8 \ (5) && (\text{por } 5 = 3+2)\\
4^8 &\equiv (-1)^8 \ (5) && (\text{por } 5 = 4+1)\\
5^8 &\equiv 0 \ (5) && (\text{por } 5 \mid 5)\\
6^8 &\equiv 1^8 \ (5) && (\text{por } 6 = 5+1)\\
7^8 &\equiv 2^8 \ (5) && (\text{por } 7 = 5+2)\\
8^8 &\equiv 3^8 \equiv (-2)^8 \ (5) && (\text{por } 8 = 5+3)
\end{aligned}$$

Luego,

$$\begin{aligned}
&1^8 + 2^8 + 3^8 + 4^8 + 5^8 + 6^8 + 7^8 + 8^8\\
&\equiv 1+1+1+1+0+1+1+1 = 7 \equiv 2 \ (5)\,.
\end{aligned}$$

Para módulo 7: (completar detalles) Ahora, $4^8 \equiv (-3)^8 \ (7)$, $5^8 \equiv (-2)^8 \ (7)$, $6^8 \equiv (-1)^8 \ (7)$, y $8^8 \equiv 1^8 \ (7)$. Como $2^3 \equiv 1 \ (7)$ y $3^2 \equiv 2 \ (7)$, entonces $2^8 = 2^6 \cdot 2^2 \equiv 4 \ (7)$ y $3^8 \equiv 2^4 \equiv 2 \ (7)$. De donde,

$$\begin{aligned}
&1^8 + 2^8 + 3^8 + 4^8 + 5^8 + 6^8 + 7^8 + 8^8\\
&\equiv 1+4+2+2+4+1+0+1 = 15 \equiv 1 \ (7)\,.
\end{aligned}$$

b) $x = 3 \cdot 11 \cdot 17 \cdot 71 \cdot 101$.
Rta: Completar detalles.

$$\begin{aligned}
x &= 3 \cdot 11 \cdot 17 \cdot 71 \cdot 101 \equiv 3 \cdot 1 \cdot 2 \cdot 1 \cdot 1 \equiv 6 \equiv 1 \ (5)\,;\\
x &= 3 \cdot 11 \cdot 17 \cdot 71 \cdot 101 \equiv 3 \cdot 4 \cdot 3 \cdot 1 \cdot 3 \equiv 108 \equiv 3 \ (7)\,.
\end{aligned}$$

(4) Sea $n \in \mathbb{Z}$. Probar que el resto de dividir n^2 por 4 es igual a 0 si n es par, y 1 si n es impar.

Rta: Si $n = 2k$, para algún $k \in \mathbb{Z}$, se tiene que:

$$n^2 \equiv 4k^2 \equiv 0 \ (4) \quad \Leftrightarrow \quad 4 \mid n^2 \quad \checkmark$$

Si $n = 2t + 1$, para algún $t \in \mathbb{Z}$, tenemos

$$n^2 \equiv 4t^2 + 4t + 1 \equiv 1 \ (4) \quad \checkmark$$

(5) Sean a, b, c números enteros, ninguno divisible por 3. Probar que

$$a^2 + b^2 + c^2 \equiv 0 \ (3)\,.$$

Rta: Si ninguno es divisible por 3, tenemos que cada uno de ellos es de la forma: $x \equiv 1 \pmod 3$ o $x \equiv 2 \pmod 3$, por lo tanto $x^2 \equiv 1 \pmod 3$ o $x^2 \equiv 4 \equiv 1 \pmod 3$. Luego, a^2, b^2, c^2 son congruentes a 1 módulo 3, y en consecuencia

$$a^2 + b^2 + c^2 \equiv 1+1+1 \equiv 3 \equiv 0 \ (3)\,.$$

Por lo tanto, $3 \mid (a^2 + b^2 + c^2)$.

(6) *a)* Probar las reglas de divisibilidad por $2, 3, 4, 5, 8, 9$ y 11.

Rta:

Reglas del 2 y 5. Como $10 = 2 \cdot 5$, entonces para todo $j \in \mathbb{N}$: $10^j \equiv 0\ (2)$. Ahora bien, si aplicamos la definición de la base 10 a $n \in \mathbb{N}$, esto es, $n = \sum_{j=0}^{k} a_j 10^j$, obtenemos:

$$n \equiv a_0 + \sum_{j=1}^{k} a_j 0^j \equiv a_0\ (2)\,.$$

Por lo tanto,

$$2 \mid n \ \Leftrightarrow\ n \equiv 0\ (2) \ \Leftrightarrow\ a_0 \equiv 0\ (2) \ \Leftrightarrow\ 2 \mid a_0.$$

Debido a que $0 \leq a_0 \leq 9$, concluimos que n es divisible por 2 si y sólo si n termina en $0, 2, 4, 6, 8$.

Notar que lo mismo pasa con 5 por ser $10 \equiv 0\ (5)$, es decir

$$5 \mid n \ \Leftrightarrow a_0 \in \{0, 5\}.$$

Reglas del 3 y 9. Como $10 \equiv 1\ (3)$ (ya que $10 = 3 \cdot 3 + 1$), entonces para todo $j \geq 0$ se satisface que $10^j \equiv 1\ (3)$. Luego,

$$n \equiv \sum_{j=0}^{k} a_j 10^j \equiv \sum_{j=0}^{k} a_j 1^j \equiv \sum_{j=0}^{k} a_j\ (3)\,.$$

Por lo tanto, $3 \mid n$ si y sólo si $3 \mid \left(\sum_{j=0}^{k} a_j\right)$.

Notar que lo mismo pasa con 9 por ser $10 \equiv 1\ (9)$. Así,

$$9 \mid n \ \Leftrightarrow\ 9 \mid \left(\sum_{j=0}^{k} a_j\right).$$

Reglas del 4 y 8. Tenemos que $10^j \equiv 0\ (4)$ si $j \geq 2$ (ya que $10^2 = 4 \cdot 25$), y $10^j \equiv 0\ (8)$ si $j \geq 3$ (pues $10^3 = 8 \cdot 125$). Por lo tanto,

$$n \equiv 10a_1 + a_0 \equiv 2a_1 + a_0\ (4) \quad (10 = 2 \cdot 4 + 2).$$

$$\begin{aligned} n &\equiv 10^2 a_2 + 10a_1 + a_0 \\ &\equiv 4a_2 + 2a_1 + a_0\ (8) \quad (10^2 = 12 \cdot 8 + 4). \end{aligned}$$

Es decir,

$$4 \mid n \ \Leftrightarrow\ 4 \mid (2a_1 + a_0); \qquad 8 \mid n \ \Leftrightarrow\ 8 \mid (4a_2 + 2a_1 + a_0).$$

Regla del 11. Como $11 = 10 + 1$, entonces $10 \equiv -1\ (11)$. De donde, para todo $j \geq 0$: $10^j \equiv (-1)^j\ (11)$. Así,

$$n \equiv \sum_{j=0}^{k} a_j 10^j \equiv \sum_{j=0}^{k} a_j (-1)^j \equiv \sum_{j=0}^{k} (-1)^j a_j\ (11)\,.$$

Por lo cual, $11 \mid n$ si y sólo si 11 divide a la suma alternada de sus dígitos.

b) Decir por cuáles de los números del 2 al 11 son divisibles los siguientes números:

$$12342 \qquad 5176 \qquad 314573 \qquad 899.$$

Rta: Usaremos las reglas de divisibilidad probadas en el inciso anterior. *Para* $n := 12342$. Tenemos que $2 \mid 2$, $3 \mid (1+2+3+4+2) = 12$, $4 \nmid (2 \cdot 4 + 2) = 10$, $5 \nmid 2$, $12342 = 1763 \cdot 7 + 1$, $9 \nmid 12$, y $11 \mid (1-2+3-4+2) = 0$. Por lo tanto, $2 \mid n$, $3 \mid n$, $4 \nmid n$ ($\Rightarrow 8 \nmid n$), $5 \nmid n$ ($\Rightarrow 10 \nmid n$), $6 \mid n$ (2 y 3 lo dividen), $7 \nmid n$, $9 \nmid n$, y $11 \mid n$.

Los demás números se analizan de la misma manera, se dejan al lector.

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

Rta: Tenemos que para todo natural $j \geq 2$, $10^j \equiv 0\ (100)$. Luego, para cualquier $n \in \mathbb{N}$ escrito en la base 10, se satisface que:

$$n \equiv \sum_{j=2}^{k} a_j 0^j + 10a_1 + a_0 \equiv 10a_1 + a_0\ (100)\,, \qquad (*)$$

donde a_1 es la cifra de las decenas y a_0 es la cifra de las unidades. Luego, basta con hallar $0 \leq r < 100$ tal que

$$7^{15} \equiv r\ (100)\,.$$

Ahora bien,

$$\begin{aligned}
7 &\equiv 7\ (100) \\
7^2 &\equiv 49\ (100) \\
7^3 &\equiv 343 \equiv 43\ (100) && \text{(por (*))} \\
7^4 &\equiv 7 \cdot 43 \equiv 301 \equiv 1\ (100) && \text{(por (*))} \\
7^{15} &\equiv (7^4)^3 \cdot 7^3 \equiv 7^3 \equiv 43\ (100)
\end{aligned}$$

Así, $a_1 = 4$ y $a_0 = 3$.

Observación:

Sean $a \in \mathbb{Z}$ y $n \in \mathbb{N}$. Si $a = n \cdot q + r$, para algún $q \in \mathbb{Z}$, $n \geq 2$ y $0 \leq r < n$, entonces $a \equiv r\ (n)$, luego $a^2 \equiv r^2\ (n)$. Por lo tanto, para hallar las soluciones enteras de $x^2 \equiv b\ (n)$ (con $0 \leq b < n$) ó de $x^2 \equiv x\ (n)$, basta con hallar las soluciones particulares $0 \leq x_0 < n$, y todas las soluciones serían de la forma $x_0 + kn$, para algún $k \in \mathbb{Z}$.

(8) Hallar todos los $x \in \mathbb{Z}$ que satisfacen:

a) $x^2 \equiv 1\ (4)$

Rta: Resolvemos primero para $0 \leq x_0 \leq 3$. Esto es, $x_0 = 1$ ó $x_0 = 3$, y por lo tanto $x = 1 + 4k$ ó $x = 3 + 4k$, para algún $k \in \mathbb{Z}$, lo cual también se puede escribir como $x = 4k \pm 1$.

b) $x^2 \equiv x\ (12)$
Rta: Soluciones menores que 12: $x_0 = 0, 1, 4, 9$. Luego el conjunto solución es $\{12k, 12k+1, 12k+4, 12k-3\ :\ k \in \mathbb{Z}\}$.

c) $x^2 \equiv 2\ (3)$
Rta: No tiene soluciones pues $0^2 \equiv 0\ (3)$, $1^2 \equiv 1\ (3)$, $2^2 \equiv 1\ (3)$.

d) $x^2 \equiv 1\ (5)$
Rta: Soluciones menores que 5: $\{1, 4\}$. Luego las soluciones son $5k \pm 1,\ k \in \mathbb{Z}$.

e) $x^4 \equiv 1\ (16)$
Rta: Si $x = 2t$, para algún $t \in \mathbb{Z}$, entonces $x^4 \equiv 16t^4 \equiv 0\ (16)$. Por lo tanto, x debe ser impar. Ahora bien, podemos tomar $-8 \leq x_0 \leq 8$, es decir $x_0 \in \{-7, -5, -3, -1, 1, 3, 5, 7\}$, ya que por ejemplo $9 \equiv -7\ (16)$. De donde, $x_0^2 \in \{1, 9, 25, 49\}$, esto es: $x_0^2 \equiv 1\ (16)$ o bien $x_0^2 \equiv 9\ (16)$ (ya que $25 = 16+9,\ 49 = 16\cdot 3+1$). A su vez, cuando elevamos estos al cuadrado, como $9^2 = 81 \equiv 1\ (16)$ (por $81 = 16 \cdot 5 + 1$), obtenemos que todo número impar es solución de la ecuación.

f) $x^2 \equiv 9\ (19)$
Rta: Vemos que 3 y 16 son los únicos restos que son solución (usar que $18 \equiv -1\ (19)$, $17 \equiv -2\ (19)$, $16 \equiv -3\ (19)$,..., $10 \equiv -9\ (19)$). Luego, todas las soluciones buscadas son $19k \pm 3$, $k \in \mathbb{Z}$.

(9) Sean $a, b \in \mathbb{Z}$. Si $m, d \in \mathbb{N}$ cumplen que $d \mid a$, $d \mid b$ y $d \mid m$, probar que la ecuación $a\,x \equiv b\ (m)$ tiene solución si y sólo si la ecuación

$$\frac{a}{d}\,x \equiv \frac{b}{d}\ \left(\frac{m}{d}\right)$$

tiene solución.

Rta: La ecuación $\frac{a}{d}\,x \equiv \frac{b}{d}\ \left(\frac{m}{d}\right)$ tiene solución si y sólo si $\left(\frac{a}{d}, \frac{m}{d}\right) \mid \frac{b}{d}$ si y sólo si $\frac{(a,m)}{d} \mid \frac{b}{d}$ si y sólo si $(a, m) \mid b$ si y sólo si la ecuación $a\,x \equiv b\ (m)$ tiene solución.

(10) Resolver las siguientes ecuaciones:

a) $2x \equiv -21\ (8)$
Rta: Como $-21 = (-3)\cdot 8 + 3$, entonces $-21 \equiv 3\ (8)$, por lo tanto la ecuación es equivalente a $2x \equiv 3\ (8)$. Como $(2, 8) = 2 \nmid 3$, entonces no hay solución.

b) $2x \equiv -12\ (7)$
Rta: Tenemos que $-12 \equiv 2\ (7)$ (ya que $-12 = (-2)\cdot 7 + 2$), por lo tanto la ecuación es equivalente a $2x \equiv 2\ (7)$. Evidentemente 1 es solución de la ecuación, y como $1 = (2, 7)$, todas las soluciones son de la forma $x = 1 + 7k,\ k \in \mathbb{Z}$.

c) $3x \equiv 5\ (4)$
Rta: $5 \equiv 1\ (4)$, por lo tanto la ecuación es equivalente a $3x \equiv 1\ (4)$. Probando se encuentra que 3 es solución, y como $1 = (4, 3)$, todas las soluciones son de la forma $x = 3 + 4k,\ k \in \mathbb{Z}$.

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

Rta: Notemos que 221, 85 y 340 son divisibles por 17. Sus respectivos cocientes son 13, 5 y 20. Por el ejercicio (9), podemos entonces resolver

$$13x \equiv 5\ (20)\,.$$

Por el algoritmo de Euclides: $(13, 20) = 1 = (-3) \cdot 13 + 2 \cdot 20$, por lo tanto $5 = (-15) \cdot 13 + 10 \cdot 20$. Haciendo congruencia módulo 20 obtenemos $5 \equiv (-15) \cdot 13 \equiv 5 \cdot 13\ (20)$ (por $20 = 15 + 5$). Entonces 5 es una solución, y todas la soluciones son de la forma $x = 5 + 20k$, con $k \in \mathbb{Z}$.
Por último, $0 \leq x < 340 \iff 0 \leq 5 + 20k < 340 \iff -0.25 \leq k < 16.75$. Como k debe ser un entero, entonces $k = 0, 1, 2, \ldots, 16$. Así, obtenemos que el conjunto buscado es: $\{5, 25, 45, \ldots, 305, 325\}$.

(12) *a)* Encontrar todas las soluciones de la ecuación $36\,x \equiv 8\ (20)$.
Rta: Tenemos que $4 = (36, 20)$. Como $4|8$ la ecuación tiene solución. Ahora bien, por el ejercicio 9, podemos entonces resolver

$$9x \equiv 2\ (5) \iff 4x \equiv 2\ (5)\,.$$

Por el algoritmo de Euclides:

$$(5, 4) = 1 = 5 - 4 \Rightarrow 2 = 2 \cdot 5 + (-2) \cdot 4 \Rightarrow 2 \equiv (-2) \cdot 4\ (5)$$

entonces -2 es solución, y todas la soluciones son de la forma $x = -2 + 5k$, con $k \in \mathbb{Z}$.

b) Dar todas las soluciones x de la ecuación anterior tales que $-8 < x < 30$.
Rta: Por el inciso anterior:
$-8 < x < 30 \iff -8 < -2 + 5k < 30 \iff -6 < 5k < 32$.
De donde, k debe tomar los valores $-1, 0, 1, 2, 3, 4, 5, 6$, y por lo tanto el conjunto buscado es $\{-7, -2, 3, 8, 13, 18, 23, 28\}$.

(13) *a)* Encontrar todas las soluciones de la ecuación $21\,x \equiv 6\ (30)$.
Rta: Tenemos que $21\,x \equiv 6\ (30) \iff 7\,x \equiv 2\ (10)$. Luego,
$1 = (-2) \cdot 10 + 3 \cdot 7 \Rightarrow 2 = (-4) \cdot 10 + 6 \cdot 7 \Rightarrow 2 \equiv 6 \cdot 7\ (10)$. De donde, la ecuación tiene como soluciones $x = 6 + 10k$, con k entero.

b) Dar todas las soluciones x de la ecuación anterior tales que $0 < x < 35$.
Rta: En base al ítem anterior,

$$0 < x < 35 \iff 0 < 6 + 10k < 35 \iff -0.6 < k < 2.9.$$

De donde, k toma valores $0, 1, 2$, y las soluciones buscadas son $6, 16, 26$.

(14) Dado $t \in \mathbb{Z}$, decimos que t es *inversible módulo* m si existe $h \in \mathbb{Z}$ tal que $th \equiv 1\ (m)$.

a) ¿Es 5 inversible módulo 17?
Rta: Si, $5 \cdot 7 \equiv 1\ (17)$.

b) Probar que t es inversible módulo m, si y sólo si $(t, m) = 1$.
Rta: t es inversible módulo m si y sólo si $tx \equiv 1\ (m)$ tiene solución si y sólo si $(t, m) \mid 1$ si y sólo si $(t, m) = 1$.

c) Determinar los inversibles módulo m, para $m = 11, 12, 16$.
Rta: Por el ítem anterior y el T.F.A, obtenemos:

$$(t, 11) = 1 \Leftrightarrow 11 \nmid t.$$
$$(t, 12) = 1 \Leftrightarrow (t, 2) = 1 = (t, 3).$$
$$(t, 16) = 1 \Leftrightarrow 2 \nmid t.$$

(15) Encontrar el resto en la división de a por b en los siguientes casos:

a) $a = 11^{13} \cdot 13^8$, $b = 12$.
Rta: Como $12 = 11 + 1$ y $13 = 12 + 1$, se sigue que:

$$11^{13} \cdot 13^8 \equiv (-1)^{13} \cdot 1^8 \equiv 11\ (12)\,.$$

b) $a = 4^{1000}$, $b = 7$.
Rta: Sabemos que 7 es un número primo y que $(4, 7) = 1$, entonces por el Corolario del teorema de Fermat:

$$4^6 \equiv 1\ (7)\,.$$

Además, $4^2 \equiv 16 \equiv 2 \cdot 7 + 2 \equiv 2\ (7)$, luego

$$4^{1000} = (4^6)^{166} 4^4 \equiv (4^2)^2 \equiv 2^2 \equiv 4\ (7)\,.$$

c) $a = 123^{456}$, $b = 31$.
Rta: Tenemos que $123 = 3 \cdot 31 + 30$ y $31 = 30 + 1$, así

$$123^{456} \equiv 30^{456} \equiv (-1)^{456} \equiv 1\ (31)\,.$$

d) $a = 7^{83}$, $b = 10$.
Rta: Para cualquier entero x se satisface que $x \equiv a_0\ (10)$, donde a_0 es la cifra de las unidades. Por lo cual,

$$7^2 \equiv 9\ (10)\,, \quad 7^3 \equiv 7 \cdot 9 \equiv 3\ (10)\,, \quad 7^4 \equiv 3 \cdot 7 \equiv 1\ (10)\,.$$

De donde,

$$7^{83} \equiv (7^4)^{20} 7^3 \equiv 1^{20} 3 \equiv 3\ (10)\,.$$

(16) Hallar el resto en la división de a por b en los siguientes casos:

a) $a = 2^{21}$, $b = 13$.
Rta: Como 13 es primo y $(2, 13) = 1$, por el corolario del teorema de Fermat:

$$2^{12} \equiv 1\ (13)\,.$$

De otro lado, $8 \cdot 5 \equiv 1\ (13)$ (ya que $40 = 3 \cdot 13 + 1$), así:

$$2^{12} \equiv 1\ (13) \quad \Rightarrow \quad (5 \cdot 2^3)2^9 \equiv 5\ (13) \quad \Rightarrow \quad 2^9 \equiv 5\ (13)\,.$$

Luego,

$$2^{21} = 2^{12}2^9 \equiv 2^9 \equiv 5\ (13)\,.$$

b) $a = 7^{241},\ b = 17$.
Rta: Tenemos que 17 es primo y $(7, 17) = 1$, por el corolario del teorema de Fermat:

$$7^{16} \equiv 1\ (17) \quad \Rightarrow \quad 7^{241} \equiv (7^{16})^{15} \cdot 7 \equiv 7\ (17)\,.$$

c) $a = 424^{97},\ b = 11$.
Rta: Por comodidad en las cuentas, lo primero que hacemos es reducir la base de la potencia requerida a un número más chico, esto es: por el algoritmo de la división,

$$424 = 38 \cdot 11 + 6 \quad \Rightarrow \quad 424 \equiv 6\ (11) \quad \Rightarrow \quad 424^{97} \equiv 6^{97}\ (11)\,.$$

Ahora bien, 11 es primo y $(6, 11) = 1$, por el corolario del teorema de Fermat:

$$6^{10} \equiv 1\ (11) \quad \Rightarrow \quad 6^{97} \equiv (6^{10})^9 \cdot 6^7 \equiv 6^7\ (11)\,.$$

Además,

$$6^2 \equiv 3\ (11) \qquad (\text{por } 36 = 3 \cdot 11 + 3)$$
$$6^6 \equiv 3^3 \equiv 5\ (11) \qquad (\text{por } 27 = 2 \cdot 11 + 5)$$
$$6^7 \equiv 6 \cdot 5 \equiv 8\ (11) \qquad (\text{por } 30 = 2 \cdot 11 + 8)$$

En resumen,

$$424^{97} \equiv 8\ (11)\,.$$

d) $a = 8^{25},\ b = 127$.
Rta: $8^{25} = 2^{75}$: como $2^7 = 128 \equiv 1\ (127)$, tenemos que

$$2^{75} = (2^7)^{10}2^5 \equiv 32\ (127)\,.$$

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

Rta: Notemos que $1001 = 7 \cdot 11 \cdot 13$. Por lo tanto $(a, 1001) = 1$ implica $(a, 7) = (a, 11) = (a, 13) = 1$. Entonces por el corolario del teorema de Fermat: $a^6 \equiv 1\ (7)$, $a^{10} \equiv 1\ (11)$, $a^{12} \equiv 1\ (13)$. Como $720 = 6 \cdot 10 \cdot 12$, se sigue que

$$a^{720} \equiv 1\ (7)\,, \quad a^{720} \equiv 1\ (11)\,, \quad a^{720} \equiv 1\ (13)\,.$$

Lo cual es equivalente a tener

$$7 \mid (a^{720} - 1), \quad 11 \mid (a^{720} - 1), \quad 13 \mid (a^{720} - 1).$$

Por el ejercicio 21(b) del Práctico 3, concluimos que:

$$7 \cdot 11 \cdot 13 \mid (a^{720} - 1) \quad \Leftrightarrow \quad 1001 \mid (a^{720} - 1).$$

(18) Sea p primo impar.

a) Probar que las únicas raíces cuadradas de 1 módulo p, son 1 y -1 módulo p. Es decir, probar que $x^2 \equiv 1 \pmod{p}$, entonces $x \equiv \pm 1 \pmod{p}$.

Rta: $x^2 \equiv 1 \pmod{p} \Rightarrow x^2 - 1 \equiv 0 \pmod{p}$, como $x^2 - 1 = (x-1)(x+1)$, obtenemos $(x-1)(x+1) \equiv 0 \pmod{p}$. Esto quiere decir que $p|(x-1)(x+1)$. Como p es primo, $p|(x-1)$ o $p|(x+1)$, es decir

$$x - 1 \equiv 0 \pmod{p} \quad \vee \quad x + 1 \equiv 0 \pmod{p} \quad \Leftrightarrow$$
$$x \equiv 1 \pmod{p} \quad \vee \quad x \equiv -1 \pmod{p}.$$

b) Sea $p = d \cdot 2^s + 1$, donde d es impar. Dado a entero tal que $0 < a < p$, probar que

(i) $a^d \equiv 1 \pmod{p}$, o

(ii) $a^{2^r \cdot d} \equiv -1 \pmod{p}$ para algún r tal que $0 \leq r < s$.

Rta: Consideremos la sucesión $a^{2^s \cdot d}, a^{2^{s-1} \cdot d}, \ldots, a^{2d}, a^d$. La demostración la haremos usando el teorema de Fermat, el resultado del inciso anterior y observando que cada término de la sucesión es el cuadrado del siguiente.

- Por el teorema de Fermat $a^{2^s \cdot d} = a^{p-1} \equiv 1 \pmod{p}$. Luego $(a^{2^{s-1} \cdot d})^2 \equiv 1 \pmod{p}$ y por lo tanto $a^{2^{s-1} \cdot d}$ es una raíz cuadrada de 1 módulo p. Por el inciso anterior entonces $a^{2^{s-1} \cdot d} \equiv \pm 1 \pmod{p}$.
- Si $a^{2^{s-1} \cdot d} \equiv -1 \pmod{p}$, listo, en caso contrario $a^{2^{s-1} \cdot d} \equiv 1 \pmod{p}$, luego $(a^{2^{s-2} \cdot d})^2 \equiv 1 \pmod{p}$ y por lo tanto $a^{2^{s-2} \cdot d}$ es una raíz cuadrada de 1 módulo p. Por el inciso anterior entonces $a^{2^{s-2} \cdot d} \equiv \pm 1 \pmod{p}$.
- Iterando el razonamiento anterior concluimos que alguno de los términos de la sucesión $a^{2^r \cdot d}$ es congruente a -1 módulo p o bien todos los términos son congruentes a 1, en particular $a^d \equiv 1 \pmod{p}$.