24 de Noviembre 2006 (SOLUCIONES)

(1) Sea n un entero compuesto. Demostrar:

(a) Existe un factor primo p de n cumpliendo $p \leq \sqrt{n}$.

Solución: Como n es compuesto, podemos escribirlo como $n = a \cdot b$ donde $a, b \in \mathbb{Z}$ tal que $1 < a \leq b < n$. Así obtenemos $a \leq \sqrt{n}$, ya que de lo contrario tendríamos $\sqrt{n} < a \leq b$ y $n = a \cdot b > \sqrt{n}\sqrt{n} = n$. Sea p un divisor primo de a, entonces $p \leq a \leq \sqrt{n}$. Como $p|a$, se tiene $p|n$. Por lo tanto n tiene un factor primo p tal que $p \leq \sqrt{n}$.

(b) Si el factor primo p más pequeño de n cumple $p > \sqrt[3]{n}$, entonces n/p es primo.

Solución: Sea p el factor primo más pequeño de n. Supongamos que $p > \sqrt[3]{n}$. Entonces

$$\frac{n}{p} < n^{2/3}\,. \tag{1}$$

Si n/p es compuesto, por el apartado (a), n/p tiene un factor primo q tal que $q \leq \sqrt{n/p}$ Entonces por (1) tenemos $q < \sqrt[3]{n}$. Ahora, como $q|(n/p)$, entonces $q|n$. Así que hemos encontrado un factor primo q de n más pequeño que p, que contradice la suposición de inicio. Así que n/p no puede ser compuesto y como n es compuesto, tampoco puede ser 1. Así n/p que ha de ser primo.

(2) Encontrar los últimos dos digitos de 2^{1000}.

Solución: Hemos de calcular $2^{1000} \pmod{100}$. Es decir, hemos de encontrar $x \in \{0, \ldots, 99\}$ tal que $x \equiv 2^{1000} \pmod{100}$. Factorizando $100 = 2^2 \cdot 5^2$, utilizando el teorema chino del resto, obtenemos que hemos de encontrar la solución al sistema

$$\begin{cases} x \equiv 2^{1000} \pmod{2^2} \\ x \equiv 2^{1000} \pmod{5^2} \end{cases}.$$

De la primera ecuación se obtiene que $x \equiv 0 \pmod{2^2}$. De la segunda, obsérvese que $(2^{10})^{100} = (1024)^{100} \equiv (-1)^{100} \pmod{5^2}$. Por lo tanto, $x \equiv 1 \pmod{5^2}$. También podemos llegar a la misma conclusión aplicando el lema de Hensel al polinomio $f(x) = x - 2^{1000}$. Ya que $(2^2)^{500} = (4)^{500} \equiv (-1)^{500} \equiv 1 \pmod{5}$. Así que $f(1) \equiv 0 \pmod{5}$ y como $f'(1) = 1 \not\equiv 0 \pmod{5}$, obtenemos que $x = 1$ es la única raíz de $f(x) \bmod 5^2$. Otra forma sería utilizando el teorema de Euler-Fermat. Como $\phi(5^2) = 20$ y $(2, 5^2) = 1$, tenemos $2^{20} \equiv 1 \pmod{5^2}$. Así que $2^{1000} = (2^{20})^{50} \equiv 1 \pmod{5^2}$

Por lo tanto, hemos de resolver

$$\begin{cases} x \equiv 0 \pmod{2^2} \\ x \equiv 1 \pmod{5^2} \end{cases}.$$

Por la primera condición tenemos $x = 4k$. Por lo tanto nos queda por resolver $4k \equiv 1 \pmod{5^2}$. O lo que es equivalente, $6(4k) \equiv 6 \pmod{5^2}$, es decir, $-k \equiv 6 \pmod{5^2}$. Por lo tanto, $k \equiv -6 \equiv 19 \pmod{5^2}$. Por lo tanto, $x = 4(19) = 76$. Es decir:

$$2^{1000} \equiv 76 \pmod{100}.$$

Así se concluye que los dos últimos digitos de 2^{1000} son 76.

Otra forma:

$$\begin{aligned} 2^{1000} = {} & 10715086071862673209484250490600018105614048117055336074 \\ & 37503883703510511249361224931983788156958581275946729175 \\ & 31468251871452856923140435984577574698574803934567774824 \\ & 30985421074605062371141877954182153046474983581941267398 \\ & 76755916554394607706291457119647768654216766042983165262 \\ & 86837205668069376 \end{aligned}$$

(3) Sea $n \in \mathbb{N}$. Demostrar $\displaystyle\prod_{\substack{a=1 \\ (a,n)=1}}^{n-1} a \equiv \pm 1 \,(\textbf{mod } n)$

Solución: Sea $a \in \{1, \dots n-1\}$ tal que $(a,n) = 1$, entonces a es una unidad mod n. Es decir, existe $b \in \{1, \dots n-1\}$ tal que $ab \equiv 1 \pmod{n}$. Si $b \neq a$, cada pareja (a,b) aporta un 1 al producto. Si $b = a$, entonces $(-a)a \equiv -1 \pmod{n}$. Así que la pareja $(a,-a)$ aporta un -1 al producto. Así que sólo nos queda el caso en que $a \equiv -a \pmod{n}$, es decir $2a \equiv 0 \pmod{n}$. Y como $a \in \{1, \dots n-1\}$, tendriamos que $a = n/2$, pero $(n, n/2) \neq 1$. Así que el producto es $\equiv \pm 1 \pmod{n}$.

(4) Sea p un primo impar. Calcular $\left(\frac{7}{p}\right)$.

Solución: Supongamos $p \neq 7$. La ley de reciprocidad cuadrática nos dice:

$$\left(\frac{7}{p}\right) = (-1)^{\frac{(7-1)(p-1)}{4}} \left(\frac{p}{7}\right).$$

Por lo tanto:

$$\left(\frac{7}{p}\right) = 1 \iff \begin{cases} (-1)^{\frac{p-1}{2}} = 1 & \text{y} \quad \left(\frac{p}{7}\right) = 1 \\ & \text{ó} \\ (-1)^{\frac{p-1}{2}} = -1 & \text{y} \quad \left(\frac{p}{7}\right) = -1 \end{cases} \iff \begin{cases} p \equiv 1 \pmod{4} & \text{y} \quad p \equiv 1,2,4 \pmod{7} \\ & \text{ó} \\ p \equiv 3 \pmod{4} & \text{y} \quad p \equiv 3,5,6 \pmod{7} \end{cases}$$

Ya que los cuadrados mod 7 son $0, 1, 2$ y 4.

De la primera condición tenemos que $p \equiv 1 \pmod{4}$, así que $p \equiv 1,5,9,13,17,21,25 \pmod{28}$. Como hemos de tener $p \equiv 1,2,4 \pmod{7}$, obtenemos que la primera condición es equivalente a $p \equiv 1,9,25 \pmod{28}$. Análogamente la segunda condición nos asegura que $p \equiv -1,-9,-25 \pmod{28}$.

Análogamente se haría para $\left(\frac{p}{7}\right) = -1$.

Juntándolo obtenemos:

$$\left(\frac{7}{p}\right) = \begin{cases} 1 & \text{si} \quad p \equiv \pm 1, \pm 3, \pm 9 \pmod{28} \\ -1 & \text{si} \quad p \equiv \pm 5, \pm 11, \pm 13 \pmod{28} \\ 0 & \text{si} \quad p = 7. \end{cases}$$

(5) Calcular las soluciones de las siguientes ecuaciones:

(a) $x^{22} \equiv 101$ (**mod** 225)

(b) $x^{27} \equiv 76$ (**mod** 225)

(c) $x^{37} \equiv 176$ (**mod** 225)

Solución: En primer lugar factoricemos 225, obteniendo $225 = 3^2 \cdot 5^2$. Por lo tanto,

$$x^n \equiv a \pmod{225} \iff \begin{cases} x^n \equiv a \pmod{3^2} \\ x^n \equiv a \pmod{5^2} \end{cases}$$

Como $p = 3, 5$ son primos impares tenemos un resultado que nos dice:

$$x^n \equiv a \pmod{p^r} \iff a^{\frac{\phi(p^r)}{d}} \equiv 1 \pmod{p^r} \quad \text{donde } d = (n, \phi(p^r)).$$

Además dicho resultado nos asegura que si tiene solución, entonces tiene d soluciones.

Así que aplicado a nuestros casos tenemos:

(a) $(n,a) = (22, 101)$. Para $p^r = 9$ tenemos $\phi(9) = 6$, $d = 2$ y $a \equiv 2 \pmod{9}$. Por lo tanto, tenemos $2^3 \equiv -1 \not\equiv 1 \pmod{9}$. Por lo tanto no hay solución.

(b) $(n,a) = (27, 76)$ Para $p^r = 9$ tenemos $\phi(9) = 6$, $d = 3$ y $a \equiv 4 \pmod{9}$. Por lo tanto, tenemos $4^2 \equiv 7 \not\equiv 1 \pmod{9}$. Por lo tanto no hay solución.

(c) $(n,a) = (37, 176)$. Como $n = 37$ es primo con $\phi(9) = 6$ y $\phi(25) = 9$, obtenemos que hay una única solución mod 9 y mod 25. Por lo tanto hay una única solución mod 225. Para calcular dicha solución utilizemos el lema de Hensel aplicado a $f(x) = x^{37} - 176$. En primer lugar, obsérvese que 176 es primo con 3 y 5. Por lo tanto 0 no es solución ni mod 3 ni mod 5. Por lo tanto como $f'(x) = 37x^{36}$, tendremos que las soluciones de $f(x) \equiv \pmod{3,5}$ nos darán soluciones $f(x) \equiv \pmod{3^2, 5^2}$. Tenemos $x = 5$ es solución mod 3^2 y $x = 1$ es solución mod 5^2. Por lo tanto, por el teorema chino del resto obtenemos $x = 176$ es la única solución mod 225.