Practico 6 - ejercicios

c. 2^{-1} (mód 55) y 2^{38} (mód 55).

* $2^{-1} \pmod{55}$

2 y 55 son coprimos

identidad de Bezout: $2 \cdot 28 - 55 = 1$

$2 \cdot 28 - 55 \equiv 1 \pmod{55}$

$2 \cdot 28 \equiv 1 \pmod{55}$

↑ inverso de 2 modulo 55

* $2^{38} \pmod{55}$

2 y 55 son coprimos $\Rightarrow$ podemos aplicar el teorema de Euler

$55 = 5 \cdot 11$

$\varphi(55) = \varphi(5 \cdot 11) = \varphi(5)\varphi(11) = 4 \cdot 10 = 40$

entonces, por el teorema de Euler: $2^{40} \equiv 1 \pmod{55}$

$2^{40} \equiv 1 \pmod{55}$

$2^{40} \cdot 2^{-1} \cdot 2^{-1} \equiv 2^{-1} \cdot 2^{-1} \pmod{55}$

$2^{38} \equiv 28 \cdot 28 \pmod{55}$

$2^{38} \equiv 14 \pmod{55}$

Otra forma

$r \equiv 2^{38} \pmod{55} \overset{TCR}{\iff} \begin{cases} r \equiv 2^{38} \pmod{5} \\ r \equiv 2^{38} \pmod{11} \end{cases}$

$55 = 5 \cdot 11$

(c) Hallar un entero $0 \leq m < 297$, tal que $m \equiv 30^{132} \pmod{297}$.

$297 = 3 \cdot 99 = 3 \cdot 3^2 \cdot 11 = 3^3 \cdot 11 = 27 \cdot 11$

$$m \equiv 30^{132} \pmod{297} \overset{TCR}{\iff} \begin{cases} m \equiv 30^{132} \pmod{27} \\ m \equiv 30^{132} \pmod{11} \end{cases}$$

* $m \equiv 30^{132} \pmod{27} \iff m \equiv 3^{132} \pmod{27}$

30 y 27 no son coprimos entonces no podemos aplicar el teorema $\iff m \equiv \underbrace{3^3}_{27} \cdot 3^{129} \pmod{27}$

$\iff m \equiv 0 \pmod{27}$

* $m \equiv 30^{132} \pmod{11} \iff m \equiv 8^{132} \pmod{11}$

8 y 11 son coprimos, entonces podemos aplicar el teorema de Euler

$\varphi(11) = 10$

entonces por Euler tenemos $8^{10} \equiv 1 \pmod{11}$

$132 = 13 \cdot 10 + 2$

$$\begin{aligned} 8^{132} &\equiv 8^{13 \cdot 10 + 2} \pmod{11} \\ &\equiv \underbrace{(8^{10})^{13}}_{\equiv 1 \pmod{11}} \cdot 8^2 \pmod{11} \\ &\equiv 8^2 \pmod{11} \\ &\equiv 64 \pmod{11} \\ &\equiv 9 \pmod{11} \end{aligned}$$

$\boxed{m \equiv 9 \pmod{11}}$

$$m \equiv 30^{132} \pmod{297} \overset{TCR}{\iff} \begin{cases} m \equiv 30^{132} \pmod{27} \\ m \equiv 30^{132} \pmod{11} \end{cases}$$

$$\iff \begin{cases} m \equiv 0 \pmod{27} \\ m \equiv 9 \pmod{11} \end{cases} \rightarrow \overset{+27}{0} \overset{+27}{,27} \overset{+27}{,54} ,81, 108$$

× × × × ✓

$m \equiv 0 \pmod{27} \longrightarrow m = 27x$

$m \equiv 9 \pmod{11} \longrightarrow m = 11y + 9$

entonces $27x = 11y + 9$

$$\boxed{27x - 11y = 9}$$

vamos a buscar una solución particular:

→ identidad de Bezout para 27 y 11:

$27 = 2 \cdot 11 + 5$ → $1 = 11 - 2 \cdot 5$

$11 = 2 \cdot 5 + 1$ → $1 = 11 - 2(27 - 2 \cdot 11)$

$1 = 27(-2) + 11 \cdot 5$

$27(-2) - 11(-5) = 1$ $\times 9$

$27(-18) - 11(-45) = 9$

→ solución particular: $\begin{cases} x_0 = -18 \\ y_0 = -45 \end{cases}$

una solución particular de $\begin{cases} m \equiv 0 \pmod{27} \\ m \equiv 9 \pmod{11} \end{cases}$

es $m_0 = 27x_0 = 27(-18) = -486$

entonces por el TCR

$$\begin{cases} m \equiv 0 \pmod{27} \\ m \equiv 9 \pmod{11} \end{cases} \iff m \equiv -486 \pmod{297}$$

$\iff m \equiv -486 + 2 \cdot 297 \pmod{297}$

$\iff m \equiv 108 \pmod{297}$

Ejercicio 13. Un número natural se dice *perfecto* si es igual a la suma de todos sus divisores positivos propios. Por ejemplo, 6 es perfecto pues: $6 = 1 + 2 + 3$.

a. Verificar que 28 y 496 son perfectos.

b. Probar que si $2^m - 1$ es primo entonces $2^{m-1}(2^m - 1)$ es perfecto.

b) $2^m - 1$ es primo

$p = 2^m - 1$

queremos ver que $2^{m-1} p$ es perfecto

divisores de $2^{m-1} p$: $1, 2, 2^2, 2^3, \dots, 2^{m-1}$

positivos

$p, 2p, 2^2 p, 2^3 p, \dots, 2^{m-1} p$ ← no es propio

sumamos los divisores positivos propios de $2^{m-1} p$:

$$1 + 2 + 2^2 + 2^3 + \dots + 2^{m-1} + p + 2p + 2^2 p + 2^3 p + \dots + 2^{m-2} p$$

$$= 1 + 2 + 2^2 + \dots + 2^{m-1} + p(1 + 2 + 2^2 + \dots + 2^{m-2})$$

$$= \frac{2^m - 1}{2 - 1} + p\left(\frac{2^{m-1} - 1}{2 - 1}\right)$$

$$= 2^m - 1 + p(2^{m-1} - 1) \qquad p = 2^m - 1$$

$$= 2^m - 1 + p 2^{m-1} - p$$

$$= \cancel{p} + p 2^{m-1} - \cancel{p}$$

$$= p 2^{m-1}$$

Teorema 2.6.3. *Si* $\mcd(m,n)=1$, $\varphi(mn)=\varphi(m)\varphi(n)$.

Demostración. Como la tesis es obvia si m o n es 1, demostrémoslo para $m,n>1$. La idea de la demostración es la siguiente: daremos dos conjuntos C y D tales que $\#C=\varphi(mn)$ y $\#D=\varphi(m)\varphi(n)$, y luego construiremos una función biyectiva $f:C\to D$ lo cual terminaría probado que $\#C=\#D$; es decir que $\varphi(mn)=\varphi(m)(n)$.

Sea $C=\{c\in\{0,\cdots,mn-1\}:\mcd(c,mn)=1\}$; claramente $\#C=\varphi(mn)$. Además, tenemos que

$$\mcd(c,mn)=1\Leftrightarrow \mcd(c,m)=1 \text{ y } \mcd(c,n)=1. \tag{2.6.4}$$

Así que $C=\{c\in\{0,\cdots,mn\}:\mcd(c,m)=1 \text{ y } \mcd(c,n)=1\}$.

Sean $A=\{a\in\{0,\cdots,m-1\}:\mcd(a,m)=1\}$ y $B=\{b\in\{0,\cdots,n-1\}:\mcd(b,n)=1\}$; tenemos que $\#A=\varphi(m)$, $\#B=\varphi(n)$ y por lo tanto si $D=A\times B=\{(a,b):a\in A,\ b\in B\}$ tenemos que $\#D=\varphi(m)\varphi(n)$.

Consideramos ahora la función $f:C\to D$ dada por $f(c)=(a,b)$ siendo a el resto de dividir c entre m y b el resto de dividir c entre n. Es decir $f(c)=(a,b)$ con $a\in\{0,\cdots,m-1\}$, $b\in\{0,\cdots,n-1\}$ y

$$\begin{cases} c\equiv a \pmod m \\ c\equiv b \pmod n. \end{cases}$$

Veamos primero que efectivamente, si $c\in C$ y $f(c)=(a,b)$ entonces $(a,b)\in D$. Como $c=mq+a$ y $c=nq'+b$ tememos (por la Proposición 1.2.6) que

$$\mcd(c,m)=\mcd(a,m) \text{ y } \mcd(c,n)=\mcd(b,n). \tag{2.6.5}$$

Por lo tanto si $\mcd(c,m)=1$ y $\mcd(c,n)=1$ tenemos que $\mcd(a,m)=1$ y $\mcd(b,n)=1$. Como además claramente $a\in\{0,\cdots,m-1\}$ y $b\in\{0,\cdots,n-1\}$ concluimos que $(a,b)\in D$.

Veamos ahora que la función f es biyectiva. Para ésto tenemos que ver que dado $(a,b)\in D$, existe un único $c\in C$ tal que $f(c)=(a,b)$ (la existencia de c nos da la sobreyectividad de f y la unicidad nos da la inyectividad de f). Tenemos que probar entonces que dado $(a,b)\in D$, existe un único $c\in C$ tal que

$$\begin{cases} c\equiv a \pmod m \\ c\equiv b \pmod n. \end{cases} \tag{2.6.6}$$

Como $\mcd(m,n)=1$, por el Teorema Chino del Resto sabemos que el sistema

$$\begin{cases} x\equiv a \pmod m \\ x\equiv b \pmod n. \end{cases}$$

tiene solución x_0 y que además, todas las soluciones son $x\equiv x_0 \pmod{mn}$. Por lo tanto, existe un único $c\in\{0,\cdots,mn-1\}$ que verifica (2.6.6). Resta ver que efectivamente este $c\in C$: como $\mcd(a,m)=1$, $\mcd(b,n)=1$ y $c\equiv a \pmod m$, $c\equiv b \pmod n$, por (2.6.5) tenemos que

$$\mcd(c,m)=1 \text{ y } \mcd(c,n)=1$$

y por lo tanto $c\in C$.

Teorema: m y n coprimos $\Rightarrow \varphi(mn)=\varphi(m)\varphi(n)$

$A=\{a\in\{0,\cdots,m-1\}:\mcd(a,m)=1\}$

$\varphi(m)=\#A$

$B=\{b\in\{0,\cdots,n-1\}:\mcd(b,n)=1\}$

$\varphi(n)=\#B$

$C=\{c\in\{0,\cdots,mn-1\}:\mcd(c,mn)=1\}$

$\varphi(mn)=\#C$

(a,b) con $a\in A$, $b\in B$

$\varphi(mn)=\varphi(m)\varphi(n) \iff \#C=\#A\times\#B=\#A\times B$

Queremos probar que $\#C=\#A\times B$

para eso vamos a construir una función

$$f : C \longrightarrow A \times B$$

que sea biyectiva.

Vamos a definir:

$$C = \{c \in \{0, \dots, mn-1\} : mcd(c, mn) = 1\}$$

$$A = \{a \in \underbrace{\{0, \dots, m-1\}}_{\text{posibles restos al dividir entre } m} : mcd(a, m) = 1\} \qquad B = \{b \in \underbrace{\{0, \dots, n-1\}}_{\text{posibles restos al dividir entre } n} : mcd(b, n) = 1\}$$

$f(c) = (\alpha, \beta)$ donde α es el resto de dividir c entre m

β es el resto de dividir c entre n

es decir $\begin{cases} c \equiv \alpha \pmod m \\ c \equiv \beta \pmod n \end{cases}$

① vamos a verificar que $f(c) = (\alpha, \beta) \in A \times B$ (el A sobre α)

→ tenemos que $\alpha \in \{0, \dots, m-1\}$, nos falta ver que $mcd(\alpha, m) = 1$

$$c = mq + \alpha$$

$$mcd(\alpha, m) = mcd(mq + \alpha, m) = mcd(c, m) = 1 \quad (\text{porque } mcd(c, mn) = 1)$$

→ tenemos que $\beta \in \{0, \dots, n-1\}$, nos falta ver que $mcd(\beta, n) = 1$

$$c = nq' + \beta$$

$$mcd(\beta, n) = mcd(nq' + \beta, n) = mcd(c, n) = 1$$

② f es biyectiva (existe c $\leftarrow$ (a, b))

$$f : C \longrightarrow A \times B$$

$$c \longmapsto (\alpha, \beta) \quad \text{tal que} \begin{cases} c \equiv \alpha \pmod m \\ c \equiv \beta \pmod n \end{cases}$$

Queremos ver que para todo $(\alpha, \beta) \in A \times B$ existe un único $c \in C$ tal que $f(c) = (\alpha, \beta)$.

es decir dado $(\alpha, \beta) \in A \times B$ queremos ver que hay un único $c \in C = \{c \in \{0, \dots, mn-1\} : mcd(c, mn) = 1\}$ tal que

$$\begin{cases} c \equiv \alpha \pmod m \\ c \equiv \beta \pmod n \end{cases}$$

↑ incógnita

Como m y n son coprimos por el TCR

$$\begin{cases} c \equiv \alpha \pmod m \\ c \equiv \beta \pmod n \end{cases} \iff c \equiv x_0 \pmod{mn}$$

existe un único $c \in \{0, \dots, mn-1\}$ que verifica

nos falta ver que $mcd(c, mn) = 1$

$$\left.\begin{array}{l} c \equiv \alpha \pmod m \\ mcd(\alpha, m) = 1 \end{array}\right\} \Rightarrow mcd(c, m) = 1$$

$$\left.\begin{array}{l} c \equiv \beta \pmod n \\ mcd(\beta, n) = 1 \end{array}\right\} \Rightarrow mcd(c, n) = 1$$

$$\Rightarrow mcd(c, mn) = 1$$

Entonces $f : C \to A \times B$ es biyectiva

Por lo tanto $\#C = \#A \times B$

$$\varphi(mn) = \varphi(m)\varphi(n)$$

$$\begin{cases} c \equiv \alpha \pmod m \longrightarrow c = mq + \alpha \\ mcd(\alpha, m) = 1 \end{cases}$$

$$mcd(c, m) = mcd(mq + \alpha, m) = mcd(mq + \alpha - mq, m) = mcd(\alpha, m) = 1$$

$$mcd(x, y) = mcd(sx + ty, y)$$