Teórica 28/05

T.C.R

Dado un sistema

$$\begin{cases} a_1 X \equiv c_1 \ (m_1) \\ a_2 X \equiv c_2 \ (m_2) \\ a_n X \equiv c_n \ (m_n) \end{cases}$$

Obs: Si alguna ecuación no tiene sol., el sistema no tiene solución. En este caso, el sistema no tiene solución cuando

$\exists i \ / \ (a_i : m_i) \nmid c_i$ (Fin)

Si esto no ocurre, (es decir, $\forall i$ $(a_i : m_i) \mid c_i$) Entonces podemos coprimarizando c/ecuación, podemos suponer que $(a_i : m_i) = 1 \ \forall i$

Ademas c/e.c (individualmente) tiene sol.

$$X \equiv c_i' \ (m_i)$$

En conclusión, el sistema es equivalente a un sistema de la forma

$$\begin{cases} X \equiv c_1' \ (m_1) \\ X \equiv c_2' \ (m_2) \\ X \equiv c_n' \ (m_n) \end{cases}$$

Aumentando la cant. de ecuaciones podemos llegar a un sistema con m_i coprimos $\dots \ m_i = \prod_{j=1}^{t} p_j^{r_j}$

$$X \equiv c_i' \ (m_i)$$

es equivalente al sistema

$$\begin{cases} X \equiv c_i' \ (p_1^{r_1}) \\ X \equiv c_i' \ (p_2^{r_2}) \\ X \equiv c_i' \ (p_{tt}^{r_t}) \end{cases}$$

Obs: Los m_i son coprimos 2 a 2 $\iff$ Los primos que aparecen en la descomposición de m_i no aparecen en la de m_j $(j \neq i)$

$\therefore$ si los m_i, $1 \leq i \leq m$ no son coprimos 2 a 2, en el sistema (*) amplificado, tendremos ec. de la forma

$$X \equiv c_i' \ (p^{r_i})$$

$$X \equiv c_j \ (p^{r_H})$$

Esto puede o no tener solución, se ve lo que se hace antes de resolver el sistema (grande), resolvemos 1º los subsistemas que tienen el mismo primo

Si alguno de estos subsistemas no tiene sol, entonces el sist. grande (original) no tiene sol.

Si todos los subsist. tienen sol., ellas serán de la forma

$$X \equiv c_i'' \ (p^{r_G})$$

con r_G la máx potencia de p que aparece en el sistema

Luego de hacer todo esto:

$$\begin{cases} X \equiv d_1 \ (\widetilde{m_1}) \\ \vdots \\ X \equiv d_n \ (\widetilde{m_n}) \end{cases}$$

donde $\widetilde{m_i}$ son coprimos 2a (y podemos usar el T.C.R)

Ej:
$$\begin{cases} X \equiv 1 \ (4) \\ X \equiv 2 \ (8) \\ X \equiv 3 \ (8) \end{cases}$$

PUEDE o NO TENER SOLUCIÓN

Es equivalente al sistema

$$\begin{cases} X \equiv 1 \ (2) \\ X \equiv 1 \ (3) \\ X \equiv 2 \ (8) \\ X \equiv 3 \ (7) \\ X \equiv 3 \ (7) \end{cases}$$

≡ = equivalente = ≡ ≡ $(a+b)^p \equiv a^p + b^p \ (p)$

⟹

$X \equiv 1 \ (2)$ Para c/ primo resolvemos su sub-sist.
$X \equiv 2 \ (8)$
$X \equiv 7 \ (2)$
$X \equiv 1 \ (3)$
$X \equiv 7 \ (9)$

Potencias

$$\begin{cases} X \equiv 1 \ (2) \\ X \equiv 2 \ (8) \\ X \equiv 7 \ (2) \end{cases} \text{ es } \equiv \text{ a } \begin{cases} X \equiv 1 \ (2) \\ X \equiv 2 \ (8) \end{cases}$$

$X \equiv 2 \ (8) \Rightarrow X = 2 + 8k$

Pero $2 + 8k \equiv 0 + 0k \equiv 0 \ (2)$
$\not\equiv X \equiv 1 \ (2)$

Entonces $2 + 8k$ no resuelve la ec. $X \equiv 1 \ (2)$
⟹ El sist no tiene solución

Si bien no hace falta hacemos el caso

$X \equiv 1 \ (3)$
$X \equiv 7 \ (9)$

$\Rightarrow X = 7 + 9k \to 7 + 9k \equiv 1 + 0 \ (3)$

Entonces $7 + 9k$ resuelve la 1ra ecuación

Entonces el subsistema

$$\begin{cases} X \equiv 1 \ (3) \\ X \equiv 7 \ (9) \end{cases} \equiv \text{ a } X \equiv 7 \ (9)$$

(primo a la max potencia)

Si hubiese otro ...

$$\begin{cases} \alpha \ (8) \\ \beta \ (9) \end{cases} \text{ por } 7$$

⟹ TCR

Teorema de Fermat y Test de Primalidad

T. de F.

1) Si p primo $\wedge$ $(a : p) = 1$ entonces $a^{p-1} \equiv 1 \ (p)$

2) Si p primo $a^p \equiv a \ (p)$

Veamos que 1) y 2) son ≡ (equivalentes)

Si vale 1) multiplicando por a ambos lados nos queda 2).

Para la vuelta, si vale 2)

$a^p \equiv a \ (p) \Rightarrow p \mid a^p - a \Rightarrow p \mid a(a^{p-1} - 1)$

$(\text{si } (a : p) = 1) \Rightarrow p \mid a^{p-1} - 1$

Obs (muy simple)

$aX \equiv 1 \ (p)$ tiene !

Tiene solución x con $1 \leq x < p$

En particular $aX \equiv 1 \ (p)$ con $1 \leq a < p$ tiene ! solución x con $1 \leq x < p$

Dem de Fermat

Veremos que 2) es cierto, por inducción

$0^p = 0 \equiv 0 \ (p)$ caso $n = 0$ vale

$1^p = 1 \equiv 1 \ (p)$ caso $n = 1$ vale

Supongamos vale para n, veamos que vale para $n+1$

$(n+1)^p \equiv n^p + 1^p \ (p)$

Por HI. $n^p \equiv n \ (p)$

$(n+1)^p \equiv n^p + 1^p \equiv n + 1 \ (p)$

Asamblea

Otra demostración (mucho mejor).

En este caso veremos que vale 1

Hecho clave

Si p primo $\wedge$ $(a:p)=1$ Entonces el cjto $\{a, a.2, a.3, \dots, a(p-1)\}$ de $p-1$ elementos

Cuando tomamos congruencia mod. p tiene $p-1$ elementos, es decir, que tomando $\equiv (p)$ el cjto es $\{1,2,3,\dots,p-1\}$

Si $1 \leq i < j < p$ entonces

$a.i \not\equiv a.j \ (p)$

"(RAA)" Supongamos

$a.i \equiv a.j \ (p)$

$\Rightarrow a(j-i) \equiv 0 \ (p)$

$\Rightarrow p \mid j-i \Rightarrow j = i$ (Abs)

DEM. DE FERMAT (2.0)

a^{p-1}

$(a.1)(a.2)(a.3)\dots(a.(p-1)) \equiv 1.2.3\dots(p-1) \pmod p$

$a^{p-1}.2.3\dots(p-1) \equiv (p-1)! \pmod p$

$a^{p-1}.(p-1)! \equiv (p-1)! \pmod p$

Como p primo $\wedge$ $(p:(p-1)!)=1 \Rightarrow a^{p-1} \equiv 1 \ (p)$ a

HAY QUE JUSTIFICAR ESTO

$a^{p-1}.(p-1)! - (p-1)! \equiv 0 \ (p)$

$(a^{p-1}-1).(p-1)! \equiv 0 \ (p)$

$\Rightarrow p \mid (a^{p-1}-1).(p-1)!$

Y como $(p:(p-1)!)=1$

$\Rightarrow p \mid (a^{p-1}-1)$ como una dem. anterior

COMENTARIO. TEO. DE EULER

Def. Función φ de Euler

$\varphi(n)$ = la cant. de naturales $\leq n$ coprimos con n

$\varphi(n) = |\{a \in \mathbb{N} : (a:n)=1\}|$

1) Si p primo $\varphi(p) = p-1$

2) $\varphi(p^k) = p^{k-1}(p-1)$

3) Si $(m:n)=1$ entonces $\varphi(m.n) = \varphi(m).\varphi(n)$

(Obs 1), 2), 3) permiten calcular la $\varphi(n)$ $\forall n$

$\varphi(30) = \varphi(2.3.5) = \varphi(2).\varphi(3).\varphi(5) = 1.2.4 = 8$

Teorema de Euler

Si $(a:n)=1$ entonces

$a^{\varphi(n)} \equiv 1 \ (n)$

Vemos que si $\{x_1, x_2, \dots, x_{\varphi(n)}\}$ son los nº entre 1 y n coprimos con n, entonces

$\{ax_1, ax_2, \dots, ax_{\varphi(n)}\}$ congruencia mód. n a $\{x_1, x_2, \dots, x_{\varphi(n)}\}$

y repetir la 2ª dem. del teo. de Fermat

Test de Primalidad

Teorema de Wilson:
Dado $n \in \mathbb{N}$, n es primo $\Leftrightarrow (n-1)! \equiv -1 \ (n)$

El test es malo computacionalmente (hay que hacer mil cuentas)

Dem ②

Otro test:
Fermat
Dado $n \in \mathbb{N}$, elegir a entre 1 y $n-1$ y calcular $a^n \equiv ? \ (n)$

Si $a^n \not\equiv a \ (n) \Rightarrow n$ no es primo

Si $a^n \equiv a \ (n)$ ~~n~~ (n tiene chance de ser primo) para el test porque con el número a. Repetir para ~~los~~ todos los valores de a

Atención Puede ocurrir que $a^n \equiv a \ (n) \ \forall 1 \leq a < n$
(osea n para el test siempre)
Pero n puede ser compuesto.

¡COMPUESTO!

Ej 561 es el primero de estos números. Los n que pasan el test de Fermat $\forall \ 1 \leq a < n$ se llaman Nº de Carmichel

$\exists \infty$ de estos

Parece que $C(x) = |\{n \in \mathbb{N} \ / \ n \leq x \ \text{y} \ n \text{ de Carmichel}\}| > x^{2/7}$
(para x grande)

hay log n primos
n