$\mathbb{F}_p^2$, EL TEST DE LUCAS-LEHMER, NÚMEROS CUADRÁTICOS DE MERSENNE Y DE FERMAT

Pendiente de la Clase pasada:

PM2. *Si q es un divisor de 2^p-1, donde p es primo, entonces $q \equiv 1 \pmod{2p}$*

Demostración Supongamos que q divide a $2^p - 1$. Entonces

$$2^p \equiv 1 \pmod{q} \Rightarrow 2 \text{ ord}_q(2) = p \text{ (porque } q \geq 3) \Rightarrow p/q - 1.$$

Pero $q \equiv 1 \pmod{p}$ y $q \equiv 1 \pmod{2} \Rightarrow q \equiv 1 \pmod{2p}$ $\square$

PM3. *Si q es un divisor de $2^k - 1$, donde $k \geq 3$ es impar, entonces $q \equiv \pm 1 \pmod{8}$.*

Demostración: Supongamos que q divide a $2^k - 1$. Entonces

$$2^k \equiv 1 \pmod{q} \Rightarrow (\frac{2^k}{q}) = (\frac{1}{q}) = 1.$$

Como k es impar se tiene

$$(\frac{2}{q}) = (\frac{2}{q})^k = (\frac{2^k}{q}) = 1$$

y el resultado sigue de LRC.

Alternativa:

$$2^k \equiv 1 \pmod{q} \Rightarrow 2^{k+1} \equiv 2 \pmod{q} \Rightarrow (2^{\frac{k+1}{2}}) \overset{\equiv}{} 2 \pmod{q}$$

por lo que 2 es un cuadrado módulo q y sigue que $(\frac{2}{q}) = 1$ $\square$.

El teorema de Proth:

Sean A y t enteros positivos, $A < 2^t$ impar. Sea $n = 1 + A2^t$ y $a \in \mathbb{Z}$ tal que $(\frac{a}{n}) = -1$, donde $(\frac{\cdot}{n})$ denota el símbolo de Jacobi. Las siguientes afirmaciones son equivalentes:

(1) *n es primo*

(2) $(a^{\frac{n-1}{2}}) \equiv -1 \pmod{n}$

Demostración: $(a) \Rightarrow (b)$ es consecuencia de la propiedad de Euler del símbolo de Legendre (PSL2).

$(b) \Rightarrow (a)$: Sea p un divisor de n. La hipótesis implica que

$$(a^{\frac{n-1}{2}}) \equiv -1 \pmod{p}$$

,

de donde $(a^A)^{2^{t-1}} \equiv -1 \pmod{p}$. Se deduce que el orden de a^A módulo p es 2^t (por qué?);

sigue que 2^t divide a $p-1 = |\mathbb{Z}_p^*|$, es decir que

$$p \equiv 1 \pmod{2^t} \Rightarrow p > 2^t > \sqrt{n},$$

donde la última desigualdad se deduce de $A < 2^t$ y $n = 1 + A2^t$.

Pero $p > \sqrt{n}$ $\forall$ divisor primo p de $n \Rightarrow n$ es compuesto $\square$

Ejercicio 5

(1) Demuestre que la conclusión del Teorema de Proth se cumple bajo la hipótesis $A \leq 3 + 2^{t+1}$.

(Sugerencia: Si n es compuesto $n = d\ d'$, ambos $\equiv 1 \pmod{2^t}$).

1. Extensiones cuadráticas de $\mathbb{Z}_p$. El Test de Lucas-Lehmer

Sea p un primo impar $\mathbb{Z}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$ el cuerpo de las clases de enteros mod p. Sea $a \in \mathbb{Z}$.

Si $(\frac{a}{p}) = -1$ La imagen del polinomio $x^2 - a$ en $\mathbb{Z}_p[x]$ es irreducible.

El cociente $K = \frac{\mathbb{Z}_p[x]}{(x^2-a)}$ es una extensión cuadrática de $\mathbb{Z}_p$.

K es isomorfo a $\frac{\mathbb{Z}[x]}{(p,x^2-a)} \backsimeq \mathbb{Z}_p(\sqrt{a}) = \{x + y\sqrt{a} | x, y \in \mathbb{Z}_p\}$.

$\mathbb{Z}_p^*$ es cíclico de orden $p^2 - 1 \Rightarrow \alpha^{p^2-1} = 1\ \forall \alpha \in \mathbb{Z}_p^*$.

Equivalentemente $\alpha^{p^2} = \alpha\ \forall\ \alpha \in \mathbb{Z}_p$.

La función $e(p)$ (elevar a la p) es un automorfismo no trivial (por qué?) de K que fija a $\mathbb{Z}_p$ (por qué?).

Sigue que $e(p)(\alpha) = \bar{\alpha}\ \forall\ \alpha \in \mathbb{Z}_p$.

Alternativa: $(x+y\sqrt{a})^p = (x^p + y^p\sqrt{a}^p) = (x + ya^{\frac{p-1}{2}}\sqrt{a}) = (x - y\sqrt{a})$

El símbolo cuadrático en $\mathbb{Z}[\sqrt{a}]$

Sea p un primo impar y sea $a \in \mathbb{Z}$ un no residuo cuadrático mod p.
Sea $\alpha = x + y\sqrt{a} \in \mathbb{Z}[\sqrt{a}]$.
El símbolo cuadrático se define como

$$[\frac{\alpha}{p}] \equiv \alpha^{\frac{p^2-1}{2}} \pmod{p}$$

Satisface la propiedad con la que se definió el SL:

$$[\frac{\alpha}{p}] := \begin{cases} 1, \text{ si existe } x \in \mathbb{Z}[\sqrt{a}] \text{ tal que } x^2 = \alpha \\ -1, \text{ si no} \end{cases}$$

También es el único caracter cuadrático de K^*.
La propiedad más relevante:

$$[\frac{\alpha}{p}] \equiv \alpha^{\frac{p^2-1}{2}} \pmod{p} \equiv (\bar{\alpha}/\alpha)^{\frac{p+1}{2}} \pmod{p} \equiv (\alpha\bar{\alpha})^{\frac{p-1}{2}} \pmod{p} = (\frac{\alpha\bar{\alpha}}{p})$$

Del mismo en el que el el símbolo de Legendre se extiende al de Jacobi, así mismo se extiende el símbolo cuadrático definido arriba.

Teorema (El Test de Lucas-Lehmer).

Sea p un primo impar. Sea $M_p = 2^p - 1$ un número de Mersenne. Sean $\alpha = 1 + \sqrt{3}$ y $\beta = -2 + \sqrt{3} \in \mathbb{Z}[\sqrt{3}]$

Las siguientes afirmaciones son equivalentes:

(1) *M_p es primo.*
(2) $\alpha^{\frac{p^2-1}{2}} \equiv -1 \pmod{M_p}$
(3) $\beta^{2^{p-1}} \equiv -1 \pmod{M_p}$
(4) *La sucesión de enteros S_k definida por:*

$S_0 = 4$;
$S_{k+1} = S_k^2 - 2$ *si* $k \geq 0$, *satisface*
$S_{p-2} \equiv 0 \pmod{M_p}$.

El Teorema es un casi particular del Teorema Lucasiano. Este lo enunciaremos en términos similares a los del Teorema de Proth.

Teorema Lucasiano
Sea $n = A2^t - 1$, $A < 2^t$. Sea $a \in \mathbb{Z}_n^*$ tal que el símbolo de Jacobi $(\frac{a}{n}) = -1$. Sea $\alpha \in Z_n(\sqrt{a})^*$ tal que $[\frac{\alpha}{n}] = -1$.

Los siguientes son equivalentes:

(1) n *es primo*
(2) $[\frac{\alpha}{n}] \equiv \alpha^{\frac{n^2-1}{2}} \pmod{n}$
(3) $(\bar{\alpha}/\alpha)^{\frac{n+1}{2}} \equiv -1 \pmod{n}$
(4) *La sucesión de enteros definida por* $S_0 \equiv \bar{\alpha}/\alpha)^A + (\alpha/\bar{\alpha})^A \mod n$;

$$S_{k+1} = S_k^2 - 2 \text{ satisface } S_{t-2} \equiv 0 \pmod{n}$$

Demostración:

(1) $\Longrightarrow$ (2) : Sigue de la hipótesis $[\frac{\alpha}{n}] = -1$ y de la definición del símbolo.

(1) $\Longrightarrow$ (3) : Como (1) $\Longrightarrow$ (2) tenemos $[\frac{\alpha}{n}] \equiv \alpha^{\frac{n^2-1}{2}} \pmod{n}$

$\equiv (\alpha^{n-1})^{\frac{n+1}{2}} \pmod{n} equiv (\bar{\alpha}/\alpha)^{\frac{n+1}{2}} \equiv -1 \pmod{n}$.

(3) $\Longrightarrow$ (4) : Se verifica que la sucesión $T_k := ((\bar{\alpha}/\alpha)^A)^{2^k} + ((\alpha/\bar{\alpha})^A)^{2^k}$ satisface $T_k \equiv S_k \pmod{n}$ $\forall k \geq 0$.

Sigue de (3) que $S_{t-1} \equiv -2 \pmod{n}$ y $S_{t-2} \equiv 0 \pmod{n}$.