Enrique R. Aznar García
eaznar@ugr.es

RANGO DE UN NÚMERO PARA UNA SUC. DE LUCAS

Dados $P, Q \in \mathbb{Z}$, con $d = P^2 - 4Q$ no cuadrado perfecto, sus s.L. se definen por las ecuaciones

$$\begin{cases} V_n = PV_{n-1} - QV_{n-2} \\ U_n = PU_{n-1} - QU_{n-2} \end{cases}$$

con las condiciones iniciales $V_0 = 2, U_0 = 0, V_1 = P, U_1 = 1$.

Dado un entero n, se define su **rango $w(n)$** para $P, Q \in \mathbb{Z}$, con $d = P^2 - 4Q$ no cuadrado perfecto, como el primer índice e distinto de cero tal que $U_e \equiv 0 \pmod{n}$.

La primera propiedad del rango es que **si existe $w(n)$, entonces $n|U_r \Leftrightarrow w(n)|r$**.

Por tanto, si $p \in \mathbb{Z}$ es primo, el TPF para enteros cuadráticos nos asegura que existe $w(p)$ para todo P, Q, con $d = P^2 - 4Q$ no cuadrado perfecto, y debe ser un divisor de $p - \left(\frac{d}{p}\right)$.

A continuación demostraremos que existe $w(n)$ para todo $n \in \mathbb{Z}$ y que si existe una s.L., $\{U_i\}_{i \in \mathbb{N}}$, tal que $w(n) = n - \left(\frac{d}{n}\right)$ entonces n es primo (la s.L. es el análogo a un elemento primitivo para n).

RANGO DE UNA POTENCIA DE PRIMO

Por inducción, para $t \geq 2$, suponemos que $w(p^{t-1})$ existe y que divide a $e = p^{t-2}\left(p - \left(\frac{d}{n}\right)\right)$. Como

$$\left(\frac{V_e + U_e\sqrt{d}}{2}\right)^p = \alpha^{ep} = \frac{V_{ep} + U_{ep}\sqrt{d}}{2} \Leftrightarrow 2^{p-1}\left(V_{ep} + U_{ep}\sqrt{d}\right) = \left(V_e + U_e\sqrt{d}\right)^p$$

Si desarrollamos la potencia p-ésima, vemos que el coeficiente de $\sqrt{d}$ es

$$pV_e^{p-1}U_e + \binom{p}{3}V_e^{p-3}U_e^3 d + \binom{p}{5}V_e^{p-5}U_e^5 d^2 + \cdots + U_e^p d^{(p-1)/2}$$

como cada coeficiente binomial es múltiplo de p (por ser primo), entonces cada sumando es múltiplo de p^t.

Como p no divide a 2^{p-1}, entonces p^t divide a U_{ep} y hemos demostrado el

TEOREMA

Sea $\{U_i\}_{i\in\mathbb{N}}$ la s.L. determinada por P, Q y sea p primo, $(p, 2Q) = 1$.
Entonces, $w(p^t)$ existe y divide a $p^{t-1}\left(p - \left(\frac{d}{n}\right)\right)$.

RANGO DE UN NÚMERO COMPUESTO

Si $\{U_i\}_{i\in\mathbb{N}}$ es una s.L. determinada por P, Q y $n = p_1^{e_1} \cdots p_r^{e_r}$, con$(n, 2Q) = 1$.
Entonces, para cada i por el teorema anterior, $p_i^{e_i}$ divide a $U_{kp_i^{e_i-1}\left(p_i - \left(\frac{d}{n}\right)\right)}$ para todo $k > 1$.

Como son primos diferentes, n divide a U_s, donde s es el mínimo común múltiplo de los $p_i^{e_i-1}\left(p_i - \left(\frac{d}{n}\right)\right)$.

Por tanto, $w(n)$ existe y divide a ese mcm y hemos demostrado el

COROLARIO

Para cualquier s.L., si $n = p_1^{e_1} \cdots p_r^{e_r}$ es compuesto, $w(n)$ existe y divide al mcm de los $p_i^{e_i-1}\left(p_i - \left(\frac{d}{n}\right)\right)$.

COROLARIO

Si encontramos una s.L. $\{U_i\}_{i\in\mathbb{N}}$ determinada por P, Q, con $d = P^2 - 4Q$ no cuadrado perfecto y $n \in \mathbb{Z}$ satisface $(n, 2Qd) = 1$ y $w(n) = n \pm 1$. Entonces, n es primo.

Por reducción al absurdo, si n es divisible por 2 o mas primos, el corolario anterior nos dice que $w(n) < n - 1 \leq n \pm 1$ que contradice la hipótesis.

Si $n = p^t$, con $t > 1$, por un teorema anterior $w(n)$ es un divisor de $p^{t-1}\left(p - \left(\frac{d}{n}\right)\right) = p^t \pm p^{t-1}$.
Pero $n \pm 1 = p^t \pm 1$ no puede dividirlo. Y también contradice la hipótesis.

PRIMOS EN ENTEROS CUADRÁTICOS

Si p es un primo impar y d no es un residuo cuadrático módulo p (i.e. $\left(\frac{d}{p}\right) = -1$).
Si p divide a $(a + b\sqrt{d})(f + g\sqrt{d}) = af + bgd + (bf + ag)\sqrt{d})$,
entonces también divide a $(a - b\sqrt{d})(f - g\sqrt{d}) = af + bgd - (bf + ag)\sqrt{d})$.

Por tanto, p^2 divide a $(a^2 - db^2)(f^2 - dg^2)$ y así p divide a uno de los dos, por ej a $a^2 - db^2$.
Ahora, si p no divide a b, existe el inverso de $b \pmod{p}$ y en consecuencia
$(ab^{-1})^2 \equiv d \pmod{p}$ lo que contradice la hipótesis. Necesariamente, p divide a b y como divide a $a^2 - db^2$, también dividirá a a como queríamos. Así,

LEMA

Si p primo impar con $\left(\frac{d}{p}\right) = -1$. Entonces, si p divide a $(a + b\sqrt{d})(f + g\sqrt{d})$ divide a uno de los dos factores.

COROLARIO

Si p primo impar con $\left(\frac{d}{p}\right) = -1$. Entonces, p sigue siendo primo en el anillo
$A = O_{\sqrt{d}} = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, de enteros cuadráticos en $\mathbb{Q}[\sqrt{d}]$. En particular, el anillo cociente
$K = A/pA$ es cuerpo.

EL CUERPO COCIENTE

Si p primo impar con $\left(\frac{d}{p}\right) = -1$. Entonces, como existe $2^{-1} \pmod{p}$, todo elemento del cuerpo cociente

$$K = \frac{O_{\sqrt{d}}}{(p)}$$

tiene un representante $a + b\sqrt{d}$, con $a, b \in \{0, 1, \ldots, p-1\}$. Además, si

$$a + b\sqrt{d} \equiv f + g\sqrt{d} \pmod{p} \Leftrightarrow (a-f) + (b-g)\sqrt{d} = p(s + t\sqrt{d}) \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} a - f = st \Leftrightarrow a \equiv f \pmod{p} \\ b - g = pt \Leftrightarrow b \equiv g \pmod{p} \end{cases}$$

COROLARIO

Si p primo impar con $\left(\frac{d}{p}\right) = -1$. Entonces, el anillo cociente $K = O_{\sqrt{d}}/(p)$ es un cuerpo finito con p^2 elementos.

Por lo anterior, el conjunto

$$K = \{a + b\sqrt{d} \in \mathbb{C} : \ 0 \le a, b < p\}$$

con el producto usual módulo p es un modelo concreto para este cuerpo.

EXISTENCIA DE ELEMENTOS PRIMITIVOS EN CUERPOS FINITOS

Como el grupo multiplicativo es $U(K) = K - \{0\}$, para $K = \frac{O_{\sqrt{d}}}{(p)}$ con p primo impar, $\left(\frac{d}{p}\right) = -1$ tenemos
$|U(K)| = p^2 - 1 = (p-1)(p+1)$
Por el teorema de Lagrange, el orden multiplicativo de cada elemento de K, debe ser un un divisor de $p^2 - 1$.

Si existe $\alpha \in K$ de orden multiplicativo r, entonces sus r potencias distintas $1, \alpha, \dots, \alpha^{r-1} \in K$, todas satisfacen la ecuación $x^r - 1 = 0$. Esos son exactamente los elementos que tienen de orden un divisor de r ya que la ecuación $x^r - 1 \in K[x]$ tiene como máximo r raíces en K. Entre ellos $\varphi(r)$ tienen exactamente orden r.

Como además, para todo $m \in \mathbb{N}$, $m = \sum_{r|m} \varphi(r)$, con $\varphi(r)$ la función de Euler, entonces la igualdad

$$p^2 - 1 = \sum_{r|p^2-1} \varphi(r) = \varphi(1) + \varphi(2) + \cdots + \varphi(p^2 - 1)$$

nos demuestra que tiene que haber en $U(K)$ elementos de orden cualquier divisor de $p^2 - 1$. En particular, existen $\varphi(p^2 - 1)$ elementos de orden máximo, $p^2 - 1$, y estos generan al grupo multiplicativo $U(K)$. O sea,

TEOREMA

Si p primo impar con $\left(\frac{d}{p}\right) = -1$, el grupo multiplicativo de $K = O_{\sqrt{d}}/(p)$ es cíclico de orden $p^2 - 1$.

EXISTENCIA DE LUCAS-CERTIFICADO PARA UN PRIMO

Si p primo impar con $\left(\frac{d}{p}\right) = -1$, entre los $p^2 - 1$ elementos de $U(K)$,
$a + b\sqrt{d} \in K, 1 \leq a < p, 0 \leq b < p$
hay elementos de orden cualquier divisor de $p^2 - 1 = (p-1)(p+1)$.

Ahora, sea una s.L., $\{U_i\}_{i\in\mathbb{N}}$, definida por $P, Q \in \mathbb{Z}$, con $d = P^2 - 4Q$ no cuadrado perfecto, y $\alpha = \frac{P+\sqrt{d}}{2}$.
Sea también p primo impar con $\left(\frac{d}{p}\right) = -1$.
Por el TPF para ent. cuadr., la s.L. $\{U_i\}_{i\in\mathbb{N}}$ certifica que p es primo si y sólo si $p+1$ es la menor potencia de α que sale congruente, módulo p, con un entero racional. Esto es cierto, si en el cuerpo cociente la clase de α, módulo p, tiene de orden multiplicativo $(p^2-1)/t$ con t un divisor primo con $p+1$ (i.e., t divisor impar de $p-1$).

Recíprocamente, si $a + b\sqrt{d} \in K$ tiene de orden $(p^2-1)/t$ con t un divisor impar de $p-1$, entonces la s.L. asociada a $P = 2a, Q = a^2 - b^2 d \pmod p$ certifica la primalidad de p. Así

TEOREMA

Existen al menos tantas s.L. que certifican la primalidad de p como elementos en K tienen orden $(p^2-1)/t$ con t un divisor impar de $p-1$.

PROBABILIDAD DE UN LUCAS-CERTIFICADO DE PRIMALIDAD

Como

$$\sum_{t|p-1,\text{ t impar}} \varphi((p^2-1)/t) = (p-1)\varphi(p+1)$$

la probabilidad de encontrar una s.L.-certificado es $\frac{(p-1)\varphi(p+1)}{p^2-1} = \frac{\varphi(p+1)}{p+1}$

Ahora, si $\alpha = a + b\sqrt{d} \in K$ tiene orden $(p^2-1)/t$ con t un divisor impar de $p-1$, como existe $a^{-1} \pmod{p}$, también el elemento

$$\beta = (2a)^{-1}\alpha = (2a)^{-1}(a + b\sqrt{d}) = \frac{1 + a^{-1}b\sqrt{d}}{2} = \frac{1 + \sqrt{a^{-2}b^2d}}{2}$$

tiene el mismo orden y su correspondiente s.L está asociada a $P = 1$, $Q \equiv (1 - a^{-2}b^2d)/4 \pmod{p}$.

Por tanto, se tiene

COROLARIO

La probabilidad de encontrar una s.L.-certificado es $\frac{(p-1)\varphi(p+1)}{p^2-1} = \frac{\varphi(p+1)}{p+1}$ y basta buscar entre las s.L., $\{U_i\}_{i\in\mathbb{N}}$, definidas por $P = 1, Q \in \mathbb{N}$, con $d = 1 - 4Q$ no cuadrado perfecto, para certificar la primalidad de p.

Enrique R. Aznar García
eaznar@ugr.es