Revista Colombiana de Matemáticas
Vol. XXI (1987), págs. 263-284

EL FAMOSO POLINOMIO GENERADOR DE PRIMOS DE EULER Y EL NUMERO DE CLASE DE LOS CUERPOS CUADRATICOS IMAGINARIOS(*)

por

Paulo RIBENBOIM (**)

Introducción. ¿Puede un polinomio no constante, de coeficientes enteros, tomar solamente valores primos?

¡No! a causa del siguiente

TEOREMA. *Si* $f(x) \in \mathbf{Z}[X]$ *tiene grado positivo, entonces existe una cantidad infinita de números naturales* n *para los cuales* f(n) *es un número compuesto.*

Demostración. El teorema es válido si f(n) es siempre compuesto para todo $n \geq 1$. Supongamos pues, que existe $n_0 \geq 1$ tal que $f(n_0) = p$ es un número primo. Como $\lim_{n\to\infty} |f(n)| = \infty$ existe n_1 tal que si $n \geq n_1$, entonces $|f(x)| \geq p$. Tomemos cualquier h que cumpla $n_0 + ph \geq n_1$. Entonces $f(n_0 + ph) = f(n_0) + (\text{múlti-}$

(*) Este es el texto de una conferencia dada en la Universidad de Roma, el 8 de mayo de 1986. Las notas originales desaparecieron cuando mis maletas fueron hurtadas en Toronto (¡!) Sin embargo, había dado una copia a mi amigo Paolo Maroscia, a quien no le hurtaron su equipaje en Roma(¡!) y quien amablemente me dejó consultarla. Es bueno tener amigos.

(**) Traducción de Víctor S. Albis.

plo de p) = (múltiplo de p), de modo que $f(n_0 + ph)$ es compuesto.

Por otro lado, cabe preguntarse si un polinomio no constante $f(x) \in \mathbb{Z}[X]$ debe siempre asumir un valor primo. Esta pregunta es interesante si f(X) es irreducible, primitivo (es decir, el máximo común divisor de sus coeficientes es igual a 1) y si más aún no hay ningún primo p que divida a todos los valores de f(n) (para enteros arbitrarios n).

Bouniakowsky y más tarde Schinzel & Sierpiński (1958) conjeturaron que cualquier polinomio $f(X) \in \mathbb{Z}[X]$ que satisfaga las anteriores condiciones asume un valor primo. Esto nunca ha sido demostrado para polinomios arbitrarios. Para los polinomios específicos f(X) = aX + b, con m.c.d. (máximo común divisor) (a,b) = 1, la conjetura es válida, pues no es otra cosa que el famoso teorema de Dirchlet: *toda progresión aritmética* $\{b+ka \mid k = 0,1,2,\ldots\}$, con m.c.d. (a,b) = 1, *contiene un número infinito de primos.*

En mi nuevo libro intitulado "The Book of Prime Number Records" (El libro de récords de los números primos, Springer-Verlag, 1987), he indicado algunas consecuencias asombrosas de la hipótesis de Bouniakowsky, encontradas por Schinzel & Sierpiński. Pero este no es el tema de este artículo.

A pesar del teorema y de lo que acabo de comentar, para muchos polinomios es muy fácil verificar que pueden tomar valores primos, y hasta es posible concebir que puedan tomar valores primos para muchos p enteros consecutivos. Por ejemplo, el famoso polinomio de Euler: $f(X) = X^2 + X + 41$ es tal que f(n) es un primo si n = 0,1,...,39 (cuarenta valores primos sucesivos):

41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197, 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 797, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523, 1601.

Sin embargo, $f(40) = 40^2+40+41 = 40\times41+41 = (41)^2$. Ob-

servemos que si $n > 0$, entonces $(-n)^2 + (-n) + 41 = (n-1)^2 + (n-1) + 41$, de modo que X^2+X+41 toma también valores primos para todos los enteros $n = -40, -39, \ldots, -2, -1$.

¿Qué otros polinomios se comportan de manera semejante?

Algunos de tales polinomios pueden obtenerse fácilmente a partir de $X^2 + X + C$ cambiando X por X-a, para algún $a \geq 1$. Por ejemplo, $(X-a)^2+(X-a)+41 = X^2-(2a-1)X + (a^2-a+41)$; haciendo $a = 1$, tenemos X^2-X-41, que toma valores primos para todo entero n entre -39 y 40; mientras que si hacemos $a = 40$, tenemos $X^2-79X + 1601$ que toma valores primos para todo entero n entre 0 y 79, pero éstos son los mismos valores que toma $X^2 + X + 41$, apareciendo cada uno dos veces. Resumiendo, es de interés concentrar nuestra atención en los polinomios de la forma $X^2 + X + C$ y sus valores en los enteros consecutivos $n = 0,1,2,\ldots$. Si el valor en 0 es un primo q entonces $C = q$. Como $(q-1)^2+(q-1)+q = q^2$, entonces en el mejor de los casos $X^2 +X + q$ toma valores primos para $0,1,2,\ldots,q-2$ (como en el caso $q = 41$). Por ejemplo si $f(X) = X^2 + X + q$ y $q = 2,3,5,11,17,41$, entonces $f(n)$ es primo para $n = 0,1,\ldots,q-2$. Empero, si $q = 7,13,19,23,29,31,37$ esto no es cierto como puede verificarse con facilidad.

¿Pueden encontrarse primos $q > 41$ para los cuales $X^2 + X + q$ tiene valores primos en $n = 0,1,\ldots,q-2$? ¿Hay una cantidad finita o una cantidad infinita de tales primos? En el caso de que ésta cantidad sea finita, ¿cuál es el máximo valor posible de q?

El mismo problema puede plantearse para polinomios de grado uno: $f(X) = aX + b$, con $a,b \geq 1$. Si $f(0)$ es un primo q, entonces $b = q$. Luego $f(q) = aq + q = (a+1)q$ es compuesto y en el mejor de los casos, $aX + q$ toma valores primos para $X = 0,1,\ldots,q-1$.

¿Se pueden encontrar estos polinomios? O, equivalentemente,

¿pueden encontrarse progresiones aritméticas de q números primos que tengan como primer elemento a q?

Para valores pequeños de q esto no es difícil.

Si q = 3, tomemos: 3,5,7, de modo que $f(X) = 2X + 3$.
Si q = 5, tomemos: 5,11,17,23,29, de modo que $f(X) = 6X + 5$.
Si q = 7, tomemos: 7,157,307,457,607,757,907, de modo que $f(X) = 150X + 7$.

Muy recientemente, Keller me ha comunicado que para q = 11,13 las más pequeñas de estas sucesiones están dadas por los polinomios $f(X) = d_{11}X + 11$ y $f(X) = d_{13}X + 13$, con

$$d_{11} = 1536160080 = 2\times3\times5\times7\times7315048$$
$$d_{13} = 9918821194590 = 2\times3\times5\times7\times11\times4293861989,$$

respectivamente; esta determinación requirió una considerable cantidad de cálculos, ejecutados por Keller and Löh.

No se sabe si para cada primo q exista una progresión aritmética de q primos que empiece con q. Inclusive el problema de hallar progresiones aritméticas arbitrariamente grandes conformadas sólo por números primos (sin restricciones sobre el término inicial o la diferencia), aún permanece sin respuesta. La mayor de tales progresiones aritméticas conocida contiene 19 primos y fué hallada por Pritchard (1985).

La determinación de todos los polinomios $f(X) = X^2+X+q$ que cumplen: f(n) es un primo para n = 0,1,...,q-2 está íntimamente relacionada con la teoría de los cuerpos cuadráticos imaginarios. Con el fin de entender esta relación indicaré en seguida los principales resultados que precisaremos.

A) Extensiones cuadráticas. Sea d un entero que no es un cuadrado, y designemos con $K = \mathbb{Q}(\sqrt{d})$ al cuerpo de todos los elementos de la forma $\alpha = a+b\sqrt{d}$, $a,b \in \mathbb{Q}$. No hay pérdida sustancial de la generalidad si suponemos que d no admite factores cuadráticos, y, por tanto, que $d \not\equiv 0$ (mód 4). $K/\mathbb{Q}$

es una *extensión cuadrática*, esto es, K es un espacio vectorial de dimensión dos sobre $\mathbb{Q}$. Recíprocamente, si K es un cuerpo que es extensión cuadrática de $\mathbb{Q}$, entonces necesariamente es de la forma $K = \mathbb{Q}(\sqrt{d})$, donde d es un entero sin factores cuadráticos.

Si $d > 0$, entonces K es un subcuerpo del cuerpo $\mathbb{R}$ de los números reales y se le llama entonces un *cuerpo cuadrático real*.

Si $d < 0$, entonces K no es un subcuerpo de $\mathbb{R}$ y se le llama un *cuerpo cuadrático imaginario*.

Si $\alpha = a + b\sqrt{d} \in K$, con $a,b \in \mathbb{Q}$, su *conjugado* es $\alpha' = a - b\sqrt{d}$. Claramente $\alpha = \alpha'$ precisamente cuando $\alpha \in \mathbb{Q}$.

La *norma* de α es $N(\alpha) = \alpha\alpha' = a^2 - db^2 \in \mathbb{Q}$. Es obvio que $N(\alpha) \neq 0$ sólo cuando $\alpha \neq 0$. Si $\alpha,\beta \in K$ entonces $N(\alpha\beta) = N(\alpha)N(\beta)$, en particular, si $\alpha \in \mathbb{Q}$ entonces $N(\alpha) = \alpha^2$.

La *traza* de α es $Tr(\alpha) = \alpha+\alpha' = 2a \in \mathbb{Q}$. Si $\alpha,\beta \in K$, entonces $Tr(\alpha+\beta) = Tr(\alpha) + Tr(\beta)$; en particular, si $\alpha \in \mathbb{Q}$, entonces $Tr(\alpha) = 2\alpha$.

Es claro también que α y α' son las raíces de la ecuación cuadrática $X^2 - Tr(\alpha)X + N(\alpha) = 0$.

B) Anillos de enteros. Sea $K = \mathbb{Q}(\sqrt{d})$ donde d es un entero sin factores cuadráticos. Decimos que $\alpha \in K$ es un *entero algebraico* cuando existen enteros $m,n \in \mathbb{Z}$ tales que $\alpha^2 + m\alpha + n = 0$.

Sea A el conjunto de todos los enteros algebraicos de K. Entonces A es un subanillo de K, el cual es a su vez el cuerpo de fracciones de A. Además, $A \cap \mathbb{Q} = \mathbb{Z}$. Si $\alpha \in A$ entonces su conjugado α' también lo está. Claramente, $\alpha \in A$ si, y sólo si, tanto $N(\alpha)$ como $Tr(\alpha)$ están en $\mathbb{Z}$.

El siguiente es un criterio para decidir si el elemento $\alpha = a+b\sqrt{d}$, $a,b \in \mathbb{Q}$, es un entero algebraico: $\alpha \in A$ si, y sólo si,

$$\begin{cases} 2a = u \in \mathbb{Z}, & 2b = v \in \mathbb{Z}, \\ u^2 - dv^2 \equiv 0 \pmod 4 \end{cases}$$

Usando este criterio, puede mostrarse que:

Si $d \equiv 2$ ó $3 \pmod 4$, entonces $A = \{a+b\sqrt{d};\ \ a,b \in \mathbb{Z}\}$

Si $d \equiv 1 \pmod 4$, entonces $A = \{\frac{a+b\sqrt{d}}{2};\ \ a,b \in \mathbb{Z},\ a \equiv b \pmod 2\}$

Si α_1 y α_2 son enteros algebraicos tales que todo elemento $\alpha \in A$ puede expresarse unívocamente en la forma $\alpha = m_1\alpha_1 + m_2\alpha_2$, con $m_1, m_2 \in \mathbb{Z}$, decimos que $\{\alpha_1, \alpha_2\}$ es una *base entera* de A. En otras palabras $A = \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2$.

Si $d \equiv 2$ ó $3 \pmod 4$, entonces $\{1, \sqrt{d}\}$ es una base entera de A.

Si $d \equiv 1 \pmod 4$, entonces $\{1, \frac{1+\sqrt{d}}{2}\}$ es una base entera de A.

C) Discriminante. Sea α_1, α_2 una base entera de A. Entonces

$$D = D_K = \det \begin{pmatrix} Tr(\alpha_1^2) & Tr(\alpha_1\alpha_2) \\ Tr(\alpha_1\alpha_2) & Tr(\alpha_2^2) \end{pmatrix}$$

es independiente de la escogencia de la base entera. D_K se llama el *discriminante* de K y es un entero distinto de 0.

Si $d \equiv 2$ ó $3 \pmod 4$ entonces

$$D = \det \begin{pmatrix} Tr(1) & Tr(\sqrt{d}) \\ Tr(\sqrt{d}) & Tr(d) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d\ .$$

Si $d \equiv \pmod 4$, entonces

$$D = \det \begin{pmatrix} Tr(1) & Tr(\frac{1+\sqrt{d}}{2}) \\ Tr(\frac{1+\sqrt{d}}{2}) & Tr((\frac{1+\sqrt{d}}{2})^2) \end{pmatrix} = \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix} = d.$$

Siempre se tiene $D \equiv 0$ ó $1 \pmod 4$. En términos del discriminante, podemos escribir

$$A = \{\frac{a+b\sqrt{d}}{2} \mid a,b \in \mathbb{Z},\ \ a^2 \equiv Db^2 \pmod 4\},$$

D) Descomposición de primos. Sea $K = \mathbb{Q}(\sqrt{d})$, donde d no tiene factores cuadráticos, y sea A su anillo de enteros. El ideal $P \neq 0$ de A es un *ideal primo* si el anillo residual (anillo cociente) A/P no tiene divisores de cero.

Si P es un ideal primo de A, existe entonces un único número primo p tal que $P \cap \mathbb{Z} = \mathbb{Z}p$, o lo que es equivalente, tal que $P \supseteq Ap$.

Si I y J son ideales no nulos de A, se dice que I *divide* a J cuando existe un ideal I_1 de A tal que $I \cdot I_1 = J$.

El ideal primo P que contiene al número primo p divide al ideal Ap.

Si I es un ideal no nulo de A entonces el anillo residual A/I es finito. La norma de I se define como $N(J) = \#(A/I)$.

Propiedades de la norma.

Si I y J son ideales no nulos, entonces $N(I \cdot J) = N(I)N(J)$.

Si I divide a J entonces N(I) divide a N(J).

Si $\alpha \in A$, $\alpha \neq 0$, entonces $N(A\alpha) = |N(\alpha)|$ (valor absoluto de la norma de α). En particular, si $a \in \mathbb{Z}$ entonces $N(Aa) = a^2$.

Si el ideal primo P divide a Ap, entonces N(P) es igual a p o a p^2.

Si I y J son ideales no nulos y $I \supseteq J$ entonces I divide a J.

Cada ideal $I \neq 0$ se expresa unívocamente como el producto de potencias de ideales primos

$$I = \prod_{i=1}^{n} P_i^{e_i}$$

Todo ideal $I \neq 0$ puede ser generado por dos elementos unos de los cuales se pude tomar en $\mathbb{Z}$: si $I \cap \mathbb{Z} = \mathbb{Z}n$, entonces $I = An + A\alpha$, para algún $\alpha \in A$. En este caso usamos la siguiente notación $I = (n,\alpha)$.

Consideremos ahora el caso especial de un número primo. Entonces Ap es de uno de los tipos siguientes:

$Ap = P^2$, donde P es un ideal primo: p se *ramifica en* K

$Ap = P$, donde P es un ideal primo: p es *inerte en* K

$Ap = P_1P_2$, donde P_1 y P_2 son dos ideales primos distintos: p se *descompone en* K.

Observemos también que si $Ap = I \cdot J$, donde I y J son ideales $\neq A$, no necesariamente distintos, entonces I y J deben de hecho ser primos.

Indicaremos ahora cúando un número primo p se ramifica, se descompone o es inerte y daremos también generadores para los ideales primos de A. Hay dos casos: $p \neq 2$, $p = 2$.

Si $\left(\frac{d}{p}\right)$ denota el *símbolo de Legendre*, tenemos:

$\left(\frac{d}{p}\right) = 0$ cuando p divide a d

$\left(\frac{d}{p}\right) = +1$ cuando d es un cuadrado módulo p

$\left(\frac{d}{p}\right) = -1$ cuando d no es un cuadrado módulo p.

Supongamos que $p \neq 2$.

1) Si p divide a d entonces $Ap = (p,\sqrt{d})^2$

2) Si p no divide a d y no existe $a \in \mathbb{Z}$ tal que $d \equiv a^2$ (mód p), entonces Ap es un ideal primo.

3) Si p no divide a d y existe $a \in \mathbb{Z}$ tal que $d \equiv a^2$ (mód p), entonces $Ap = (p,a+\sqrt{d}) \cdot (p,a-\sqrt{d})$.

Luego

1) p *se ramifica si, y sólo si,* $\left(\frac{d}{p}\right) = 0$

2) p *es inerte si, y sólo si,* $\left(\frac{d}{p}\right) = -1$

3) p *se descompone si, y sólo si,* $\left(\frac{d}{p}\right) = 1$.

Demostración. Esta se divide en varias partes:

a) *Si* $\left(\frac{d}{p}\right) = -1$ *entonces* Ap *es un ideal primo.* Supongamos

que no, de modo que $Ap = PP'$ ó P^2, donde $P \cap \mathbb{Z} = \mathbb{Z}p$. Sea $\alpha \in A$ tal que $P = (\alpha, p) \in A\alpha$; entonces $P \mid A\alpha$ y consecuentemente p divide a $N(P)$, el cual a su vez divide a $N(A\alpha) = |N(\alpha)|$. Si $p \mid \alpha$, entonces $\alpha/p \in A$ y $P = Ap(1, \frac{\alpha}{p}) = Ap$, lo cual es absurdo. Luego $p \nmid \alpha$. Entonces

$$\left\{\begin{array}{l} d \equiv 2 \text{ ó } 3 \pmod 4 \\ d \equiv 1 \pmod 4 \end{array}\right\} \Rightarrow \left\{\begin{array}{l} \alpha = a+b\sqrt{d}, \text{ con } a,b \in \mathbb{Z} \\ \alpha = \frac{a+b\sqrt{d}}{2}, \text{ con } a,b \in \mathbb{Z},\ a \equiv b \pmod 2 \end{array}\right\}$$

$$\Rightarrow \left\{\begin{array}{l} N(\alpha) = a^2 - db^2 \\ N(\alpha) = \frac{a^2-db^2}{4} \end{array}\right\} \Rightarrow p \text{ divide a } a^2 - db^2.$$

Luego $a^2 \equiv db^2 \pmod p$ y $p \nmid b$ (pues si nó, $p \mid a$ y por tanto $p \mid \alpha$, lo cual es absurdo).

Sea b' tal que $bb' \equiv 1 \pmod p$, de modo que $(ab')^2 \equiv d \pmod p$. De aquí resulta que o bien $p \mid d$, o bien $(\frac{d}{p}) = +1$, lo cual es contradictorio.

b) *Si* $(\frac{d}{p}) = 0$ *entonces* $Ap = (p, \sqrt{d})^2$. En efecto, sea $P = (p, \sqrt{d})$, de modo que $P^2 = (p^2, p\sqrt{d}, d) = Ap.\ (p,\ d, d/p)$ puesto que $d/p \in \mathbb{Z}$. Pero d no tiene factores cuadráticos y así $m.c.d.(p,\ d/p) = 1$; por consiguiente, $p^2 = Ap$ y esto implica que P es un ideal primo.

c) *Si* $(\frac{d}{p}) = -1$ *entonces* $Ap = (p, a+\sqrt{d})(p, a-\sqrt{d})$, *donde* $1 \leqslant a \leqslant p-1$ *y* $a^2 \equiv d \pmod p$.

En efecto $(p, a+\sqrt{d})(p, a-\sqrt{d}) = (p^2, pa+p\sqrt{d}, pa-p\sqrt{d}, a^2-d) = Ap(p, a+\sqrt{d}, a-\sqrt{d}, (a^2-d)/p) = Ap \cdot (p, a+\sqrt{d}, a-\sqrt{d},\ 2a, \frac{a^2-d}{p}) = Ap$, porque $m.c.d.\ (p, 2a) = 1$. Si uno de los ideales $(p, a+\sqrt{d})$, $(p, a-\sqrt{d})$ fuese igual a A, también lo sería el otro, lo cual es imposible.

Luego $(p, a+\sqrt{d})$ y $(p, a-\sqrt{d})$ son ideales primos. Además, son distintos, pues si $(p, a+\sqrt{d}) = (p, a-\sqrt{d})$, serían iguales a su suma $(p, a+\sqrt{d}) + (p, a-\sqrt{d}) = (p, a+\sqrt{d}, a-\sqrt{d}, 2a) = A$, lo cual es absurdo.

Finalmente, estos tres casos son excluyentes y exhaustivos. Por lo cual las aseveraciones recíprocas son también válidas.

Nota. Si $d \equiv 1 \pmod 4$ y $d \equiv a^2 \pmod p$, entonces $(p, a+\sqrt{d}) = (p, \ell(a-1)+\omega)$, donde $\omega = (1+\sqrt{d})/2$ y $2\ell \equiv 1 \pmod p$. Luego si $\left(\frac{d}{p}\right) \neq -1$ existe $b \in \mathbb{Z}$, $0 \leq b \leq p-1$, tal que p divide a $N(b+\omega)$ y, además, si $b = p-1$ entonces $d \equiv 1 \pmod 4$.

En efecto, $a+\sqrt{d} = a-1+2\omega$. Si $2\ell \equiv 1 \pmod p$, entonces $(p, a+\sqrt{d}) = (p, (a-1)+2\omega) = (p, \ell(a-1)+\omega)$.

Si $\left(\frac{d}{p}\right) \neq -1$, existe entonces un ideal primo P que divide a Ap, donde $P = (p, a\sqrt{d})$, $0 \leq a \leq p-1$. De modo que $P = (p, b+\omega)$ donde $0 \leq b \leq p-1$, $b \equiv \ell(a-1) \pmod p$.

Como $P \supseteq A(b+\omega)$, entonces p divide a $N(P)$, que a su vez divide a $N(b+\omega)$. Finalmente, si p divide a $N(p-1+\omega) = N((2p-1+\sqrt{d})/2) = [(2p-1)^2-d]/4$, entonces p divide a $(1-d)/4$, de donde $d \equiv 1 \pmod p$.

Supongamos que $p = 2$.

Si $d \equiv 2 \pmod 4$, entonces $A2 = (2, \sqrt{d})^2$.
Si $d \equiv 3 \pmod 4$, entonces $A2 = (2, 1+\sqrt{d})^2$.
Si $d \equiv 1 \pmod 8$, entonces $A2 = (1, \omega)(2, \omega')$.
Si $d \equiv 5 \pmod 8$, entonces A2 es un ideal primo.

Luego:

1) 2 *se ramifica si, y sólo si,* $d \equiv 2$ ó $3 \pmod 4$

2) 2 *es inerte si, y sólo si,* $d \equiv 5 \pmod 8$

3) 2 *se descompone si, y sólo si,* $d \equiv 1 \pmod 8$.

Demostración. También se divide en varias partes:

a) *Si* $d \equiv 5 \pmod 8$, *entonces* A2 *es un ideal primo.* Si nó, $A2 = pp'$ ó p^2, donde $P \cap \mathbb{Z} = \mathbb{Z}2$. Luego existe $\alpha \in A$ tal que $P = (2, \alpha) \supseteq A\alpha$, de modo que P divide a $A\alpha$ y 2 divide a $N(P)$, el cual a su vez divide a $N(\alpha)$.

Si $2 \mid \alpha$ entonces $P = A2$. $(1, \alpha/2) = A2$, lo cual es absurdo. Luego $2 \nmid \alpha = (a+b\sqrt{d})/2$, donde $a \equiv b \pmod 2$, de modo que $N(\alpha) = (a^2-db^2/4$. De $2 \mid N(\alpha)$ resulta que 8 divide a $a^2-db^2 \equiv a^2-5b^2 \equiv a^2+3b^2 \pmod 8$.

Si a y b son impares, entonces $a^2 \equiv b^2 \equiv 1 \pmod 8$, con lo cual $a^2+3b^2 \equiv 4 \pmod 8$, que es absurdo. Luego a y b son ambos pares: $a = 2a'$, $b = 2b'$, $\alpha = a'+b'\sqrt{d}$ y 2 divi-

de a $N(\alpha) = a'^2 - db'^2$.

Cuando d es impar, entonces a' y b' son ambos pares o ambos impares. Si a' y b' son pares, entonces 2 divide a α lo cual es absurdo.

Si a' y b' son ambos impares, entonces $\alpha = a' + b'\sqrt{d}$ = (múltiplo de 2) + 1 + $\sqrt{d}$ = (múltiplo de 2) + 2ω = (múltiplo de 2), lo que es también absurdo.

b) *Si* $d \equiv 1$ (mód 8) *entonces* $A2 = (2,\omega)(2,\omega')$. En efecto, $(2,\omega)(2,\omega') = (4,2\omega,2\omega',(1-d)/4) = A2(2,\omega,\omega',(1-d)/8) = A2$, pues $\omega + \omega' = 1$.

También $(2,\omega) \neq (2,\omega')$, porque si no estos ideales serían iguales a su suma $(2,\omega,\omega') = A$, ya que $\omega + \omega' = 1$.

c) *Si* $d \equiv 2$ *ó* 3 (mód 4) *entonces* $A2 = (2,\sqrt{d})^2$ *ó* $(2,1+\sqrt{d})^2$, *respectivamente*. Primero hagamos $d = 4e+2$, de modo que $(2,\sqrt{d})^2 = (4,2\sqrt{d},d) = A2\cdot(2,\sqrt{d},2e+1) = A2$; de esto resulta que $(2,\sqrt{d})$ es un ideal primo.

Ahora, hagamos $d = 4e+3$, de modo que $(2,1+\sqrt{d})^2 = (4,2+2\sqrt{d},1+d+2\sqrt{d}) = (4,2+2\sqrt{d},4(e+1)+2\sqrt{d}) = A2\cdot(2,1+\sqrt{d},2(e+1)+\sqrt{d}) = A2\cdot(2,2e+1,1+\sqrt{d},2(e+1)+\sqrt{d}) = A2$, de esto resulta que $(2,1+\sqrt{d})$ también es primo.

Finalmente, estos tres casos son excluyentes y exhaustivos, por lo que las afirmaciones recíprocas son también válidas.

E) Unidades. El elemento $\alpha \in A$ es una *unidad* si existe $\beta \in A$ tal que $\alpha\beta = 1$. El conjunto U de las unidades es un grupo para la multiplicación. Aquí presentamos una descripción del grupo de las unidades en los varios casos. Supongamos primero que $d < 0$.

Sea $d \neq -1, -3$. Entonces $U = \{\pm 1\}$.
Sea $d = -1$. Entonces $U = \{\pm 1, \pm i\}$, donde $i = \sqrt{-1}$.
Sea $d = -3$. Entonces $U = \{\pm 1, \pm\rho, \pm\rho^2\}$, donde $\rho^3 = 1$, $\rho \neq 1$, es decir, $\rho = (-1+\sqrt{-3})/2$.

Sea ahora $d > 0$. Entonces el grupo de las unidades es el producto $U = \{\pm 1\} \times C$, donde C es un grupo multiplicativo cíclico infinito. Luego $C = \{\varepsilon^n \mid n \in \mathbb{Z}\}$, donde ε es la unidad más pequeña mayor que 1. Esta unidad ε se llama la *unidad fundamental*.

F) El número de clase. La teoría de los cuerpos cuadráticos de números se originó en el estudio de las *formas cuadráticas binarias* $aX^2 + bXY + cY^2$ (donde $a,b,c \in \mathbb{Z}$ y $ac \neq 0$). El *discriminante de la forma* es, por definición, $D = b^2 - 4ac$. Observemos que $D \equiv 0$ ó $1 \pmod 4$, de modo que podemos escribir $d = D/A$ ó $d = D$, respectivamente.

Un entero m se dice que es *representable por la forma* si existen enteros x e y que cumplen $m = ax^2 + bxy + cy^2$.

Si una forma $a'X'^2 + b'X'Y' + c'Y'^2$ se obtiene de la anterior mediante un cambio lineal de variables.

$$X = hX' + kY',$$

$$Y = mX' + nY',$$

donde h,k,m y n son enteros y el determinante $hn - km = 1$, entonces las dos formas representan los mismos enteros. En este sentido es razonable considerar estas formas como *equivalentes*. Claro está, formas equivalentes tienen el mismo discriminante.

En sus "Disquisitiones Arithmeticae" Gauss clasificó a las formas binarias cuadráticas con un discriminante dado D. Definió así mismo una operación de composición entre clases de equivalencia de formas con un discriminante dado. Estas clases conforman un grupo para esta operación. Mostró además que, para cualquier discriminante dado D, sólo existe un número finito de clases de equivalencia de formas binarias cuadráticas.

Más tarde la teoría se reinterpretó asociando con cada forma $aX^2 + bXY + cY^2$ de discriminante D, el ideal I de $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{D})$ generado por a y $(-b+\sqrt{D})/2$. Si declaramos dos *ideales* I y I' como *equivalentes* cuando existe $\alpha \in \mathbb{Q}(\sqrt{d})$,

$\alpha \neq 0$, tal que $I = A\alpha \cdot I'$, vemos que formas binarias cuadráticas equivalentes se corresponden con ideales equivalentes, y que la composición de clases de formas se corresponde con la multiplicación de clases equivalentes de ideales. Luego $\mathbb{Q}(\sqrt{d})$ *tiene un número finito de clases de ideales*. Denotemos con $h = h(d)$ el número de clases de ideales, o *número de clase del cuerpo* $\mathbb{Q}(\sqrt{d})$.

Este número clasal $h(d)$ es igual a 1 precisamente cuando cada ideal de $\mathbb{Q}(\sqrt{d})$ es un ideal principal.

Gauss conjeturó que para cada $h \geq 1$ existe sólo una cantidad finita de cuerpos cuadráticos imaginarios $\mathbb{Q}(\sqrt{d})$ $(d < 0)$, que tienen número de clase igual a h. Dentro de poco diré algo más sobre esta conjetura.

Por ahora indicaré cómo calcular el número de clase del cuerpo cuadrático $\mathbb{Q}(\sqrt{D})$. Definamos el número real θ de la siguiente manera

$$\theta = \begin{cases} D/2 & \text{si} \quad D > 0, \\ 2\sqrt{-D}/\pi & \text{si} \quad D < 0. \end{cases}$$

Un ideal no nulo I de A se dice *normalizado* si $N(I) \leq [\theta]$ (la parte entera de θ). Diremos que I es *primitivo* si no existe ningún primo p tal que Ap divide a I.

Con N denotemos al conjunto de los ideales primitivos normalizados de A. Si $I \in N$ y p es un primo ramificado, entonces $p^2 | N(I)$; si p es inerte, entonces $p | N(I)$. Luego

$$N(I) = \prod_{r \text{ se ramifica}} r \times \prod_{p \text{ se descompone}} p^{e(p)}$$

Puede demostrarse que cada clase de ideales contiene un ideal primitivo normalizado. Como para cada $m \geq 1$ existe a lo sumo un número finito de ideales I de A tales que $N(I) = m$, esto muestra una vez más, que el número de las clases de ideales es finito.

Observemos que si N consiste tan sólo del ideal unidad

$A = A \cdot 1$, entonces $h = 1$. Luego, si todo primo p que cumple $p \leq [\theta]$ es inerte, se tiene que $h = 1$. En efecto, si $I \in N$ entonces $N(I) = 1$, luego es el ideal unidad, lo que hace que $h = 1$.

Denotemos con $N(N)$ al conjunto de enteros $N(I)$, donde $I \in N$.

Con el fin de decidir si los ideales I' y $I \in N$ son equivalentes, será necesario decidir qué enteros $m \in N(N)$ son de la forma $m = N(A\alpha)$.

Sea $m \geq 1$ y hagamos

$$\alpha = \begin{cases} u + v\sqrt{d} & \text{cuando } d \equiv 2 \text{ ó } 3 \pmod 4, \text{ con } u,v \in \mathbb{Z}, \\ \dfrac{u+v\sqrt{d}}{2} & \text{cuando } d \equiv 1 \pmod 4, \text{ con } u,v \in \mathbb{Z},\ u \equiv v \pmod 2 \end{cases}$$

Entonces $A\alpha$ *es un ideal primitivo con* $N(A\alpha) = m$ *si, y sólo si,*

$$\begin{cases} m = u^2 - dv^2, \text{ m.c.d. } (u,v) = 1 & \text{si } d \equiv 2 \text{ ó } 3 \pmod 4 \\ m = \dfrac{u^2-dv^2}{4}, \text{ m.c.d. } \left(\dfrac{u-v}{2}, v\right) = 1 & \text{si } d \equiv 1 \pmod 4. \end{cases}$$

(ésta es la llamada *representación primitiva de* m).

Demostración. Sean $d \equiv 2$ ó $3 \pmod 4$, $m = N(A\alpha) = |u^2 - dv^2|$, de modo que m.c.d. $(u,v) = 1$, pues $A\alpha$ es primitivo.

Sean $d \equiv 1 \pmod 4$, $m = N(A\alpha) = |u^2 - dv^2|/4$. Como $p \mid (u,v)/2$ y $p \mid v$ implica que $\alpha = (u,v)/2 + v(1+\sqrt{d})/2$ es divisible por p, lo cual es contrario a las hipótesis, resulta también que m.c.d. $((u-v)/2, v) = 1$.

Recíprocamente, sea $d \equiv 2$ ó $3 \pmod 4$, de modo que $N(A\alpha) = m$; si p divide a $A\alpha$ y dado que $\{1, \sqrt{d}\}$ es una base entera, entonces $p \mid u$, $p \mid v$, lo cual es absurdo.

Sea $d \equiv 1 \pmod 4$, de modo que $N(A\alpha) = m$; si p divide a $A\alpha$ y dado que $\alpha = (u-v)/2 + v(1+\sqrt{d})/2$ y $\{1, (1+\sqrt{d})/2\}$, es una base entera, resulta que p divide a $(u-v)/2$ y a v, ¡lo que es absurdo!

Cálculo del número de clase. Sea $d > 0$, de modo que $\theta = \sqrt{D}/2$. $[\theta] = 1$.

Como $1 \leq \sqrt{D}/2 < 2$ entonces $A \leq D < 16$, con $D = 0$ ó 1 (mód 4), luego $D \in \{4,5,8,9,12,13\}$ y, por consiguiente, $d \in \{5,2,3,13\}$.

Ahora $N(N) = \{1\}$, luego N consiste únicamente del ideal unidad, y en consecuencia, $h = 1$.

$[\theta] = 2$.

Como $2 \leq \sqrt{D}/2 < 3$, entonces $16 \leq D < 36$, con $D \equiv 0$ ó 1 (mód 4); luego $D \in \{16,17,20,21,24,25,28,29,32,33\}$ y en consecuencia $d \in \{17,21,6,7,29,33\}$.

Ahora $N(N) = \{1,2\}$.

Tomemos por ejemplo $d = 17$. Como $17 \equiv 1$ (mód 8), tenemos que $A2 = PP'$, $N(P') = 2$, $2 = |3^2 - 17\times 1^2|/4$, m.c.d. $(\frac{3-17}{2}, 17) = 1$; luego $P = A\alpha$, $\alpha = (3+\sqrt{17})/2$, $P' = A\alpha'$, $\alpha' = (3-\sqrt{17})/2$. Luego el número de clase es 1.

Tomemos ahora $d = 21$. Como $21 \equiv 5$ (mód 8), entonces $A2$ es un ideal primo, 2 es inerte y por tanto $h = 1$.

Si $d = 6$, entonces 2 divide a $24 = D$, de modo que 2 se ramifica: $A2 = P^2$, y $2 = |2^2 - 6\times 1^2|$, m.c.d. $(2,1) = 1$. Luego $P = A\alpha$, con $\alpha = 2+\sqrt{6}$. Por consiguiente $h = 1$.

$[\theta] = 3$.

Como $3 \leq \frac{1}{2}\sqrt{D} < 4$ entonces $36 \leq D < 64$, con $D \equiv 0$ ó 1 (mód 4). Luego $D \in \{36,37,40,44,45,48,49,52,53,56,57,60,61\}$ y, por consiguiente, $d \in \{37,10,41,11,53,14,57,15,61\}$.

Ahora $N(N) = \{1,2,3\}$.

Tomemos por ejemplo $d = 10$. Como 2 divide a $40 = D$ entonces 2 ramifica $A2 = R^2$. Como $(\frac{10}{3}) = (\frac{1}{3}) = 1$, entonces 3 se descompone: $A3 = P\cdot P'$. Los ideales R, P, P' son primitivos.

2 no tiene representación primitiva: si $2 = |u^2 - 10v^2|$ entonces $u^2 = 10v^2 \pm 2 \equiv \pm 2$ (mód 10), lo que no es posible.

3 no tiene representación primitiva: si $3 = u^2 - 10v^2$ entonces $u^2 = 10v^2 \pm 3 \equiv \pm 3$ (mód 10), lo que tampoco es posible.

Luego R, P, P' no son ideales principales. Los ideales

RP, RP' son primitivos. También, $-2\times3 = -6 = 2^2-10\times1^2$, m.c.d. $(2,1)=1$, $2\times3 = N(RP) = N(RP')$; luego RP y RP' son ideales principales. En conclusión h = 2.

Sea ahora $d < 0$, de modo que $\theta = 2\sqrt{-D}/\pi$.

$[\theta] = 1$.

Como $1 \leqslant 2\sqrt{-D}/\pi < 2$, entonces $\pi^2/4 \leqslant |D| < \pi^2$, y $[\theta] = 0$ ó 3 (mód 4) implican que $|D| \in \{3,4,7,8\}$. Por consiguiente, $d \in \{-3,-1,-7,-2\}$. Ahora $N(N) = 1$, luego N consiste sólo del ideal unidad, de modo que h = 1.

$[\theta] = 2$.

Como $2 \leqslant 2\sqrt{-D}/\pi < 3$, entonces $\pi^2 \leqslant |D| < g\pi^2/4$, y $[\theta] \equiv 0$ ó 3 (mód 4) implican que $|D| \in \{11,12,15,16,19,20\}$, y, en consecuencia, $d \in \{-11,-15,-19,-5\}$.

Tomemos, por ejemplo, $d = -11$. Como $-11 \equiv 5$ (mód 8), 2 es inerte y así h = 1.

Tomemos $d = -5$. Como 2 divide a $D = -20$ se ramifica: $A2 = P^2$.

2 no tiene representación primitiva: si $2 = |u^2+5v^2|$ entonces $u^2 = -5v^2+2 \equiv 2$ (mód 5) lo que es imposible. También $-5 \equiv 3$ (mód 4). Luego P no es principal y así h = 2.

Tomemos $d = -19$. Como $-19 \equiv 5$ (mód 8), 2 es inerte y consecuentemente h = 1.

$[\theta] = 3$.

Como $3 \leqslant 2\sqrt{-D}/\pi < 4$ entonces $p\pi^2/4 \leqslant |D| < 4\pi^2$, y $|D| \equiv 0$ ó 3 (mód 4), lo cual implica que $|D| \in \{23,24,27,28,31,32,35,36,39\}$ y, por tanto, $d \in \{-23,-6,-31,-35,-39\}$.

Tomemos $d = -31$. Como $-31 \equiv 1$ (mód 8) entonces $A2 = PP'$. Como $\left(\frac{-31}{3}\right) = \left(\frac{-1}{3}\right)\left(\frac{1}{3}\right) = -1$, A3 es un ideal primo.

2 no tiene representación primitiva: si $2 = |u^2+3/v^2|/4$, con m.c.d. $((u-v)/2,v) = 1$, entonces $8 = u^2+3/v^2$, lo que es imposible. Como $-31 \equiv 1$ (mód 4), P y P' no son ideales principales. Si P y P' son equivalentes, entonces $P = P'\cdot A\alpha$, de modo que $P^2 = PP'A\alpha = A(2\alpha)$ y así $4 = N(P^2) = 4N(A\alpha)$ y, en consecuencia, $N(A\alpha) = 1$. Resulta, pues, que $A\alpha = A\alpha$ y $P = P'$, lo cual es absurdo. En conclusión, h = 3.

Estos ejemplos bastan para ilustrar cómo calcular el número de clase al menos para valores pequeños del discriminante.

Determinación de todos los cuerpos cuadráticos con número de clase 1.

Sea $d > 0$. Se ha conjeturado que existe una cantidad infinita de enteros $d > 0$ para los cuales $\mathbb{Q}(\sqrt{d})$ tiene número de clase 1. Este asundo es difícil de resolver, pero se espera que la conjetura sea cierta.

Por ejemplo, sabemos que existen 142 cuerpos $\mathbb{Q}(\sqrt{d})$, con $2 \leqslant d < 500$, que tienen a 1 como número de clase.

Sea $d < 0$. Hemos visto que si N contiene sólo al ideal unidad, entonces $h = 1$. Pero recíprocamente:

Si $d < 0$ *y* $h = 1$, *entonces* $N = \{A\}$.

Demostración. Si $|D| \leqslant 7$, la afirmación es correcta. Sea, pues, $|D| > 7$, y supongamos que existe $I \in N$, $I \neq A$, de modo que existe un ideal primo P que divide a I. Entonces $N(P) = p$ ó p^2, donde p es un número primo. Si $N(P) = p^2$ entonces p es inerte a $Ap = P$ divide a I y así I no sería primitivo, lo que es contradictorio. Si $N(P) = p$ y dado que P divide a I, entonces $p \leqslant N(I) \leqslant [\theta] \leqslant 2\sqrt{|D|}/\pi$. Si p tiene una representación primitiva: si $d \equiv 2$ ó 3 (mód 4), entonces $d = D/4$, de modo que $p = u^2 - dv^2$; luego $v \neq 0$ y, por consiguiente, $2\sqrt{|D|}/\pi \geqslant p \geqslant |d|/4 \geqslant |D|/4$, con lo cual $7 \geqslant D$, nuevamente un absurdo. Por tanto, P no es aun ideal principal y $h \neq 1$, lo que es contrario a la hipótesis!

Gauss desarrolló una *teoría de géneros* y demostró:

Si $d < 0$ y si t es el número de factores primos distintos de D, entonces 2^{t-1} divide al número de clase de $\mathbb{Q}(\sqrt{d})$.

Luego si $h = 1$, entonces $D = -4, -8$ ó $-p$, donde p es un primo, $p \equiv 3$ (mód 4); luego $d = -1, -2$ ó $-p$.

De esta discusión se sigue que:

Si $D = -3, -4, -7, -8$, entonces $h = 1$.
Si $D \neq -3, -4, -7, -8$ y $D = -p$, $p \equiv 3$ (mód 4), entonces $h = 1$ si, y sólo si, $N = \{A\}$, y esto es equivalente a las siguientes condiciones: 2 es inerte en $\mathbb{Q}(\sqrt{-p})$, y si p es cualquier primo impar y $q \leqslant [\theta]$, entonces $\left(\frac{-p}{q}\right) = -1$, es decir, q es inerte en $\mathbb{Q}(\sqrt{-p})$.

Este criterio se usa en la determinación de todos los

$D < 0$, $|D| \leq 200$, tales que $h = 1$.

$[\theta] = 1$. Esto da los discriminantes $D = -3, -4, -7, -8$.

$[\theta] = 2$. Ahora $-20 \leq D \leq -11$, con $D = -p$, $p \equiv 3$ (mód 4), de modo que $D = -11$ ó -19.

Como $-11 \equiv 5$ (mód 8), 2 es inerte y, por tanto, para $D = -11$ es $h = 1$.

Análogamente, como $-19 \equiv 5$ (mód 8), 2 es inerte y, por tanto, para $D = -19$ es $h = 1$.

$[\theta] = 3$. Ahora $-39 \leq D \leq -23$, con $D = -p$, $p \equiv 3$ (mód 4), de modo que $D = -23$ ó -31. Pero $-23 \not\equiv 5$ (mód 8), $-31 \not\equiv 5$ (mód 8) y así los números de clase de $\mathbb{Q}(\sqrt{-23})$ y $\mathbb{Q}(\sqrt{-31})$ no son iguales a 1.

$[\theta] = 4$. Ahora $-59 \leq D \leq -40$, $D = -p$, $p \equiv 3$ (mód 4), de modo que $D = -43, -47, -59$. Como $-43 \equiv 5$ (mód 8) y $\left(\frac{-43}{3}\right) = -1$, entonces $\mathbb{Q}(\sqrt{-43})$ tiene número de clase 1. Como $-47 \not\equiv 5$ (mód 8) y $\left(\frac{-59}{3}\right) = 1$, entonces 3 no existe. Luego los números de clase de $\mathbb{Q}(\sqrt{-47})$ y $\mathbb{Q}(\sqrt{-59})$ no son iguales a 1.

El mismo tipo de cálculos conduce a:

$[\theta] = 5$: $D = -67$, con número de clase 1.
$[\theta] = 6$: ningún discriminante.
$[\theta] = 7$: ningún discriminante.
$[\theta] = 8$: $D = -163$, con número de clase 1.

Este proceso puede continuarse más allá de 200, pero no conduce a ningún discriminante de número de clase igual a 1. Por supuesto, esto no nos permite decidir si existen otros tales discriminantes, ni decidir tampoco si sólo hay un número finito de cuerpos cuadráticos imaginarios de número de clase igual a 1.

En un trabajo clásico, Heilbronn y Linfoot mostraron en 1934, usando métodos analíticos, que además de los ejemplos anteriores existía a lo sumo otro valor de $d < 0$ para el cual el número de clase de $\mathbb{Q}(\sqrt{d})$ era 1. Lehmer mostró que si un tal discriminante existía, debía cumplir con $|d| > 5\times10^9$. En 1952, Heegner demostró que ningún otro d podía

existir, pero su prueba contenía algunos pasos confusos y posiblemente una brecha en su razonamiento. Baker llegó a la misma conclusión en 1966, con su método que involucra cotas inferiores efectivas en formas lineales de tres logaritmos; esto también lo mencionará en su artículo de 1971. Por caso la misma época, e ignorante de los resultados de Heegner, pero con ideas muy semejantes, que tienen que ver con las funciones elípticas modulares, Stark demostró que no es posible que exista otro valor adicional de d. En esta forma se determinaron todos los cuerpos cuadráticos imaginarios de número de clase 1. En 1968 se produjo algo así como un anticlímax, cuando Deuring logró enderezar la demostración de Heegner.

Este es el momento para decir que la conjetura de Gauss también se resolvió afirmativamente. Gracias a los trabajos de Hecke, Deuring, Mordell y Heilbronn, se pudo establecer que si $d < 0$ y $|d|$ tiende a infinito, también lo hace el número de clase de $\mathbb{Q}(\sqrt{d})$. Luego para cada $h \geq 1$ sólo existe una cantidad finita de cuerpos $\mathbb{Q}(\sqrt{d})$, con $d < 0$, que tienen número de clase h. La determinación de todos los cuerpos cuadráticos imaginarios de número de clase igual a 2 fue lograda por Baker, Stark y Weinberger.

Una estimativa explícita de la cantidad de cuerpos cuadráticos imaginarios con número de clase dado se ha obtenido gracias a los esfuerzos de Siegel, Goldfeld, Gross y Zagier. Para este asunto, sugiero leer el artículo de Goldfeld (1985).

G) El teorema principal.

TEOREMA. *Sea* q *un número primo y hagamos* $f_q(X) = X^2 + X + q$. *Entonces las siguientes condiciones son equivalentes:*

1) $q = 2,3,5,11,17,41$.

2) $f_q(n)$ *es un primo para* $n = 0,1,2,\ldots,q-2$.

3) $\mathbb{Q}(\sqrt{1-4q})$ *tiene número de clase igual a 1.*

Demostración. La implicación 1) => 2) es una simple ve-

rificación. La equivalencia de las condiciones 2) y 3) fue demostrada por la primera vez por Rabinovitch en 1912. En 1936, Lehmer demostró otra vez que 2) $\Rightarrow$ 3), mientras que 3) $\Rightarrow$ 2) fue demostrada de nuevo por Szekeres (1974) y por Ayoub & Chowla (1981), que dieron una demostración más sencilla. La demostración de 3) $\Rightarrow$ 1) sigue de la determinación completa de todos los cuerpos cuadráticos imaginarios de número de clase igual a 1. Como esta implicación requiere profundos resultados, daré también la demostración de 3) $\Rightarrow$ 2).

2) $\Rightarrow$ 3). Sea $d = 1-4q < 0$, de modo que $d \equiv 1 \pmod 4$. Si $q = 2$ ó 3, entonces $d = -7$ ó -11 y $\mathbb{Q}(\sqrt{d})$ tiene a 1 como número de clase, como ya hemos visto. Supongamos ahora que $q \geq 5$. Basta mostrar que todo primo $p < 2\sqrt{|d|}/\pi$ es inerte en $\mathbb{Q}(\sqrt{d})$.

En primer lugar, tomemos $p = 2$, como $q = 2t-1$, entonces $d = 1-4q = 1-4(2t-1) \equiv 5 \pmod 8$, lo que muestra que 2 es inerte en $\mathbb{Q}(\sqrt{d})$.

Tomemos ahora $p \neq 2$, $p \leq 2\sqrt{|d|}/2 < \sqrt{|d|}$ y supongamos que p no es inerte. Entonces $\left(\frac{d}{p}\right) \neq -1$ y como ya lo hemos observado, existe $b \in \mathbb{Z}$, $0 \leq b \leq p-1$, tal que p divide a $N(b+\omega)$, donde $\omega = (1+\sqrt{d})/2$; es decir, p divide a $(b+\omega)(b+\omega') = b^2+b(\omega+\omega') + \omega\omega' = b^2 + b + \frac{1-d}{4} = b^2 + b + q = f_q(b)$. Debemos también notar que $b \neq p-1$, pues como ya lo hemos visto, p divide a $1-d = 4q$, de donde $p = q < \sqrt{|d|} = \sqrt{|1-4q|}$, de modo que $q^2 < 4q-1$ y, por consiguiente, $q = 2$ ó 3, contrariamente a las hipótesis.

Por hipótesis, $f_q(b)$ es entonces un número primo; luego $\sqrt{4q-1} > p = f_q(b) \geq f_q(0) = q$ y de nuevo $q = 2$ ó 3, contrario otra vez con las hipótesis.

Esto muestra que todo primo p menor que $2\sqrt{|d|}/\pi$ es inerte y así que $h = 1$.

3) $\Rightarrow$ 1). Si $\mathbb{Q}(\sqrt{1-4q})$ tiene número de clase 1, entonces $d = 1-4q = -7,-11,-19,-43,-67,-163$; luego $q = 2,3,5,11,17,41$!

Como ya lo he dicho, la demostración queda así completa; pero aún así es interesante indicar la demostración de 3) $\Rightarrow$ 2).

Supongamos que $d = 1-4q$ y que $\mathbb{Q}(\sqrt{-d})$ tiene a 1 por número de clase. Entonces, o bien $d = -1,-2,-3,-7$, o bien $d < -7$, de modo que $d = -p$, donde $p \equiv 3$ (mód 4) y $q > 2$.

Como hemos observado antes, 2 es inerte en $\mathbb{Q}(\sqrt{-p})$, de modo que $p \equiv 3$ (mód 8). En seguida mostramos que si ℓ es cualquier número primo impar, $\ell < q$, entonces $(\frac{\ell}{p}) = -1$. En efecto, si $(\frac{\ell}{p}) = 1$, ℓ descompone en $\mathbb{Q}(\sqrt{-p})$. Pero $h = 1$, indica que existe un entero algebraico $\alpha = (a+b\sqrt{-p})/2$ tal que $A\ell = A\alpha \cdot A\alpha'$. Entonces $\ell^2 = N(A\ell) = N(A\alpha)N(A\alpha') = N(A\alpha)^2 = N(\alpha)^2$, de modo que $\ell = N(\alpha) = (a^2+b^2p)/4$. Por consiguiente, $p+1 = 4q > 4\ell = a^2+b^2p$; de aquí $1 > a^2 + (b^2-1)p$ y necesariamente $a^2 = 0$, $b^2 = 1$; es decir, $4\ell = p$, lo cual es absurdo.

Supongamos ahora que existe m, $0 \leqslant m \leqslant q-2$, tal que $f_q(m) = m^2+m+q$ no sea un número primo. Entonces existe un primo ℓ tal que $\ell^2 \leqslant m^2+m+q$ y $m^2+m+q = a\ell$, con $a \geqslant 1$. Como m^2+m+q es impar, entonces $\ell \neq 2$. Por otra parte,

$$4\ell^2 \leqslant (2m+1)^2 + p < (\frac{p-1}{p})^2 + p = (\frac{p+1}{2})^2 ,$$

luego $\ell < (p+1)/4 = q$. Como se demostró, $(\frac{\ell}{p}) = -1$. Sin embargo, $4a\ell = (2m+1)^2 + 4q-1 = (2m+1)^2 + p$; luego $-p$ es un cuadrado módulo ℓ; entonces, por la ley de la reciprocidad cuadrática de Gauss, obtenemos

$$1 = (\frac{-p}{\ell}) = (\frac{-1}{\ell})(\frac{p}{\ell}) = (-1)^{(\ell-1)/2} (\frac{\ell}{p}) (-1)^{(\ell-1)/2\times(p-1)/2}$$

$$= (\frac{\ell}{p}) ,$$

lo cual es absurdo (!!).

BIBLIOGRAFIA

[1] Ayoub, R. and Chowla, S., *On Euler's polynomial*. J. Nb. Th., **13**, 1981, 443-445.

[2] Borevich, Z.I. and Shafarevich, I.R., *Number Theory*. Academic Press, New York, 1966.

[3] Cohn, H., *Advanced Number Theory*. Dover Publ., New York, 1962.
[4] Goldfeld, D., *Gauss' class number problem for imaginary quadratic fields*. Bull. Amer. Math. Soc., **13**, 1985 23-37.
[5] Lehmer, D.H., *On the function* x^2+x+A. Sphinx 6, 1936, 212-214.
[6] Pritchard, P.A., *Long arithmetic progressions of primes: some old, some new*. Math. of Comp., 45, 1985, 263-267.
[7] Rabinovitch, G., *Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörper*. Intern. Congress of Math., Cambridge, 1912, vol. 1, 418-421.
[8] Ribenboim, P., *Algebraic Numbers*. Wiley-Interscience, New York, 1972.
[9] Ribenboim, P., *The Book of Prime Number Records*. Springer Verlag, New York, 1987.
[10] Schinzel, A. and Sierpiński, W., *Sur certaines hypothèses concernant les nombres premiers. Remarques*. Acta Arithm., 4, 1958, 185-208 and 5, 1959, p. 259.
[11] Schinzel, A., *Remarks on the paer "Sur certaines hypothèses concernant les nombres premiers"*. Acta Arithm., 7, 1961, 1-8.
[12] Szekeres, G., *On the number of divisors of* x^2+x+A. J. Nb. Th., **6**, 1984, 434-442.

*

Queen University
Department of Mathematics and Statistics
Kingston, Ontario K7L 3N6
CANADA.

(Recibido en Febrero de 1987)