UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

POSGRADO EN CIENCIAS MATEMÁTICAS

FACULTAD DE CIENCIAS

Divisores primos de $x^3 - 2$

QUE PARA OBTENER EL GRADO ACADÉMICO DE

MAESTRO(A) EN CIENCIAS

P R E S E N T A

Lic. **Sergio Guzmán Sánchez**

DIRECTOR(A) DE LA TESINA: Dr. Florian Luca

MÉXICO, D.F. Diciembre, 2009

Contenido

Introducción **2**

1 Analizando el campo $\mathbb{Q}[\alpha]$ **3**

2 Algunas cotas y desigualdades **9**

3 Formas lineales en logaritmos **12**

4 Algoritmo LLL **15**

5 Encontrando las soluciones **18**

Introducción

A continuación explicaremos cómo encontrar que $x = 3$ es la única solución entera positiva de la ecuación

$$x^3 - 2 = p_1^{n_1} p_2^{n_2} p_3^{n_3} p_4^{n_4} p_5^{n_5} \qquad n_i \geq 0, \quad i = 1, 2, \ldots, 5. \tag{1}$$

donde $p_1 = 5, p_2 = 11, p_3 = 17, p_4 = 23, p_5 = 29$.

Este problema se puede ver como buscar el entero impar más grande x tal que $P(x^3 - 2) < 50$, donde $P(n)$ es el factor primo más grande que divide al entero n. Los primos p_i mencionados anteriormente, son los primos impares menores a 50 que dividen a $x^3 - 2$.

En [3], resuelven algo similar usando métodos elementales como ecuaciones de Pell y congruencias. Estos métodos hacen complicado extender la cantidad de primos involucrados en el problema.

Otro problema similar fue resuelto por Florian Luca en [6], en el cual usa ecuaciones de Pell y el Teorema de los divisores primitivos (Este teorema se puede ver en [8]).

En este trabajo, haremos uso de otras herramientas para resolver el problema. Estas herramientas son las formas lineales en logaritmos y el algoritmo LLL, que con ayuda de una computadora hacen posible incrementar la cantidad de primos.

Capítulo 1

Analizando el campo $\mathbb{Q}[\alpha]$

Sea $f(x) = x^3 - 2$, $\alpha = \sqrt[3]{2}$ la raíz real de $f(x)$ y $\mathbb{K} = \mathbb{Q}[\alpha]$. Sea $\mathcal{O}_{\mathbb{K}}$ el anillo de enteros algebraicos de $\mathbb{K}$. La demostración del siguiente lema se puede ver en [5].

Lema 1. *Supongamos que el polinomio mínimo de θ es Eisenstein respecto al primo p, entonces el índice de θ no es divisible por p.*

Veamos que $1, \alpha, \alpha^2$ es una base entera de $\mathbb{K}$. Se puede verificar que

$$d_{\mathbb{K}/\mathbb{Q}}(\alpha) = -3^3 2^2,$$

entonces

$$-3^3 2^2 = m^2 d_{\mathbb{K}}.$$

donde m es el índice de α y $d_{\mathbb{K}}$ el discriminante del campo.

Como el polinomio mínimo de α es Eisenstein respecto a 2, por el Lema (1) sabemos que $2 \nmid m$, por lo tanto $12 | d_{\mathbb{K}}$.

Ahora veremos que $3 \nmid m$, para ello observemos que $(x+2)^3 - 2$ es Eisenstein respecto a 3 y una raíz de este polinomio es $\alpha - 2$, por lo tanto

$$d_{\mathbb{K}/\mathbb{Q}}(\alpha - 2) = d_{\mathbb{K}/\mathbb{Q}}(\alpha) = -3^3 2^2,$$

de aquí se sigue que

$$-3^3 2^2 = s^2 d_{\mathbb{K}},$$

donde s es el índice de $\alpha - 2$. Aplicando otra vez el Lema (1), obtenemos que $3^3 | d_{\mathbb{K}}$, por lo tanto $m = 1$ y $d_{\mathbb{K}} = -3^3 2^2$, esto nos dice que $1, \alpha, \alpha^2$ es una base entera de $\mathbb{K}$.

De lo anterior, obtenemos que el discriminante de $\mathbb{K}$ es

$$d_{\mathbb{K}} = -3^3 \cdot 2^2,$$

que coincide tambien con el discriminante de $f(x)$,

$$\Delta(f) = \prod_{1 \leq i < j \leq 3} (\alpha^i - \alpha^j)^2 = -3^3 \cdot 2^2.$$

Teorema 1 (Teorema de las unidades de Dirichlet). *Sea $\mathbb{K}$ un campo de números algebraicos de grado n. Sea r el número de campos reales conjugados de $\mathbb{K}$ y $2s$ el número de campos conjugados complejos de $\mathbb{K}$. Entonces $\mathcal{O}_{\mathbb{K}}$ contiene $r+s-1$ unidades $\epsilon_1, ..., \epsilon_{r+s-1}$ tal que cada unidad de $\mathcal{O}_{\mathbb{K}}$ puede ser expresada de manera única de la forma $\rho\epsilon_1^{n_1} \cdots \epsilon_{r+s-1}^{n_{r+s-1}}$, donde ρ es una raíz de la unidad en $\mathcal{O}_{\mathbb{K}}$ y $n_1, ..., n_{r+s-1}$ son enteros. Al número $r+s-1$ le llamaremos el rango del grupo de las unidades de $\mathcal{O}_{\mathbb{K}}$.*

Para nosotros $\mathbb{K}$ es un campo real de grado $d = 3$ donde $r = 1$ y $s = 1$ (en la notación del Teorema anterior). Entonces el grupo de unidades de $\mathcal{O}_{\mathbb{K}}$ tiene rango 1, lo cual nos dice que $\mathcal{O}_{\mathbb{K}}$ tiene una unidad fundamental de norma mayor a 1, a la cual la denotaremos β_1. Como $\mathcal{O}_{\mathbb{K}}$ es completamente real, las únicas raíces de la unidad en $\mathcal{O}_{\mathbb{K}}$ son ± 1. Por lo tanto, cualquier unidad en $\mathcal{O}_{\mathbb{K}}$ se expresa como $\pm\beta_1^n$, donde n es entero.

Para encontrar la unidad fundamental de $\mathcal{O}_{\mathbb{K}}$ necesitaremos el siguiente lema que se puede ver en [1].

Lema 2. *Para toda $x \in \mathbb{R}$ y toda $\theta \in \mathbb{R}$*

$$\sin^2\theta(x - 2\cos\theta)^2 < x^2 + 4$$

Teorema 2. *Sean $\mathbb{K} = \mathbb{Q}[\sqrt[3]{2}]$ y $\beta > 1$ la unidad fundamental de $\mathcal{O}_{\mathbb{K}}$. Entonces*

$$\beta^3 > \frac{|d_{\mathbb{K}}|}{4} - 7$$

donde $d_{\mathbb{K}}$ es el discriminante del campo.

Proof. Sean $\beta, \rho e^{i\theta}, \rho e^{-i\theta}$ los conjugados de β, donde $\rho \in \mathbb{R}^+$. Como β es unidad, tenemos que $N(\beta) = \pm 1$, donde $N(\beta)$ es la norma de β, entonces

$$\beta\rho e^{i\theta}\rho e^{-i\theta} = \pm 1,$$

esto es

$$\beta\rho^2 = \pm 1.$$

Como $\beta > 0$ y $\rho^2 > 0$, se debe tener $\beta\rho^2 = 1$, entonces

$$\beta = \rho^{-2}.$$

Ahora calculemos $d_{\mathbb{K}/\mathbb{Q}}$

$$\begin{aligned} d_{\mathbb{K}/\mathbb{Q}}(\beta) &= \prod_{1\leq r\leq s<3} (\beta^r - \beta^s)^2 \\ &= (\rho^{-2} - \rho e^{i\theta})^2(\rho^{-2} - \rho e^{-i\theta})^2(\rho e^{i\theta} - \rho e^{-i\theta})^2 \\ &= -4\sin^2\theta(\rho^3 + \rho^{-3} - 2\cos\theta)^2. \end{aligned} \tag{1.1}$$

Aplicando el Lema (2) tenemos

$$|d_{\mathbb{K}/\mathbb{Q}}(\beta)| = 4\sin^2\theta(\rho^3+\rho^{-3}-2\cos\theta)^2 < 4((\rho^3+\rho^{-3})^2-4) = 4(\beta^3+\beta^{-3}+6).$$

Siempre que $|d_{\mathbb{K}}| < |d_{\mathbb{K}/\mathbb{Q}}(\beta)|$, tenemos

$$\beta^3 > \frac{|d_{\mathbb{K}}|}{4} - 6 - \beta^{-3} > \frac{|d_{\mathbb{K}}|}{4} - 7.$$

□

Ahora veremos que β_1 (la unidad fundamental de $\mathcal{O}_{\mathbb{K}}$) es $\alpha^2 + \alpha + 1$. Primero observemos que

$$(\alpha - 1)(\alpha^2 + \alpha + 1) = \alpha^3 - 1 = 1,$$

por lo tanto $\alpha^2 + \alpha + 1$ es unidad de $\mathcal{O}_{\mathbb{K}}$.

Por el Teorema (2), sabemos que

$$\beta_1^3 > \frac{108}{4} - 7 = 20,$$

entonces

$$\beta_1^2 > \sqrt[3]{20^2} > 7.$$

Como $\dfrac{1}{7} < \alpha - 1 < 1$, se sigue que

$$1 < (\alpha - 1)^{-1} = \alpha^2 + \alpha + 1 < 7 < \beta_1^2.$$

Siempre que $\alpha^2+\alpha+1$ es una potencia de β_1, dicha potencia debe ser 1, por lo tanto $\beta_1=\alpha^2+\alpha+1$.

Teorema 3. *Sea $\mathbb{K}=\mathbb{Q}[\theta]$ un campo de números algebraicos de grado n tal que*

$$\mathcal{O}_{\mathbb{K}}=\mathbb{Z}+\mathbb{Z}\theta+\cdots+\mathbb{Z}\theta^n$$

Sean p un primo racional, $f(x)$ el polinomio mínimo de θ. Sea $^-$ la aplicación natural : $\mathbb{Z}[x]\to\mathbb{Z}_p[x]$. Supongamos que

$$\overline{f}(x)=g_1(x)^{e_1}\cdots g_r(x)^{e_r},$$

donde $g_1(x),\ldots,g_r(x)$ son diferentes polinomios mónicos e irreducibles en $\mathbb{Z}_p[x]$ y $e_1,\ldots,e_r$ son enteros positivos. Para $i=1,2,\ldots,r$ sea $f_i(x)$ un polinomio mónico en $\mathbb{Z}[x]$ tal que $\overline{f}_i=g_i$. Sea

$$P_i=\langle p,f_i(\theta)\rangle, i=1,2,\ldots,r.$$

Entonces $P_1,\ldots,P_r$ son ideales primos distintos en $\mathcal{O}_{\mathbb{K}}$ tales que

$$\langle p\rangle=P_1^{e_1}\cdots P_r^{e_r},$$

y

$$N(P_i)=p^{degf_i},\quad i=1,2,\ldots,r.$$

donde $degf_i$ es el grado del polinomio f_i.

Como $\{1,\alpha,\alpha^2\}$ es una base entera de $\mathbb{K}$, vimos anteriormente que el discriminante del campo es $d_{\mathbb{K}}=-108$. Ahora veremos que el número de clases de $\mathcal{O}_{\mathbb{K}}$ es 1 y por lo tanto $\mathcal{O}_{\mathbb{K}}$ es un dominio de ideales principales. Para ello, calculamos la cota de Minkowski

$$M_{\mathbb{K}}=\left(\frac{2}{\pi}\right)^s\sqrt{|d_{\mathbb{K}}|}=\frac{2}{\pi}\sqrt{108}<7.$$

Entonces, los primos racionales $p<M_{\mathbb{K}}$ son $p=2,3$ y 5. Aplicando el Teorema (3), vemos que
$\langle 2\rangle=\langle\alpha,2\rangle^3$,
$\langle 3\rangle=\langle\alpha+1,3\rangle^3$,
$\langle 5\rangle=\langle\alpha+1,5\rangle\cdot\langle\alpha^2-2\alpha-1,5\rangle$.

Como

$$\alpha^3 = 2,$$

entonces $\alpha|2$ en $\mathcal{O}_{\mathbb{K}}$, por lo tanto

$$\langle 2\rangle = \langle \alpha, 2\rangle^3 = \langle \alpha\rangle^3.$$

Como

$$(\alpha+1)^3 = (\alpha^3 + 3\alpha^2 + 3\alpha + 1) = (3\alpha^2 + 3\alpha + 3) = 3(\alpha^2 + \alpha + 1),$$

entonces

$$(\alpha+1)^3(\alpha - 1) = 3$$

por lo tanto $\alpha + 1|3$ en $\mathcal{O}_{\mathbb{K}}$, entonces se tiene que

$$\langle 3\rangle = \langle \alpha + 1, 3\rangle^3 = \langle \alpha + 1\rangle^3.$$

Ahora observemos que

$$(\alpha^2+1)(1 + 2\alpha - \alpha^2) = (\alpha^2+1)(\alpha^4 - \alpha^2 + 1) = \alpha^6 + 1 = 5, \qquad (1.2)$$

entonces $1 + 2\alpha - \alpha^2|5$ en $\mathcal{O}_{\mathbb{K}}$ lo que nos da

$$\langle \alpha^2 - 2\alpha - 1, 5\rangle = \langle \alpha^2 - 2\alpha - 1\rangle = \langle 1 + 2\alpha - \alpha^2\rangle$$

y

$$\langle \alpha + 2, 5\rangle = \langle 5\rangle\langle 1 + 2\alpha - \alpha^2\rangle^{-1} = \langle 5(1 + 2\alpha - \alpha^2)^{-1}\rangle = \langle 1 + \alpha^2\rangle$$

donde la última igualdad se ve de la ecuación (1.2).

Como todos los factores primos de $2, 3$ y 5 son principales, tenemos que el número de clase es 1.

Para continuar, necesitamos la factorización de los primos p_i en $\mathcal{O}_{\mathbb{K}}$ tales que $f(x) \pmod{p_i}$ admite solución. Para ello, primero encontraremos la factorización de $\langle p_i\rangle$ aplicando el Teorema (3), así obtenemos

$\langle 5\rangle = \langle \alpha + 2, 5\rangle \cdot \langle \alpha^2 + 3\alpha + 4, 5\rangle,$
$\langle 11\rangle = \langle \alpha + 4, 11\rangle \cdot \langle \alpha^2 + 7\alpha + 5, 11\rangle,$
$\langle 17\rangle = \langle \alpha + 9, 17\rangle \cdot \langle \alpha^2 + 9\alpha + 13, 17\rangle,$
$\langle 23\rangle = \langle \alpha + 7, 23\rangle \cdot \langle \alpha^2 + 16\alpha + 3, 23\rangle,$
$\langle 29\rangle = \langle \alpha + 3, 29\rangle \cdot \langle \alpha^2 + 26\alpha + 9, 29\rangle.$

Como $\mathcal{O}_{\mathbb{K}}$ es dominio de ideales principales, cada uno de estos ideales es principal. Podemos hacer artificios como los mostrados anteriormente para encontrar los generadores. También se puede verificar con SAGE estos generadores. Así tenemos que

$\langle 5\rangle = \langle \gamma_1\rangle \cdot \langle \delta_1\rangle$ donde $\gamma_1 = -\alpha^2 - 1$, $\delta_1 = \alpha^2 - 2\alpha - 1$,
$\langle 11\rangle = \langle \gamma_2\rangle \cdot \langle \delta_2\rangle$ donde $\gamma_2 = \alpha^2 + \alpha - 1$, $\delta_2 = 2\alpha^2 + 3\alpha - 1$,
$\langle 17\rangle = \langle \gamma_3\rangle \cdot \langle \delta_3\rangle$ donde $\gamma_3 = 2\alpha - 1$, $\delta_3 = 4\alpha^2 - 2\alpha + 1$,
$\langle 23\rangle = \langle \gamma_4\rangle \cdot \langle \delta_4\rangle$ donde $\gamma_4 = -2\alpha^2 - \alpha - 1$, $\delta_4 = \alpha^2 - 7\alpha + 3$,
$\langle 29\rangle = \langle \gamma_5\rangle \cdot \langle \delta_5\rangle$ donde $\gamma_5 = \alpha + 3$, $\delta_5 = \alpha^2 - 3\alpha + 9$.

De aquí, podemos verificar que la factorización de los primos p_i en $\mathcal{O}_{\mathbb{K}}$ es

$$5 = \gamma_1 \cdot \delta_1, \quad 11 = \gamma_2 \cdot \delta_2, \quad 17 = \gamma_3 \cdot \delta_3, \quad 23 = \gamma_4 \cdot \delta_4, \quad 29 = \gamma_5 \cdot \delta_5.$$

Sea $y = x - \alpha$ y $z = x^2 + \alpha x + \alpha^2$. Sustituyendo en la ecuación (1) tenemos

$$y \cdot z = x^3 - 2 = \gamma_1^{n_1} \cdot \delta_1^{n_1} \cdot \gamma_2^{n_2} \cdot \delta_2^{n_2} \cdots \gamma_5^{n_5} \cdot \delta_5^{n_5}.$$

Por lo tanto

$$y = \beta\gamma_1^{k_1}\delta_1^{r_1} \cdots \gamma_5^{k_5}\delta_5^{r_5} \quad y \quad z = \beta^{-1}\gamma_1^{n_1-k_1}\delta_1^{n_1-r_1} \cdots \gamma_5^{n_5-k_5}\delta_5^{n_5-r_5},$$

donde β es una unidad.

Veremos que k_i y r_i son iguales a n_i ó 0. Supongamos que no, entonces existe algún γ_i ó δ_i (le llamemos ϱ) tal que divide a y y z. Como $z = (x-\alpha^{(1)})(x-\alpha^{(2)})$, entonces ϱ divide a $x-\alpha$ y $x-\alpha^{(i)}$ para algún $i \in \{1,2\}$, por lo tanto, ϱ divide a $\Delta(f) = -3^3 2^2$. Como ϱ tiene norma una potencia de p_i para algún $i \in \{1,\ldots,5\}$, pero esto no puede suceder, por lo tanto $k_i = n_i$ y $r_i = 0$ ó $k_i = 0$ y $r_i = n_i$.

Como $N(\gamma_i) = p_i$ y $N(\delta_i) = p_i^2$ se tiene que:

$$y = \beta \cdot \gamma_1^{n_1} \cdot \gamma_2^{n_2} \cdot \cdots \cdot \gamma_5^{n_5} \qquad z = \beta^{-1}\delta_1^{n_1} \cdots \delta_5^{n_5}$$

Como β es una unidad, se tiene que

$$y = \epsilon\beta_1^{m_1} \cdot \gamma_1^{n_1} \cdot \gamma_2^{n_2} \cdots \gamma_5^{n_5} \tag{1.3}$$

$$z = \epsilon\beta_1^{-m_1} \cdot \delta_1^{n_1} \cdot \delta_2^{n_2} \cdots \delta_5^{n_5} \tag{1.4}$$

donde m_1 es un entero y $\epsilon \in \{\ 1, -1\}$.

Capítulo 2

Algunas cotas y desigualdades

Con la computadora buscamos las soluciones de la ecuación (1) cuando $\max\{n_i\} \leq 118$ y obtenemos la solución $x = 3$. A continuación supondremos que $\max\{n_i\} > 118$.

Hagamos algunas estimaciones sobre y. Supongamos $x > 1$, entonces

$$x < x^3 - 2 = p_1^{n_1} p_2^{n_2} p_3^{n_3} p_4^{n_4} p_5^{n_5} \leq p_5^{5\max\{n_i\}}, \tag{2.1}$$

por lo tanto

$$|y| = |x - \alpha| \leq x + |\alpha| < p_5^{5\max\{n_i\}} + \sqrt[3]{2} < (1.001) \cdot p_5^{5\max\{n_i\}}. \tag{2.2}$$

Como

$$x^3 > x^3 - 2 = p_1^{n_1} p_2^{n_2} p_3^{n_3} p_4^{n_4} p_5^{n_5} \geq p_1^{\max\{n_i\}},$$

se tiene que

$$x \geq p_1^{\frac{\max\{n_i\}}{3}}, \tag{2.3}$$

por lo tanto

$$|y| = |x - \alpha| \geq x - |\alpha| > p_1^{\frac{\max\{n_i\}}{3}} - \sqrt[3]{2} > (0.99) \cdot p_1^{\frac{\max\{n_i\}}{3}}. \tag{2.4}$$

Por la fórmula de Taylor, se puede verificar que

$$z = \sum_{k=1}^{3} \frac{f^{(k)}(\alpha)}{k!}(x - \alpha)^{k-1}$$

y

$$y^2 = \frac{f^{(3)}(\alpha)}{3!}(x-\alpha)^2,$$

entonces

$$|z - y^2| = \left| f'(\alpha) + \frac{f''(\alpha)}{2!} \cdot y \right| = |y| \cdot \left| \frac{f'(\alpha)}{y} + \frac{f''(\alpha)}{2!} \right|.$$

Como

$$\left| \frac{f'(\alpha)}{y} \right| < \frac{3 \cdot |\alpha|^2}{0.9 \cdot 5^{10}} < 0.01 \quad \text{y} \quad \left| \frac{f''(\alpha)}{2} \right| = 3|\alpha| < 3.78,$$

tenemos que

$$|z - y^2| < 3.8|y|.$$

Por lo tanto

$$|1 - \frac{z}{y^2}| < \frac{3.8}{y} < \frac{3.8}{0.9 \cdot 5^{\frac{\max\{n_i\}}{3}}} < \frac{3.8}{y} < \frac{4.23}{5^{\frac{\max\{n_i\}}{3}}} \tag{2.5}$$

Observemos que

$$\frac{4.23}{5^{\frac{\max\{n_i\}}{3}}} < \frac{1}{5^9}$$

entonces

$$\left| \frac{z}{y^2} \right| < 1 + \frac{1}{5^9}$$

por lo tanto

$$\left| 1 + \frac{z}{y^2} \right| < 2.1 \tag{2.6}$$

De las desigualdades (2.5) y (2.6) se sigue que

$$\left| 1 - \frac{z^2}{y^4} \right| < \frac{9}{5^{\frac{\max\{n_i\}}{3}}} \tag{2.7}$$

Ahora queremos una cota para m_1. Haciendo los cálculos necesarios tenemos que

$|\gamma_1| < 2.5875$, $|\gamma_2| < 1.8474$, $|\gamma_3| < 1.5199$,
$|\gamma_4| < 5.4348$, $|\gamma_5| < 4.2599$, $|\delta_1| < 1.9325$,
$|\delta_2| < 5.9546$, $|\delta_3| < 4.8298$, $|\delta_4| < 4.2321$,
$|\delta_5| < 6.8077$.

Si $m_1 \geq 0$, de la ecuación (1.3) y las desigualdad (2.2), tenemos que

$$|\beta_1^{m_1}| = \frac{|x-\alpha|}{\prod_{i=1}^{5}|\gamma_i|^{n_i}} < \frac{1.0001 \cdot p_5^{5\max\{n_i\}}}{|\gamma_3|^{\max\{n_i\}}},$$

así obtenemos que

$$m_1 < \frac{1}{\log(1+\alpha+\alpha^2)}[\log(1.0001)+5\cdot\log(29)\cdot\max\{n_i\}-\log(1.5199)\cdot\max\{n_i\}].$$

De donde concluimos

$$m_1 < 12.2 \cdot \max\{n_i\}.$$

Si $m_1 < 0$, de la ecuación (1.4) y las desigualdad (2.2), tenemos que

$$|\beta_1^{-m_1}| = \frac{|x^2+\alpha x+\alpha^2|}{\prod_{i=1}^{5}|\delta_i|^{n_i}} < \frac{1.0001 \cdot p_5^{10\max\{n_i\}}}{|\delta_1|^{\max\{n_i\}}},$$

así obtenemos que

$$-m_1 < \frac{1}{\log(1+\alpha+\alpha^2)}[\log(1.0001)+10\cdot\log(29)\cdot\max\{n_i\}-\log(1.9325)\cdot\max\{n_i\}].$$

Para este caso, tenemos

$$-m_1 < 24.6 \cdot \max\{n_i\}.$$

En conclusión, siempre se tiene

$$|m_1| < 24.6 \cdot \max\{n_i\}.$$

Capítulo 3

Formas lineales en logaritmos

Sean $\eta_0 = 1 + \alpha + \alpha^2$, $\eta_1 = \dfrac{\delta_1}{\gamma_1^2}$, $\eta_2 = \dfrac{\delta_2}{\gamma_2^2}$, $\eta_3 = \dfrac{\delta_3}{\gamma_3^2}$, $\eta_4 = \dfrac{\delta_4}{\gamma_4^2}$, $\eta_5 = \dfrac{\delta_5}{\gamma_5^2}$, $b_0 = -6m_1$, $b_i = 2n_i$ y $\lambda = 1 - \eta_0^{b_0} \cdot \eta_1^{b_1} \cdots \eta_5^{b_5}$.

Sustituyendo lo anterior y las ecuaciones (1.3) y (1.4) en (2.7) obtenemos

$$|1 - \eta_0^{b_0} \cdot \eta_1^{b_1} \cdots \eta_5^{b_5}| = |\lambda| < \frac{9}{5^{\frac{\max\{n_i\}}{3}}},$$

por lo tanto

$$\log|\lambda| < \log 9 - \frac{\max\{n_i\}}{3} \log 5. \tag{3.1}$$

Ahora queremos hallar una cota inferior de $\log|\lambda|$, para ello recurriremos a un resultado de Matveev [7]. Recordemos que si η es un número algebraico de grado d con polinomio mínimo

$$g(x) = a_0 \prod_{i=1}^{d} (x - \eta^{(i)})$$

la altura logarítmica de η se define como

$$h(\eta) = \frac{1}{d} \left(\log|a_0| + \sum_{i=1}^{d} \log \max\{|\eta^{(i)}|, 1\} \right)$$

Teorema 4. *Sea $\mathbb{K}$ un campo de números algebraicos de grado d, $\eta_1, \ldots, \eta_k$ números en $\mathbb{K}$ diferente de cero y $b_1, \ldots, b_k$ enteros, definamos*

$$B = \max\{|b_1|, \ldots, |b_k|\}$$

y

$$\lambda = 1 - \prod_{i=1}^{k} \eta_i^{b_i}.$$

Si $A_1, \ldots, A_k$ *son números reales tales que*

$$A_j \geq \max\{dh(\eta_j), |\log \eta_j|, 0.16\},\ j = 1, \ldots, k.$$

Entonces, si $\lambda \neq 0$*, tenemos que*

$$\log|\lambda| > -3 \cdot 30^{k+4}(k+1)^{5.5} d^2 (1 + \log d)(1 + \log(kB)) \prod_{i=1}^{k} A_i.$$

Si además $\mathbb{K}$ *es real, entonces*

$$\log|\lambda| > -1.4 \cdot 30^{k+3} k^{4.5} d^2 (1 + \log d)(1 + \log(B)) \prod_{i=1}^{k} A_i.$$

Para aplicar este resultado, sea

$$B = \max\{|b_i|\} < 6 \cdot (24.6 \cdot \max\{n_i\}) < 147.6 \max\{n_i\}.$$

Para $\eta_0 = 1 + \alpha + \alpha^2$, tenemos:
Polinomio mínimo $x^3 - 2$.
$Dh(\eta_0) = \log|\eta_0^{(3)}| = 1.3477$ por lo tanto $A_0 > 1.3477$.

Para $\eta_1 = \dfrac{\delta_1}{\gamma_1^2}$, tenemos:
Polinomio mínimo $x^3 - \frac{23}{25}x^2 + 3x + 1$.
$Dh(\eta_1) = 4.46139$ y tenemos $A_1 > 4.46139$.

Para $\eta_2 = \dfrac{\delta_2}{\gamma_2^2}$, tenemos:
Polinomio mínimo $x^3 - \frac{39}{121}x^2 - \frac{21}{11}x - 1$.
$Dh(\eta_2) = 5.3524$
$\log(\eta_2) = 0.55$
y tenemos $A_2 > 5.3524$.

Para $\eta_3 = \dfrac{\delta_3}{\gamma_3^2}$, tenemos:

Polinomio mínimo $x^3 - \frac{435}{289}x^2 + 3x - 1$.
$Dh(\eta_3) = 6.60846$
$\log(\eta_3) = 0.942035$
y tenemos $A_3 > 6.60846$.

Para $\eta_4 = \dfrac{\delta_4}{\gamma_4^2}$, tenemos:
Polinomio mínimo $x^3 - \frac{2721}{529}x^2 + \frac{177}{23}x + 1$.
$Dh(\eta_4) = 8.21392$
$\log(\eta_4) = 0.942035$
y tenemos $A_4 > 8.21392$.

Para $\eta_5 = \dfrac{\delta_5}{\gamma_5^2}$, tenemos:
Polinomio mínimo $x^3 - \frac{1065}{841}x^2 + 3x - 1$.
$Dh(\eta_5) = 7.71505$
$\log(\eta_5) = 0.9804$
y tenemos $A_5 > 7.71505$.

Aplicando el Teorema (4), tenemos que

$$\log|\lambda| > -1.4{\cdot}30^9{\cdot}6^{4.5}{\cdot}3^2{\cdot}(1+\log 3){\cdot}(1+\log(147.6\max\{n_i\})){\cdot}A_0\cdots A_5 \quad (3.2)$$

De (3.1) y (3.2) obtenemos la siguiente desigualdad

$$\frac{\max\{n_i\}}{3}{\cdot}\log 5 - \log 9 < 12.6{\cdot}30^9{\cdot}6^{4.5}{\cdot}(1+\log 3){\cdot}(1+\log(147.6\max\{n_i\})){\cdot}A_0\cdots A_5.$$

Resolviendo la desigualdad para $\max n_i$, tenemos

$$\max\{n_i\} < 2.5823 \cdot 10^{24}$$

por lo tanto,

$$B < 147.6 \cdot (2.5823 \cdot 10^{24}) = 3.8115 \cdot 10^{26}.$$

Capítulo 4

Algoritmo LLL

A continuación describiremos el algoritmo LLL (H. W. Lenstra, A. Lenstra y L. Lovasz), el cual nos da una cota inferior para

$$m = \min\{|\sum_{i=1}^{n} x_i \ln \alpha_i| : |x_i| \leq X, (x_1, \ldots, x_n) \neq 0\},$$

donde $\log \alpha_1, \ldots, \log \alpha_n$ son logaritmos de números algebraicos, reales e independientes sobre $\mathbb{Q}$.

Paso 1. Sea $C > (nX)^n$. Formamos la matriz de $n \times n$ dada por

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ \lfloor C \log \alpha_1 \rfloor & \lfloor C \log \alpha_1 \rfloor & \lfloor C \log \alpha_1 \rfloor & \cdots & \lfloor C \log \alpha_1 \rfloor & \lfloor C \log \alpha_1 \rfloor \end{pmatrix}$$

Paso 2. Para el retículo Γ generado por las columnas de la matriz de arriba, calculamos una base reducida (más adelante comentaremos a que nos referimos con una base reducida). Sea esta base $b_1, \ldots, b_n$.

Paso 3. Calculamos $b_1^*, \ldots, b_n^*$, la base Gram-Schmidt de $b_1, \ldots, b_n$. Es decir,

$$b_i^* = b_i - \sum_{1 \leq j < i} \mu_{i,j} b_j^* \quad \textit{donde} \quad \mu_{i,j} = \frac{b_i \cdot b_j^*}{b_j^* \cdot b_j^*} \;\; 1 \leq j < i.$$

Paso 4. Calculamos

$$c_1 = \max\left\{\frac{||b_1||}{||b_i^*||}\right\}_{1\leq i\leq n},$$

y

$$d = \frac{||b_1||}{c_1}$$

Paso 5. Si $d^2 > nX^2$ y $\sqrt{d^2 - nX^2} > \dfrac{1+nX}{2}$, entonces

$$m > \frac{\sqrt{d^2 - nX^2} - \frac{1+nX}{2}}{C}$$

En el algorítmo descrito, la base reducida se refiere a unas condiciones técnica que debe satisfacer $\{b_1, b_2, \ldots, b_n\}$, estas son

- $|\mu_{i,j}| \leq \frac{1}{2}$ para todo $i = 1, 2, \ldots, n$ y $j < i$;
- Para $i \geq 2$ se tiene

$$||b_i^* + \mu_{i,i-1}b_{i-1}^*||^2 \geq \frac{3}{4}||b_{i-1}||^2.$$

Hasta ahora tenemos

$$|1 - \eta_0^{b_0} \cdot \eta_1^{b_1} \cdots \eta_5^{b_5}| < \frac{9}{5^{\frac{\max\{n_i\}}{3}}},$$

$$\max\{b_i\} < 3.8115 \cdot 10^{26}.$$

Sea $\theta = b_0 \log \eta_0 + b_1 \log \eta_1 + \cdots + b_5 \log \eta_5$.

Aplicamos el algoritmo LLL para hallar una cota inferior de $|\theta|$. Para ello sea $X = 3.8115 \cdot 10^{26}$ y $C > (6X)^6$, tomamos $C = 10^{165}$.

De esta forma, tenemos la matriz descrita en el paso 1. Para obtener la base reducida usamos el comando LatticeReduce de la biblioteca de Mathematica. Aplicando el resto del algoritmo obtenemos que una cota inferior para $|\theta|$ es $8.4784 \cdot 10^{-139}$. De esta forma obtenemos la siguiente desigualdad

$$8.4784 \cdot 10^{-139} < \frac{9}{5^{\frac{\max\{n_i\}}{3}}}.$$

Resolviendo para $\max\{n_i\}$ obtenemos

$$\max\{n_i\} < 597.$$

Como la cota que obtenemos para $\max\{n_i\}$ es un poco alta, volvemos a aplicar el algoritmo LLL tomando $X = 147.6 * 597 = 88117.2$, por lo tanto tenemos $C = 10^{35}$. Al aplicar dos veces más el algoritmo se obtiene $\max\{n_i\} < 118$. Lo cual es una contradicción, por lo tanto, la única solución es $x = 3$. En el siguiente capitulo mostraremos como se verificaron todas las soluciones cuando $\max\{n_i\} < 118$.

Capítulo 5

Encontrando las soluciones

Queremos encontrar todas las soluciones de la ecuación (1) cuando $\max\{n_i\} \leq 118$. Escribamos $p_1^{n_1} \cdots p_5^{n_5} = dz^3$ donde d es un entro libre de cubos. Entonces

$$x^3 - dz^3 = 2,$$
$$(x - \sqrt[3]{d}z)(x^2 + \sqrt[3]{d}zx + \sqrt[3]{d^2}z^2) = 2.$$

Entonces tenemos

$$\left|\frac{x}{z} - \sqrt[3]{d}\right| = \left|\frac{2}{x^2 + \sqrt[3]{d}zx + \sqrt[3]{d^2}z^2}\right|. \tag{5.1}$$

Como x y z son positivos, se tiene que $x > \sqrt[3]{d}z$, entonces $x^2 > \sqrt[3]{d^2}z^2$. Por lo tanto $x^2 + \sqrt[3]{d}zx + \sqrt[3]{d^2}z^2 > 3\sqrt[3]{d^2}z^2$. De la ecuación (5.1) tenemos

$$\left|\frac{x}{z} - \sqrt[3]{d}\right| < \frac{2}{3\sqrt[3]{d^2}z^2},$$

Como $d > 2$, tenemos

$$\left|\frac{x}{z} - \sqrt[3]{d}\right| < \frac{1}{2z^2}.$$

Teorema 5. *Sea ϕ un número irracional. Si $\frac{p}{q}$ es un número racional tal que $\left|\frac{p}{q} - \phi\right| < \frac{1}{2q^2}$, entonces $\frac{p}{q}$ es una convergente de la fracción continua de ϕ.*

Aplicando el teorema anterior, tenemos que $\frac{x}{z}$ es una convergente de la fracción continua de $\sqrt[3]{d}$.

Sean $\frac{P_n}{Q_n}$ convergentes de $\sqrt[3]{d}$, de lo anterior, vemos que basta buscar la solución x en las convergentes de $\sqrt[3]{d}$. Sea $\frac{x}{z} = \frac{P_n}{Q_n}$ tal que x es una solución, como x y z son primos relativos, tenemos que $x = P_n$ y $z = Q_n$.

Como $z^3 < (5 \cdot 11 \cdot 17 \cdot 23 \cdot 29)^{118}$, se tiene que $z < 623645^{40}$. Por lo tanto $Q_n < 623645^{40}$.

Se puede verificar por inducción que $Q_n \geq F_n$, donde F_n es el n-ésimo término de la sucesión de Fibonacci.

Para ello, recordemos que $\frac{P_n}{Q_n} = [a_0, a_1, \ldots, a_n]$ es la n-ésima convergente de la fracción continua $[a_1, a_2, \ldots, a_n, \ldots]$ (donde $a_2, a_3, \ldots, a_n, \ldots$ son enteros positivos), recordemos también que para $n \geq 2$ se tiene que $Q_n = a_n Q_{n-1} + Q_{n-2}$ y $Q_0 = 0$, $Q_1 = 1$.

De lo anterior, se puede observar que $Q_0 = F_0 = 0$, $Q_1 = F_1 = 1$ y $Q_n = a_n Q_{n-1} + Q_{n-2} \geq Q_{n-1} + Q_{n-2} \geq F_{n-1} + F_{n-2} = F_n$, por lo tanto se concluye que $Q_n \geq F_n$ para todo n entero positivo.

Como $F_n = \frac{\gamma^n - \beta^n}{\sqrt{5}}$ donde $\gamma = \frac{1+\sqrt{5}}{2}$ y $\beta = \frac{1-\sqrt{5}}{2}$, se puede verificar que $F_n > \gamma^{n-2}$. Por lo tanto se tiene

$$Q_n > \left(\frac{1+\sqrt{5}}{2}\right)^{n-2}$$

Por lo tanto

$$623645^{40} \geq \gamma^{n-2},$$

entonces

$$n \leq 1112.$$

Lo que nos dice que basta buscar en las primeras 1112 convergentes de la fracción continua de $\sqrt[3]{d}$ las soluciones de la ecuación. Haciendo esto, obtenemos que la única solución es $x = 3$.

Bibliography

[1] Saban Alaca, Kenneth S. Williams, *Introductory Algebraic Number Theory* , Cambridge University, 2004.

[2] A. Baker, *"Linear Forms in logarithms of algebraic numbers. I, II, III"*, Mathematika 13 (1966); 204-216, ibid. 14 (1967), 102-107; ibid. 14 (1967), 220-228.

[3] J. Buchmann, K. Gyory, M. Nignotte y N. Tzanakis, *Lower bounds for $P(x^3+k)$, an elementary aproach*,Publicaciones Matemáticas Debrecen. 38 (1991), 145-163.

[4] Henri Cohen, *Number Theory Volume I: Elementary and Algebraic Methods for Diophantine Equations* , Springer-Verlag, 2007.

[5] Jody Esmonde, M. Ram Murty, *Problems in Algebraic Number Theory*, Springer-Verlag, New York, 1999.

[6] Florian Luca, *Primitive divisors of Lucas sequences and prime factors of $x^2 + 1$ and $x^4 + 1$* , Acta Academiae Pedagociae Agriensis Sectio Mathematicae, 31 (2004), 19-24.

[7] E.M. Matveev, *An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II* , Izv. Ross. Akad. Nauk Ser. Mat. 64 (2000), 125-180; Traducción en Ingles en Izv. Math. 64 (2000), 1217-1269.

[8] Morgan Ward, *The Intrinsic Divisors of Lehmer Numbers* , Annals of Mathematics, Vol 62, No.2 Septiembre 1955, 230-236.