CUBO, Vol. 3, Octubre 1987
Págs. 106-128

ESTRUCTURA DE LOS GRUPOS DE UNIDADES DE LOS ANILLOS COCIENTES DE $Z[\sqrt{2}]$ MODULO POTENCIAS DE PRIMOS

René Romo C. *

INTRODUCCION.

En The American Mathematical Monthly V. 90 N°8 (1983, pág. 518-528) aparece un artículo de J. Cross titulado The Euler Ø-function in the Gaussian Integers. En ese trabajo se define y estudia la función Ø de Euler en $Z[\sqrt{-1}]$ determinando la estructura de los grupos de unidades de los anillos cuocientes módulo potencias de primos en este dominio principal y obteniendo como resultado adicional todos los enteros gaussianos que tiene raíces primitivas.

En mi trabajo definimos y estudiamos la función Ø Euler en $Z[\sqrt{2}]$ y determinamos la estructura de los grupos de unidades de los anillos cuocientes de $Z[\sqrt{2}]$ módulo potencias de

* Dpto. Matemática y Estadística, Universidad de la Frontera.

primos de este dominio principal siguiendo un programa análogo al de Cross en su trabajo [1].

1.- NOCIONES PRELIMINARES:

Sean n un entero $\neq 0$ y $\mathbb{Z}/n\mathbb{Z}$ el anillo cuociente de $\mathbb{Z}$ módulo n. Si $n > 0$, entonces

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$$

donde los paréntesis cuadrados indican clases de equivalencia, módulo n. Las unidades de este anillo forman un grupo multiplicativo que se denota por $(\mathbb{Z}/n\mathbb{Z})^*$. El valor de la función ϕ de Euler en n se define como el orden de este grupo, es decir, para todo $n > 1$,

$$\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$$

Es claro que si $[k]$ en $\mathbb{Z}/n\mathbb{Z}$ es una unidad si y solo si k y n son relativamente primos. Así, para $n > 1$ $\phi(n)$ es el número de enteros positivos menores que n y relativamente primos con n.

Si denotamos por C_n el grupo aditivo (cíclico) de $\mathbb{Z}/n\mathbb{Z}$, entonces para $m > 1$ la estructura de $(\mathbb{Z}/m\mathbb{Z})^*$ está dada por:

i) $(\mathbb{Z}/2\mathbb{Z})^* \cong C_1$

ii) $(\mathbb{Z}/4\mathbb{Z})^* \cong C_2$

iii) $(\mathbb{Z}/2^n\mathbb{Z})^* \cong C_2 \times C_{2^{n-2}}$, $n > 2$

iv) $(\mathbb{Z}/p^n\mathbb{Z})^* \cong C_{p^n - p^{n-1}}$, p primo impar

v) $(\mathbb{Z}/mn\mathbb{Z})^* \cong (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$, $(m,n) = 1$

La estructura de $(\mathbb{Z}/m\mathbb{Z})^*$ para $m > 1$ se obtiene por su factorización en primos. Para una demostración ver [5].

De (v) se obtiene en particular

$$\phi(mn) = \phi(m)\,\phi(n) \text{ , si } (m,n) = 1$$

La definición de la función ϕ de Euler puede extenderse de manera natural a $\mathbb{Z}[\sqrt{2}]$. Sea $\beta \neq 0$ en $\mathbb{Z}[\sqrt{2}]$ y $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\mathbb{Z}[\sqrt{2}]}\right)^*$ el grupo de unidades del anillo $\frac{\mathbb{Z}[\sqrt{2}]}{\beta\mathbb{Z}[\sqrt{2}]}$. Entonces la función ϕ de Euler sobre $\mathbb{Z}[\sqrt{2}]$ se define por

$$\phi(\beta) = \#\left(\frac{\mathbb{Z}[\sqrt{2}]}{\beta\mathbb{Z}[\sqrt{2}]}\right)^* \text{ , } \forall\, \beta \neq 0 \text{ en } \mathbb{Z}[\sqrt{2}]\,.$$

Con mayor generalidad, para todo cuerpo de números $K/\mathbb{Q}$ con anillo de enteros O_k se define la función ϕ_k sobre el conjunto de ideales $\mathfrak{N} \neq (0)$ de O_k por

$$\phi_k(\mathfrak{N}) = \left(\frac{O_k}{\mathfrak{N}}\right)^*$$

Nosotros en este trabajo nos limitamos a considerar solamente el caso $K = \mathbb{Q}(\sqrt{2})$, $O_K = \mathbb{Z}[\sqrt{2}]$.

Por el Teorema Chino del Resto aplicado a $\mathbb{Z}[\sqrt{2}]$ se tiene

$$\frac{\mathbb{Z}[\sqrt{2}]}{(\gamma_1 \cdots \gamma_n)} \cong \frac{\mathbb{Z}[\sqrt{2}]}{(\gamma_1)} \times \cdots \times \frac{\mathbb{Z}[\sqrt{2}]}{(\gamma_m)}$$

donde $\gamma_1, \ldots, \gamma_m$ son enteros relativamente primos. En particular, si $\beta = \beta_1^{n_1} \cdots \beta_r^{n_r}$, $n_i \geq 1$ es la factorización de β en

primos de $Z[\sqrt{2}]$:

$$\frac{Z[\sqrt{2}]}{\beta Z[\sqrt{2}]} \simeq \frac{Z[\sqrt{2}]}{\beta_1^{n_1} Z[\sqrt{2}]} \times \cdots\cdots \times \frac{Z[\sqrt{2}]}{\beta_r^{n_r} Z[\sqrt{2}]}$$

Este isomorfismo de anillos induce un isomorfismo de grupos de unidades

$$\left(\frac{Z[\sqrt{2}]}{\beta Z[\sqrt{2}]}\right)^* \simeq \left(\frac{Z[\sqrt{2}]}{\beta_1^{n_1} Z[\sqrt{2}]}\right)^* \times \cdots \times \left(\frac{Z[\sqrt{2}]}{\beta_r^{n_r} Z[\sqrt{2}]}\right)^*$$

En particular,

$$\phi(\beta) = \phi(\beta_1^{n_1}) \cdots\cdots \phi(\beta_r^{n_r})$$

Vemos que para conocer nuestra función ϕ sobre $Z[\sqrt{2}]$ necesitamos conocer la estructura del grupo de unidades

$\left(\frac{Z[\sqrt{2}]}{\beta^n Z[\sqrt{2}]}\right)$, donde β es un primo en $Z[\sqrt{2}]$. Para ello i) identificamos los primos en $Z[\sqrt{2}]$: Hay solo tres tipos de ellos (Ver, por ejemplo, [3], pág. 221); ii) describimos los elementos de los anillos cuocientes de $Z[\sqrt{2}]$, módulo potencias de primos y los elementos de los grupos de unidades de tales anillos; iii) estudiamos la estructura de estos grupos mediante ejemplos que permitan formular algunas afirmaciones sobre dichas estructuras y (v) demostramos estas afirmaciones.

Afirmamos sin demostración (para una demostración ver [3], página 121) que los primos en $Z[\sqrt{2}]$. Son

a) $\sqrt{2}$

b) Los primos racionales de la forma $8k \pm 3$.

c) Los factores $a+b\sqrt{2}$ de los primos racionales de la forma $8k \pm 1$ (y los asociados de cada uno de los números anteriores).

2.- LAS CLASES DE EQUIVALENCIA EN $\frac{Z[\sqrt{2}]}{\beta^n Z[\sqrt{2}]}$ Y EN $\left(\frac{Z[\sqrt{2}]}{\beta^n Z[\sqrt{2}]}\right)^*$, DONDE β ES PRIMO EN $Z[\sqrt{2}]$.

En esta sección determinamos los elementos de los anillos cuocientes de $Z[\sqrt{2}]$, módulo β^n, β primo en $Z[\sqrt{2}]$ y los elementos de los grupos de unidades de estos anillos. Para ello adoptamos la siguiente notación: $p > 0$ y q indican primos racionales tales que $p \equiv \pm 3(8)$ y $q \equiv \pm 1(8)$. $\widetilde{\Pi}$ indica un factor primo de q y $\alpha = \sqrt{2}$. No hay restricción al considerar solo primos p positivos, pues $(-p)^n = (-1)^n p^n$ y en consecuencia

$$\frac{Z[\sqrt{2}]}{(-1)^n p^n Z[\sqrt{2}]} = \frac{Z[\sqrt{2}]}{p^n Z[\sqrt{2}]}$$

TEOREMA 1.

Las clases de equivalencia de $Z[\sqrt{2}]$, módulo una potencia de un primo están dadas por:

1.- $\frac{Z[\sqrt{2}]}{\pi^n Z[\sqrt{2}]} = \{ [a] \mid 0 \leq a < |q|^n \}$

2.- $\frac{Z'[\sqrt{2}]}{p^n Z'[\sqrt{2}]} = \{[a + b\sqrt{2}] \quad 0 \leq a < p^n, \quad 0 \leq b < p^n\}$

3.- $\frac{Z'[\sqrt{2}]}{\alpha^{2m} Z'[\sqrt{2}]} = \{[a + b\sqrt{2}] \quad 0 \leq a < 2^m ; \quad 0 \leq b < 2^m\}$

4.- $\frac{Z'[\sqrt{2}]}{\alpha^{2m+1} Z'[\sqrt{2}]} = \{[a + b\sqrt{2}] \; 0 \leq a < 2^{m+1}, \; 0 \leq b < 2^m\}$

En el enunciado de este Teorema, así como en los ejemplos que consideramos a continuación entendemos que los conjuntos de representantes son completos y sin repetición.

Dem:

Observemos primero que $\frac{Z'[\sqrt{2}]}{\alpha^{2m} Z'[\sqrt{2}]} = \frac{Z'[\sqrt{2}]}{2^m Z'[\sqrt{2}]}$ y $\frac{Z'[\sqrt{2}]}{\alpha^{2m+1} Z'[\sqrt{2}]} = \frac{Z'[\sqrt{2}]}{2^m \alpha Z'[\sqrt{2}]}$, pues $\alpha^{2m} = 2^m$. Si $a+b\sqrt{2} \equiv c+d\sqrt{2}(\alpha^{2m})$, 2^m divide a $a-c-(b-d)\sqrt{2}$, es decir, 2^m divide a $a-c$ y a $b-d$. Pero $0 \leq a, c < 2^m$, $0 \leq b, d < 2^m$. Luego $a = c$ y $b = d$. Esto significa que las clases en (3) son todas distintas. Un argumento similar se usa para probar que las clases en (2) no se repiten. Las clases en (1) son todas distintas pues si $[a] = [b]$ en $\frac{Z'[\sqrt{2}]}{\pi^n Z'[\sqrt{2}]}$, entonces π^n divide a $a-b$. Sea $a-b = \pi\gamma$, para algún γ en $Z'[\sqrt{2}]$. Conjugando se tiene $a-b = \bar{\pi}\bar{\gamma}$, de manera que $\bar{\pi}$ divide a $a-b$. Como π y $\bar{\pi}$ son primos no asociados se deduce que $\pi^n \bar{\pi}^n = q^n$ divide a $a-b$. Así $a = b$ y las clases en (1) son todas distintas. Finalmente, si $a+b\sqrt{2} \equiv c+d\sqrt{2}(\alpha^{2m+1})$, entonces $2^m \alpha$ divide a $a-c+(b-d)\sqrt{2}$ y 2^m divide a $b-d$. Como $0 \leq b, d < 2^m$, se tiene que $b=d$. Ahora $2^m \alpha$ divide a $a-c$, es decir

$$\frac{a-c}{2^m\alpha} = \frac{(a-c)\alpha}{2^{m+1}} \in \mathbb{Z}[\sqrt{2}]$$

Luego 2^{m+1} divide a a-c y a=c pues $0 \leq a,b < 2^{m+1}$. Hemos probado que las clases en [4] son todas distintas. La demostración de que los sistemas dados por los conjuntos del Teorema son completo no la damos aquí. Puede encontrarse en [6] o efectuando una adaptación la demostración del Teorema 1 en [1].

Este teorema implica que $\frac{\mathbb{Z}[\sqrt{2}]}{\pi^n \mathbb{Z}[\sqrt{2}]}$ tiene $|q|^n$ elementos, $\frac{\mathbb{Z}[\sqrt{2}]}{p^n \mathbb{Z}[\sqrt{2}]}$ tiene p^{2n} elementos y $\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^n \mathbb{Z}[\sqrt{2}]}$ tiene 2^n elementos.

Identificamos ahora las unidades de los anillos cuyos elementos han sido determinados en el Teorema 1.

TEOREMA 2:

Sea [a] en $\frac{\mathbb{Z}[\sqrt{2}]}{\pi^n \mathbb{Z}[\sqrt{2}]}$. Entonces [a] es una unidad si y solo si (a,q) = 1. Sea [a+b$\sqrt{2}$] en $\frac{\mathbb{Z}[\sqrt{2}]}{p^n \mathbb{Z}[\sqrt{2}]}$. Entonces [a+b$\sqrt{2}$] es una unidad si y solo si (a,p) =1 o (b,p) = 1. Sea [a+b$\sqrt{2}$] en $\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^n \mathbb{Z}[\sqrt{2}]}$. Entonces [a+b$\sqrt{2}$] es una unidad si y solo si a es impar.

Dem:

Sean β y γ en $\mathbb{Z}[\sqrt{2}]$. Entonces [β] es una unidad en $\frac{\mathbb{Z}[\sqrt{2}]}{\gamma \mathbb{Z}[\sqrt{2}]}$ si y solo si [β] [ν] = [1] en $\frac{\mathbb{Z}[\sqrt{2}]}{\gamma \mathbb{Z}[\sqrt{2}]}$, para algún $\nu \in \mathbb{Z}[\sqrt{2}]$. Entonces [$\beta$] es una unidad si y solo si $\beta\nu \equiv 1 \ (\gamma)$, esto es, si y solo si $\beta\nu + \gamma\eta = 1$, para cierto η en $\mathbb{Z}[\sqrt{2}]$. Así, [β] es una unidad si y solo si β y γ son relativamente primos. Se deduce

que [a]es una unidad en $\frac{Z/[\sqrt{2}]}{\pi^n Z/[\sqrt{2}]}$ si y solo si $(a, \pi^n) = 1$, si y solo si $\pi \nmid a$, si y solo si $q \nmid a$.

$[a+b\sqrt{2}]$ es una unidad en $\frac{Z/[\sqrt{2}]}{p^n Z/[\sqrt{2}]} \iff (a+b\sqrt{2}, p^n) = 1$ $\iff p \nmid a+b\sqrt{2} \iff p \nmid a$ o $p \nmid b$. Finalmente, $[a+b\sqrt{2}]$ es una unidad en $\frac{Z/[\sqrt{2}]}{\alpha^n Z/[\sqrt{2}]} \iff (a+b\sqrt{2}, \alpha^n) = 1 \iff 2 \nmid a+b\sqrt{2}$. Pero $\sqrt{2}$ divide a $a+b\sqrt{2} \iff \frac{a+b\sqrt{2}}{\sqrt{2}} = \frac{2b+a\sqrt{2}}{2} \in Z/[\sqrt{2}] \iff 2 \mid a$. Es decir $\sqrt{2}$ no divide a $a+b\sqrt{2} \iff a$ es impar.

Ejemplo 1:

Sea $\pi = 1+2\sqrt{2}$. π es primo en $Z/[\sqrt{2}]$ pues $\pi\bar{\pi} = -7$. Por los teoremas 1 y 2 se tiene

$$\frac{Z/[\sqrt{2}]}{\pi^2 Z/[\sqrt{2}]} = \{[0], [1], [2], \ldots, [48]\}$$

y $[a]$ en $\frac{Z/[\sqrt{2}]}{\pi^2 Z/[\sqrt{2}]}$ es una unidad si y solo si 7 no divide a a.

¿A qué clase módulo π^2 pertenece $\sqrt{2}$?. $\pi^2 = 9+4\sqrt{2}$, de modo que $4\sqrt{2} \equiv -9 \ (\pi^2)$. Multiplicando esta congruencia por 12 se obtiene $49\sqrt{2} - \sqrt{2} \equiv -108 \ (\pi^2)$. Ya que $\pi^2 \mid 49$, esta congruencia se reduce a $\sqrt{2} \equiv 10 (\pi^2)$, de modo que $\sqrt{2}$ pertenece a $[10]$.

Observemos que en este ejemplo

$$\left(\frac{Z/[\sqrt{2}]}{\pi^2 Z/[\sqrt{2}]}\right)^* \simeq \left(\frac{Z/}{49Z/}\right)^*$$

Ejemplo 2:

Por los teoremas 1 y 2

$\left(\frac{\mathbb{Z}[\sqrt{2}]}{9\mathbb{Z}[\sqrt{2}]}\right)^* = \{ [a+b\sqrt{2}] \mid 0 \leq a < 9 \ , \ 0 \leq b < 9 \ , \ 3$ es relativamente primo con a o b $\}$

Observemos que $\left(\frac{\mathbb{Z}}{9\mathbb{Z}}\right)^*$ está incluido isomórficamente en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{9\mathbb{Z}[\sqrt{2}]}\right)^*$ pues $\left(\frac{\mathbb{Z}}{9\mathbb{Z}}\right)^* = \{ [1], [2], [4], [5], [7], [8] \}$ puede identificarse mediante la aplicación inclusión con $\{ [1], [2], [4], [5], [7], [8] \}$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{9\mathbb{Z}[\sqrt{2}]}\right)^*$.

Ejemplo 3.

En virtud de los Teoremas 1 y 2

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^5\mathbb{Z}[\sqrt{2}]}\right)^* = \left(\frac{\mathbb{Z}[\sqrt{2}]}{4\alpha\mathbb{Z}[\sqrt{2}]}\right)^*$$

$$= \{[1], [3], [5], [7], [1+\sqrt{2}], [3+\sqrt{2}], [5+\sqrt{2}], [7+\sqrt{2}], [1+2\sqrt{2}], [3+2\sqrt{2}], [5+2\sqrt{2}], [7+2\sqrt{2}], [1+3\sqrt{2}], [3+3\sqrt{2}], [5+3\sqrt{2}], [7+3\sqrt{2}] \}$$

Observemos que $\left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right)^* = \{ [1], [3], [5], [7] \}$ está incluído isomórficamente en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{4\alpha\mathbb{Z}[\sqrt{2}]}\right)^*$. Ya que $\left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right)^*$ no es cíclico, $\left(\frac{\mathbb{Z}[\sqrt{2}]}{4\alpha\mathbb{Z}[\sqrt{2}]}\right)^*$ tampoco lo es. Determinemos la estructura de este grupo. Sean H, K y J subgrupos de $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^5\mathbb{Z}[\sqrt{2}]}\right)^*$ generados por $[1+\sqrt{2}]$, $[5]$ y $[-1]$ respectivamente. Entonces

$$H = \{[1], [1+\sqrt{2}], [3+2\sqrt{2}], [7+\sqrt{2}]\}$$
$$K = \{[1], [5]\} \quad \text{y} \quad J = \{[1], [-1]\}$$

Se tiene que $KJ = \{[1], [3], [5], [7]\}$, de modo que $H \cap KJ = \{[1]\}$. Luego el orden de HKJ es 16.

Luego $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^5 \mathbb{Z}[\sqrt{2}]}\right)^* = HKJ \simeq C_2 \times C_2 \times C_4$.

Usando los teoremas 1 y 2 podemos contar los elementos de los grupos de unidades. Encontramos los siguientes resultados:

i) $\phi(\pi^n) = q^n - q^{n-2} = q^{n-1}(q-1)$

ii) $\phi(p^n) = p^{2n} - p^{2n-2} = p^{2n-2}(p^2-1)$

iii) $\phi(\alpha^n) = 2^n - 2^{n-1} = 2^{n-1}$

3.- LA ESTRUCTURA DE $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\pi^n \mathbb{Z}[\sqrt{2}]}\right)^*$.

Vimos en el Ejemplo 1 que $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\pi^2 \mathbb{Z}[\sqrt{2}]}\right)^*$ es cíclico. Esta es exactamente la situación general.

TEOREMA 3:

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{\pi^n \mathbb{Z}[\sqrt{2}]}\right)^* \simeq C_{|q|^n - |q|^{n-1}}$$

Dem:.

Por el Teorema 2

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{\pi^n \mathbb{Z}[\sqrt{2}]}\right)^* = \{[a] \mid 0 \leq a < |q|^n \; ; \; q \nmid a\}$$

Se demuestra sin dificultad que la aplicación

$[a] \in \left(\frac{Z'}{|q|^m Z'}\right)^* \to [a] \in \left(\frac{Z'[\quad 2\quad]}{\pi^n Z'[\quad 2]}\right)^*$ es un isomorfismo

de $\left(\frac{Z'}{|q|^n Z'}\right)^*$ sobre $\left(\frac{Z'[\sqrt{2}]}{\pi^n Z'[\sqrt{2}]}\right)^*$

Esto prueba el Teorema.

4.- ALGUNAS IDEAS PRELIMINARES REFERENTES A $(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^n \mathbb{Z}[\sqrt{2}]})^*$ Y A $(\frac{\mathbb{Z}[\sqrt{2}]}{p^n \mathbb{Z}[\sqrt{2}]})^*$.

En la sección anterior tratamos de primos en $\mathbb{Z}[\sqrt{2}]$ que son factores de primos racionales. Los grupos de unidades que corresponden a los otros dos tipos de primos son en general no cíclicos, según lo visto en el Ejemplo 3. Mostramos en ese Ejemplo que $(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^5 \mathbb{Z}[\sqrt{2}]})^* \simeq C_2 \times C_2 \times C_4$. El ejemplo que damos a continuación muestra que podemos obtener una estructura similar cuando α se eleve a una potencia par.

Ejemplo 4.

Por los Teoremas 1 y 2.

$$(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^6 \mathbb{Z}[\sqrt{2}]})^* = \{ [a+b\sqrt{2}] \mid 0 \leq a,b < 8 \text{ , } a \text{ es impar.} \}$$

Sean como antes H,K y J los subgrupos de $(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^6 \mathbb{Z}[\sqrt{2}]})^*$ generados por $[1+\sqrt{2}]$, $[5]$ y $[-1]$ respectivamente. Entonces

$$H = \{[1], [1+\sqrt{2}], [3+2\sqrt{2}], [7+5\sqrt{2}], [1+4\sqrt{2}], [1+5\sqrt{2}], [3+6\sqrt{2}], [7+\sqrt{2}]\}$$

$$K = \{[1], [5]\}, \quad J = \{[1], [-1]\}$$

Se tiene que $KJ = \{[1],[3],[5],[7]\}$, de modo que $H \cap (KJ) = \{[1]\}$. Luego el orden de $H(KJ)$ es $32 = \emptyset(\alpha^6)$.

Los ejemplos 3 y 4 permiten afirmar que $(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^n \mathbb{Z}[\sqrt{2}]})^* = HKJ$; donde H,K y J son los subgrupos generados

por $[1+\sqrt{2}]$, $[5]$ y $[-1]$ respectivamente. Consideremos ahora afirmaciones referentes a $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\mathbb{Z}[\sqrt{2}]}\right)^*$. Estas involucran un subgrupo generado por $[1+p\sqrt{2}]$. Estudiaremos este subgrupo y el subgrupo H. Mediante cálculos directos podemos calcular las órdenes de algunos de los elementos de estos grupos. Los resultados de estos cálculos se resumen en la siguiente Tabla, donde hemos calculado los máximos órdenes observados y el orden de $[1+p\sqrt{2}]$

GRUPO	ORDEN	MAX.ORDEN DE UN ELTO.	ORDEN DE $[1+p\sqrt{2}]$
$\left(\frac{\mathbb{Z}[\sqrt{2}]}{3^2\mathbb{Z}[\sqrt{2}]}\right)^*$	$72=3^2(3^2-1)$	$24=3(3^2-1)$	3
$\left(\frac{\mathbb{Z}[\sqrt{2}]}{3^3\mathbb{Z}[\sqrt{2}]}\right)^*$	$648=3^4(3^2-1)$	$72=2^2(3^2(3^2-1)$	9
$\left(\frac{\mathbb{Z}[\sqrt{2}]}{5^2\mathbb{Z}[\sqrt{2}]}\right)^*$	$600=5^2(5^2-1)$	$120=5(5^2-1)$	5
$\left(\frac{\mathbb{Z}[\sqrt{2}]}{5^3\mathbb{Z}[\sqrt{2}]}\right)^*$	$15000=5^4(5^2-1)$	$600=5^2(5^2-1)$	24
$\left(\frac{\mathbb{Z}[\sqrt{2}]}{11^2\mathbb{Z}[\sqrt{2}]}\right)^*$	$11^2(11^2-1)$	$1320=11(5^2-1)$	11

Vemos que en cada caso el mayor orden observado es $p^{n-1}(p^2-1)$ y el producto de este número con p^{n-1} es $\emptyset(p^n)=p^{2n-2}(p^2-1)$. Podemos afirmar que $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\mathbb{Z}[\sqrt{2}]}\right)^* = LK$, donde L es cíclico de orden $p^{n-1}(p^2-1)$ y k tienen orden p^{n-1}. Esto implicaría que $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\mathbb{Z}[\sqrt{2}]}\right)^* = HKR$, donde H tiene orden p^{n-1} y R tiene orden p^2-1. Observamos también que el orden de $[1+p\sqrt{2}]$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\mathbb{Z}[\sqrt{2}]}\right)^*$ parece ser p^{n-1}, si $n>1$.

EJEMPLO 5.

Sabemos que

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{9\mathbb{Z}[\sqrt{2}]}\right)^* = \{[a+b\sqrt{2}] \mid 0 \leq a,b < 9;\ (3,a) = 1 \text{ o } (3,b) = 1.\}$$

Sean H,K y R los subgrupos de $\left(\frac{\mathbb{Z}[\sqrt{2}]}{9\,\mathbb{Z}[\sqrt{2}]}\right)^*$ generados por $[1 + 3\sqrt{2}]$, $[4]$ y $[7 + 5\sqrt{2}]$. Entonces

$H = \{[1], [1+3\sqrt{2}], [1+6\sqrt{2}]\}$; $K = \{[1], [4], [7]\}$

y

$R = \{[1], [7+5\sqrt{2}], [7\sqrt{2}], [7+4\sqrt{2}], [8], [2+4\sqrt{2}], [2\sqrt{2}], [2+5\sqrt{2}]\}$

ya que $H \cap K = \{[1]\}$, el orden de HK es 9 y como 8 es relativamente primo con 9, $(HK) \cap R = \{[1]\}$. Se tiene así que HKR tiene $72 = \emptyset(9)$ elementos y por lo tanto

$$\left(\frac{\mathbb{Z}[\sqrt{2}]}{9\,\mathbb{Z}[\sqrt{2}]}\right)^* = HKR$$

En resumen, los ejemplos 3,4 y 5 y la Tabla nos permiten afirmar que

i) $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^n\mathbb{Z}[\sqrt{2}]}\right)^* = HKJ$, donde H,K y J son generados por $[1+\sqrt{2}]$, $[5]$ y $[-1]$ respectivamente

ii) $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\mathbb{Z}[\sqrt{2}]}\right)^* = HKR$, donde H es generado por $[1 + p\sqrt{2}]$, k tiene orden p^{n-1} , $(n>1)$ y R tiene orden p^2-1.

Probaremos estas afirmaciones estudiando los subgrupos indicados por H en (i) y (ii) con la ayuda de los siguientes Lemas cuya demostración puede verse en [6].

LEMA 1:

Sea k entero positivo. Entonces

$(1+p\sqrt{2})^{p^k} = 1+p^{k+1}\sqrt{2} + p^{k+2}\gamma$, donde $\gamma \in Z[\sqrt{2}]$

LEMA 2:

Sea n entero positivo mayor que 1. Sea $\rho = 1 + p\sqrt{2}$. Entonces el orden de $[\rho]$ en $\left(\frac{Z[\sqrt{2}]}{p^n Z[\sqrt{2}]}\right)^*$ es p^{n-1}.

Estudiamos ahora el orden de $[1+\sqrt{2}]$ en $\left(\frac{Z[\sqrt{2}]}{\alpha^{2m} Z[\sqrt{2}]}\right)^*$ y en $\left(\frac{Z[\sqrt{2}]}{\alpha^{2m+1} Z[\sqrt{2}]}\right)^*$

LEMA 3:

Sea m entero positivo mayor que 1. Sea $\nu = 1+\sqrt{2}$. Entonces el orden de $[\nu]$ en $\left(\frac{Z[\sqrt{2}]}{\alpha^{2m} Z[\sqrt{2}]}\right)^*$ y en $\left(\frac{Z[\sqrt{2}]}{\alpha^{2m+1} Z[\sqrt{2}]}\right)^*$ es 2^m.

El siguiente Lema se refiere a la forma de los elementos del subgrupo indicado por H en (i) y (ii).

LEMA 4:

Sean m y n enteros positivos mayores que 1. Sean $\rho = 1+p\sqrt{2}$ y $\nu = 1+\sqrt{2}$. Ningún elemento, excepto [1], del subgrupo de $\left(\frac{Z[\sqrt{2}]}{p^n Z[\sqrt{2}]}\right)^*$ generado por $[\rho]$ y ningún elemento, excepto [1], del subgrupo de $\left(\frac{Z[\sqrt{2}]}{\alpha^{2m} Z[\sqrt{2}]}\right)^*$ y de $\left(\frac{Z[\sqrt{2}]}{\alpha^{2m+1} Z[\sqrt{2}]}\right)^*$ generado por $[\nu]$ puede representarse por una clase de la forma $[c]$ o $[c\sqrt{2}]$, donde c es un entero racional.

Dem:

Un número $C \in \mathbb{R}$ se llama especial si $C \in \mathbb{Z}$ o $C = C_1\sqrt{2}$, donde $C_1 \in \mathbb{Z}$. Probaremos que para todo b, $0 < b < p^{n-1}$, b no es congruente módulo p^n a un número especial. Sea

$$B = \{ b \mid 0<b<p^{n-1} \ , \ \rho^b \equiv C(p^n)\}.$$

$p^{n-2} \notin B$, pues si $p^{n-2} \in B$, entonces $\rho^{p^{n-2}} \equiv s(p^n)$. Por otra parte, haciendo $k = n-2$ en la fórmula del Lema 1 se tiene $\rho^{p^{n-2}} \equiv 1 + p^{n-1}\sqrt{2}\ (p^n)$. Es decir $1-s+p^{n-1}\sqrt{2} \equiv 0(p^n)$. Si $s \in \mathbb{Z}$, entonces $p^n | p^{n-1}$. Si $s = s_1\sqrt{2}$, entonces $p^n | 1$. En ambos casos hay contradicciones. Luego $p^{n-2} \notin B$. Para completar la demostración supongamos que B es no vacío y sea L el menor elemento de B. Sean d y r en $\mathbb{Z}$ tales que

$$p^{n-1} = L\,d + r \quad , \quad \text{con} \quad 0 \leq r < L.$$

Si $r = 0$, $p^{n-1} = Ld$ y $L = p^t$, para algún t tal que $0<k\leq n-2$. (Hemos demostrado que $t \neq n-2$).

Entonces;

$$\rho^{p^{n-2}} = \rho^{L.p^{n-2-t}}$$

Como $L \in B$, $\rho^L \equiv$ # especial (p^n) y en consecuencia

$$\rho^{p^{n-2}} = \rho^{L.p^{n-2-k}} \equiv \text{\# especial } (p^n),$$

lo que es imposible pues $p^{n-2} \notin B$. Por lo tanto $r \neq 0$.
Ya que el orden de $[\rho]$ es p^{n-1},

(1) $[1] = [\rho^{Ld}][\rho^r] = [s][\rho^r]$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\mathbb{Z}[\sqrt{2}]}\right)^*$, donde s es un número especial. Sea $s = x$ o $s = x\sqrt{2}$, x entero racional. Ya que $[s]$ es un elemento de $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\mathbb{Z}[\sqrt{2}]}\right)^*$ entonces p no divide a x.

Sea $y \in Z/$ tal que $[xy] = [1]$ en $(Z/_{p^n Z/})^*$, entonces p^n divide a $xy - 1$ en $Z/$ y también en $Z/[\sqrt{2}]$. Por tanto $[xy] = [1]$ en $\left(\frac{Z/[\sqrt{2}]}{p^n Z/[\sqrt{2}]}\right)^*$. Multiplicando (1) por $[y]$ se obtiene

(2) $[y] = [ys][\rho^r]$ en $\left(\frac{Z/[\sqrt{2}]}{p^n Z/[\sqrt{2}]}\right)^*$.

si $s = x$, entonces $[y] = [\rho^r]$

si $s = x\sqrt{2}$, entonces $[y] = [\sqrt{2}][\rho^r]$

Pero $[\sqrt{2}]$ es un elemento de $\left(\frac{Z/[\sqrt{2}]}{p^n Z/[\sqrt{2}]}\right)^*$ y $[\sqrt{2}]^{-1} = [u\sqrt{2}]$, u entero racional, es una clase especial, de manera que $[\rho^r] = [yu\sqrt{2}]$. En ambos casos ρ^r es congruente, módulo p^n, a un número especial, es decir $r \in B$ lo que contradice nuestra elección de L. Esta contradicción proviene de suponer que B no es vacío. Hemos demostrado la primera parte del Lema. La demostración de la segunda parte del Lema 4 puede verse en [6].

5.- ESTRUCTURA DE $\left(\frac{Z/[\sqrt{2}]}{p^n Z/[\sqrt{2}]}\right)^*$.

Afirmamos en la sección precedente que $\left(\frac{Z/[\sqrt{2}]}{p^n Z/[\sqrt{2}]}\right)^* = HKR$, donde H es generado por $[1+p\sqrt{2}]$, K tiene orden p^{n-1} y R es de orden p^2-1. Hemos establecido las propiedades que nos interesan de H. Estudiamos ahora el subgrupo K.

Vimos en el Ejemplo 2 que $(Z/_{9Z})^*$ está contenido en $\left(\frac{Z/[\sqrt{2}]}{9Z/[\sqrt{2}]}\right)^*$ mediante un isomorfismo obvio. Esto es un caso particular del siguiente resultado general: la aplicación

$[a] \in (\mathbb{Z}/p^n\mathbb{Z})^* \rightarrow [a] \in \left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\mathbb{Z}[\sqrt{2}]}\right)^*$

es un isomorfismo. Sabemos que $(\mathbb{Z}/p^n\mathbb{Z})^*$ es cíclico de orden $p^{n-1}(p-1)$. Entonces existe $[a]$ en $(\mathbb{Z}/p^n\mathbb{Z})^*$ de orden p^{n-1}. El isomorfismo implica luego que $[a]$ tiene orden p^{n-1} en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\mathbb{Z}[\sqrt{2}]}\right)^*$. Sea K el subgrupo generado por $[a]$. Cada elemento de K se representa por una clase especial. Así, $H \cap K = \{[1]\}$ y HK es de orden p^{2n-2}.

Estudiamos ahora el subgrupo R. Como p es primo en $\mathbb{Z}[\sqrt{2}]$, $\frac{\mathbb{Z}[\sqrt{2}]}{p\mathbb{Z}[\sqrt{2}]}$ es un cuerpo y $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p\mathbb{Z}[\sqrt{2}]}\right)^*$ es cíclico de orden p^2-1, ya que es el grupo multiplicativo de un cuerpo finito. Sea $[\beta]$ un generador de este grupo. Entonces $\beta^{p^2-1} \equiv 1\ (p)$ y $\beta^{p^2-1} = 1+\gamma p$, cierto $\gamma \in \mathbb{Z}[\sqrt{2}]$. Por la demostración del Lema 1, $(\beta^{p^2-1})^{p^{n-1}} = 1+\eta p^n$, con η en $\mathbb{Z}[\sqrt{2}]$. por tanto $(\beta^{p^{n-1}})^{p^2-1} \equiv 1(p^n)$, es decir, el orden de $[\beta^{p^{n-1}}]$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\mathbb{Z}[\sqrt{2}]}\right)^*$ es un divisor de p^2-1. Sea t el orden de $[\beta^{p^{n-1}}]$. Entonces $\beta^{p^{n-1}t} \equiv 1(p^n)$ y en consecuencia $\beta^{p^{n-1}t} \equiv 1(p)$. Ya que el orden de $[\beta]$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p\mathbb{Z}[\sqrt{2}]}\right)^*$ es p^2-1, se tiene que p^2-1 divide a tp^{n-1}. Como p^2-1 y p^{n-1} son relativamente primos, sigue que p^2-1 es un divisor de t. Luego $t = p^2-1$ y el orden de $[\beta^{p^{n-1}}]$ en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\mathbb{Z}[\sqrt{2}]}\right)^*$ es p^2-1. Sea R el subgrupo de $\left(\frac{\mathbb{Z}[\sqrt{2}]}{p^n\mathbb{Z}[\sqrt{2}]}\right)^*$ generado por $[\beta^{p^{n-1}}]$. Ya que todo elemento de HK tiene orden una potencia de p, $(HK) \cap R = \{[1]\}$ y el orden de HKR es $p^{2n-2}(p^2-1) = \phi(p^n)$. Así, la afirmación

$(\frac{Z[\sqrt{2}]}{p^n Z[\sqrt{2}]})^*$ = HKR está demostrada. En resumen

TEOREMA 4:

$$(\frac{Z[\sqrt{2}]}{p^n Z[\sqrt{2}]})^* \simeq C_{p^{n-1}} \times C_{p^{n-1}} \times C_{p^2-1}$$

La demostración de este Teorema es válida solo para $n > 1$, pero el Teorema también se cumple para $n=1$. En este caso $C_{p^{n-1}}$ es trivial y $(\frac{Z[2]}{p Z[2]})^* \simeq C_{p^2-1}$

6.- ESTRUCTURA DE $(\frac{Z[\sqrt{2}]}{\alpha^n Z[\sqrt{2}]})^*$

Afirmamos en la Sección 4 que $(\frac{Z[\sqrt{2}]}{\alpha^n Z[\sqrt{2}]})^*$ = HKJ ; donde H,K y J son los subgrupos generados por $[1+\sqrt{2}]$, $[5]$ y $[-1]$ respectivamente. Sin embargo el Lema 3 se cumple para $m > 1$, de manera que para $n < 4$ determinamos directamente la estructura de $(\frac{Z[\sqrt{2}]}{\alpha^n Z[\sqrt{2}]})^*$. Más aún, en $(\frac{Z[\sqrt{2}]}{4 Z[\sqrt{2}]})^*$ el subgrupo generado por $[5]$ es trivial. Por tanto, damos la estructura de $(\frac{Z[\sqrt{2}]}{\alpha^n Z[\sqrt{2}]})^*$ en dos Teoremas, el primero aplicable a $n = 1, 2, 3$ y 4 y el segundo, a $n \geq 5$.

TEOREMA 5:

$$(\frac{Z[\sqrt{2}]}{\alpha Z[\sqrt{2}]})^* \simeq C_1 ; \quad (\frac{Z[\sqrt{2}]}{\alpha^2 Z[\sqrt{2}]})^* \simeq C_2$$

$$\left(\frac{Z[\sqrt{2}]}{\alpha^3 Z[\sqrt{2}]}\right)^* \simeq C_4 \quad ; \quad \left(\frac{Z[\sqrt{2}]}{\alpha^4 Z[\sqrt{2}]}\right)^* \simeq C_2 \times C_4$$

Dem:

Por el Teorema 2.

$$\left(\frac{Z[\sqrt{2}]}{\alpha\, Z[2]}\right)^* = \{[1]\}$$

$$\left(\frac{Z[\sqrt{2}]}{\alpha^2 Z[\sqrt{2}]}\right)^* = \{[1], [1+\sqrt{2}]\}$$

$$\left(\frac{Z[\sqrt{2}]}{\alpha^3 Z[\sqrt{2}]}\right)^* = \{[1], [3], [1+\sqrt{2}], [3+\sqrt{2}]\}$$

$$\left(\frac{Z[\sqrt{2}]}{\alpha^4 Z[\sqrt{2}]}\right)^* = \{[1], [3], [1+\sqrt{2}], [3+\sqrt{2}], [1+2\sqrt{2}], [3+2\sqrt{2}],$$
$$[1+3\sqrt{2}], [3+3\sqrt{2}]\}$$

Podemos verificar que $\left(\frac{Z[\sqrt{2}]}{\alpha^3 Z[\sqrt{2}]}\right)^*$ es el grupo cíclico de orden 4 generado por $[1+\sqrt{2}]$ y $\left(\frac{Z[\sqrt{2}]}{\alpha^4 Z[\sqrt{2}]}\right)^*$ es el producto directo de sus subgrupos cíclicos.

$H = \{[1], [1+\sqrt{2}], [3+2\sqrt{2}], [3+\sqrt{2}]\}$; $L = \{[1], [3]\}$

Supongamos ahora que $n > 5$ y probemos la afirmación (i) de la Sección 4. Hemos estudiado el subgrupo H en lo que se refiere a su orden y a la forma de sus elementos. Las propiedades de K que nos interesan están dadas en el siguiente Lema.

LEMA 5:

Sea $n \geq 5$. El orden de [5] en $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^n \mathbb{Z}[\sqrt{2}]}\right)^*$ es 2^{m-2} o 2^{m-1} si $n = 2m$ o $n = 2m+1$. El elemento [-1 | de $\left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^n \mathbb{Z}[\sqrt{2}]}\right)^*$ no está en K.

Dem:

Se demuestra usando inducción que para $\ell \geq 3$

$$5^{2^{\ell-3}} \equiv 1 + 2^{\ell-1} \ (2^\ell)$$

y

$$5^{2^{\ell-2}} \equiv 1 \ (2^\ell)$$

Cuando $n = 2m$ o $n = 2m+1$, hagamos $\ell = m$ o $\ell = m+1$ en (*). Se obtienen

$$5^{2^{m-2}} \equiv 1 \ (2^m) \quad \text{y} \quad 5^{2^{m-1}} \equiv 1 (2^{m+1}) ,$$

es decir, [5] tiene orden 2^{m-2} en $(\mathbb{Z}/2^m\mathbb{Z})^*$ y orden 2^{m-1} en $(\mathbb{Z}/2^{m+1}\mathbb{Z})^*$

ya que las aplicaciones

$$[a] \in (\mathbb{Z}/2^m\mathbb{Z})^* \to [a] \in \left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m}\mathbb{Z}[\sqrt{2}]}\right)^*$$

y

$$[a] \in (\mathbb{Z}/2^{m+1}\mathbb{Z})^* \to [a] \in \left(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m+1}\mathbb{Z}[\sqrt{2}]}\right)^*$$

Son isomorfismos, se deduce que K tiene orden 2^{m-2} en $\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m}\mathbb{Z}[\sqrt{2}]}$ y orden 2^{m-1} en $(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^{2m+1}\mathbb{Z}[\sqrt{2}]})^*$. Para probar que $[-1]$ no está en K observemos que $-1 \equiv 5^t \ (2^\ell)$, $\forall\ \ell \geq 3$, $0<t<2^{\ell-2}$ implica $2\equiv 0(4)$ lo que es imposible.

Puesto que $[-1]$ no está en K, $K \cap J = \{[1]\}$ y ya que cada elemento de K x J es una clase de la forma $[C]$ con $C \in \mathbb{Z}$, $H \cap (KxJ) = \{[1]\}$. El orden de HxKxJ es por tanto

$2^m \cdot 2^{m-2} \cdot 2 = 2^{2m-1} = 2^{n-1} = \emptyset(\alpha^n)$, si $n = 2m$

$2^m \cdot 2^{m-1} \cdot 2 = 2^{2m} = 2^{n-1} = \emptyset(\alpha^n)$, si $n = 2m+1$

Por tanto $(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^n\mathbb{Z}[\sqrt{2}]})^* = HxKxJ$. Hemos probado el siguiente Teorema:

TEOREMA 6:

Si $n \leq 5$, entonces

$$(\frac{\mathbb{Z}[\sqrt{2}]}{\alpha^n\mathbb{Z}[\sqrt{2}]})^* \simeq \begin{cases} C_{2^m} \times C_{2^{m-2}} \times C_2 & , \text{ si } n = 2m \\ C_{2^m} \times C_{2^{m-1}} \times C_2 & , \text{ si } n = 2m+1 \end{cases}$$

REFERENCIAS:

[1] Cross, J. The Euler Ø function in The Gaussian Integers American Math. Monthey N° 8 (1983) Pág. 518-528.

[2] Romo, R. La función Ø de Euler en $Z/[\sqrt{2}]$. Tesis de Magister (1987), Facultad de Ciencias Universi - dad de Chile.

[3] Hardy, Wright. An Introduction to The Theory of Numbers Oxford Press. (1954).

[4] Ireland-Rosen. A Classical Introduction to Modern Number Theory. Springer Verlag N.Y. Inc. GTM 84 (1982) Pág. 39-45.