Visión Antataura
Vol.1, No.1 (2017):74-94
Panamá
ISSN 2520-9892

Ley de reciprocidad cuadrática en los enteros gaussianos

Temístocles Zeballos M.[1], Ronall García.[2]

[1]Magíster en Matemática Pura. Profesor, Departamento de Matemática, Centro Regional Universitario de Azuero, Universidad de Panamá; temizeballos@gmail.com
[2]Magíster en Matemática Pura. Profesor, Departamento de Matemática, Centro Regional Universitario de Azuero; ronallgarcia@hotmail.com

Resumen: Este trabajo presenta los resultados más importantes sobre la Ley de Reciprocidad Cuadrática en los Enteros Gaussianos $(\mathbb{Z}[i])$. Para ello se muestran conceptos importantes como Entero Gaussiano, Norma de un Elemento en $(\mathbb{Z}[i])$, Primo Gaussiano, Primo Inerte, Primo Ramificado y Clases Residuales en $(\mathbb{Z}[i])$. Antes de abordar la Ley de Reciprocidad Cuadrática se describen una serie de teoremas, lemas y proposiciones necesarios para llevar a cabo el estudio de dicha ley. Se desarrollaron rutinas con el Software Wolfram Mathematica 10, cuya finalidad es calcular el Símbolo de Legendre, el Símbolo de Residuo Cuártico y presentar gráficas como la de los Primos Gaussianos.

Palabras clave: Ley de Reciprocidad Cuadrática, Entero Gaussiano, Primo Gaussiano, Reciprocidad Cuártica.

Abstract: This work studies the Quadratic Reciprocity Law in $(\mathbb{Z}[i])$. For this, important concepts, like the Gaussian Integer, the Norm of an Element in $(\mathbb{Z}[i])$, the Gaussian Prime, the Inert Prime, the Ramified Prime, and the Residue Classes in $(\mathbb{Z}[i])$, are presented. Before tackling the Quadratic Reciprocity Law, a series of theorems, lemmas, and propositions are described in order to carry out the study of such Law. Routines were developed using the Software Wolfram Mathematica 10, with the purpose of calculating the Legendre Symbol, and the Quartic Residue Symbol, and also of presenting graphics as those of the Guaussian Primes.

Key words: Quadratic Reciprocity Law, Gaussian Integer, Gaussian Prime, Quartic Reciprocity.

Fecha de recepción: 1 de noviembre de 2016 *Fecha de aceptación: 10 de enero de 2017*

1. Introducción

Durante los siglos XVIII y XIX, las matemáticas se desarrollaron radicalmente. Durante este período la teoría de números tuvo un gran desarrollo. Muchos matemáticos jugaron un papel importante en el mismo, como lo fueron Fermat, Euler, Legendre y Gauss.

Gauss, conocido como el príncipe de las matemáticas, es muy importante en esta lista. En 1801 publicó su obra **Disquisitiones Arithmeticae** y fue en este trabajo que introdujo la notación moderna de congruencia. Además, en esta misma obra enuncia y demuestra la Ley de Reciprocidad Cuadrática, que es una de las joyas de la matemática del siglo XVIII y XIX.

Cabe señalar que Gauss no fue el primero en enunciar esta ley, pero fue el primero en ofrecer una prueba rigurosa y además realizó ocho pruebas diferentes.

Fermat, Euler y Legendre estudiaron esta ley y habían conjeturado que era cierta y manejaban algunos resultados que habían obtenido con la misma. Esta ley ha llamado la atención de algunos de los más grandes matemáticos, ya que a la fecha se conocen 233 pruebas distintas de esta.

En este trabajo presentaremos los resultados más importantes sobre la ley de reciprocidad cuadrática y cuártica en el anillo de los Enteros Gaussianos $\left(\mathbb{Z}\left[i\right]\right)$.

2. Enteros Gaussianos y Propiedades

2.1. Definición (Enteros Gaussianos): Los Enteros Gaussianos son los elementos del conjunto:

$$\mathbb{Z}[i]=\left\{a+bi : a,b\in\mathbb{Z}\right\}.$$

Ambos $\mathbb{Z}$ y $\mathbb{Z}[i]$ son anillos conmutativos con identidad (respectivamente 1 y $1+0i$).

2.2. Definición (Norma): La norma de $a+bi\in\mathbb{Z}[i]$ es $N\left(a+bi\right)=a^2+b^2$.

2.3. Ejemplo: $N\left(57-11i\right)=(57)^2+(11)^2=3249+121=3370.$

2.4 Lema: Para todo Entero Gaussiano s y t, $N\left(s\right)N\left(t\right)=N\left(st\right).$

Demostración: Sea $s=a+bi$ y $t=c+di.$ Primero note que:

$$st=(a+bi)(c+di)=(ac-bd)+i(ad+bc).$$

Entonces por resultados simples de álgebra tenemos que:

$$\begin{aligned}N(st)&=(ac-bd)^2+(ad+bc)^2.\\&=a^2c^2-2abcd+b^2d^2+a^2d^2+2abcd+b^2c^2.\\&=a^2c^2+b^2d^2+a^2d^2+b^2c^2.\\&=a^2(c^2+d^2)+b^2(c^2+d^2).\\&=(a^2+b^2)(c^2+d^2).\\&=N\left(s\right)N\left(t\right).\end{aligned}$$

2.5 Proposición (Unidades en $\mathbb{Z}[i]$): $\mathbb{Z}[i]^{\times}=\{1,-1,i,-i\}.$

2.6 Lema: Para todo Entero Gaussiano s y t con $t\neq 0,$

$$N\left(\frac{s}{t}\right)=\frac{N(s)}{N(t)}.$$

Demostración: Sea $s=a+bi$ y $t=c+di$ con $c\neq 0,\ d\neq 0.$ Calculemos $\frac{s}{t}$:

$$\frac{s}{t}=\frac{a+bi}{c+di}\cdot\frac{c-di}{c-di}=\frac{(a+bi)(c-di)}{c^2+d^2}=\frac{ac-adi+cbi+bd}{c^2+d^2}=\frac{(ac+bd)+(cb-ad)i}{c^2+d^2}.$$

Luego,

$$N\left(\frac{s}{t}\right)=N\left[\frac{ac+bd}{c^2+d^2}+\frac{cb-ad}{c^2+d^2}i\right].$$
$$=\frac{(ac+bd)^2}{(c^2+d^2)^2}+\frac{(cb-ad)^2}{(c^2+d^2)^2}.$$
$$=\frac{a^2c^2+b^2d^2+2acbd+c^2b^2+a^2d^2-2acbd}{(c^2+d^2)^2}.$$
$$=\frac{a^2c^2+c^2b^2+b^2d^2+a^2d^2}{(c^2+d^2)(c^2+d^2)}.$$
$$=\frac{c^2(a^2+b^2)+d^2(a^2+b^2)}{(c^2+d^2)(c^2+d^2)}.$$
$$=\frac{(a^2+b^2)(c^2+d^2)}{(c^2+d^2)(c^2+d^2)}.$$
$$=\frac{a^2+b^2}{c^2+d^2}.$$
$$=\frac{N(s)}{N(t)}.$$

Así, $N\left(\frac{s}{t}\right)=\frac{N(s)}{N(t)}$.

2.7. Definición: Decimos que un Entero Gaussiano $a+bi$ divide a un Entero Gaussiano $c+di$ si y solamente si existe un Entero Gaussiano $e+fi$ tal que:

$$c+di=(a+bi)(e+fi).$$

Si esto ocurre entonces diremos que $(a+bi)\mid(c+di)$.

2.8. Ejemplo: $14+3i\nmid 57-11i$ porque $\frac{153}{41}-\frac{65}{41}i\notin\mathbb{Z}[i]$. Pero si tratamos con otro Entero Gaussiano al azar como $7-25i$, entonces tenemos que $\frac{57-11i}{7-25i}=1+2i$. Luego $7-25i\mid 57-11i$, claramente también se tiene que $1+2i\mid 57-11i$.

Mediante la siguiente rutina desarrollada en *Mathematica 10*, se pueden calcular los divisores gaussianos (salvo unidades) de los enteros menores e iguales a n, simplemente se reemplaza n por el entero que deseamos.

```
Grid[Table[{i, Divisors[i,GaussianIntegers→True]},{i,n}]]
```

2.9. Ejemplo: Calculemos los divisores gaussianos de los enteros menores e iguales a 10, usando la rutina anterior desarrollada en Mathematica 10.

```
In[1]:= Grid[Table[{i, Divisors[i,GaussianIntegers→True]},{i,10}]]
Out[1]=
1    {1}
2    {1,1+i,2}
3    {1,3}
4    {1,1+i,2,2+2i,4}
5    {1,1+2i,2+i,5}
6    {1,1+i,2,3,3+3i,6}
7    {1,7}
8    {1,1+i,2,2+2i,4,4+4i,8}
9    {1,3,9}
10   {1,1+i,1+2i,1+3i,2,2+i,2+4i,3+i,4+2i,5,5+5i,10}
```

2.10. Definición (Primo Gaussiano): Un Entero Gaussiano γ es un Primo Gaussiano si y solamente si los únicos Enteros Gaussianos que dividen a γ son:

$$1, -1, i, -i, \gamma, -\gamma, \gamma i, \text{ y } -\gamma i.$$

De acuerdo a esta definición todos los Enteros Gaussianos tienen por lo menos 8 divisores. Ahora surgen las siguientes interrogantes: ¿Hay Primos Gaussianos? ¿Son infinitos? ¿Todo primo en $\mathbb{Z}$, es también un primo en $\mathbb{Z}[i]$?

Tomemos el primo más pequeño, es decir al 2. Como $2=(1+i)(1-i)$, entonces 2 no es un Primo Gaussiano. Luego no todos los primos en $\mathbb{Z}$ son primos en $\mathbb{Z}[i]$. Pero $2=(-1+i)(-1-i)$. Lo que da la impresión de que la factorización prima no es única.

Pero ¿estamos seguros que $(1+i), (1-i), (-1+i), (-1-i)$ son primos? Veamos esto: ellos son números que tienen norma 2. Así que cualquier número que los divide debe tener norma 1 ó 2 (2.6. Lema). Pero si uno de estos factores, digamos σ, se escribe como $\sigma=\alpha\beta$ entonces uno α ó β tiene norma 1, y por lo tanto es una unidad. Pero esto significa que los únicos divisores de σ son $1, -1, i$ y $-i$, y también $\sigma, -\sigma, i\sigma$ y $-i\sigma$. Por lo tanto, σ sería un primo y hemos encontrado nuestros primeros primos. De aquí se deduce que el 2 se escribe como producto de dos Primos Gaussianos.

Note que:

$$(1+i)(1-i)=(-i)(-1+i)(i)(-1-i).$$

Luego la factorización prima del 2 es única ya que las dos representaciones vistas son iguales, solo que una incluye múltiplos de la unidad.

Probemos ahora que la factorización en primos es única en $\mathbb{Z}[i]$:

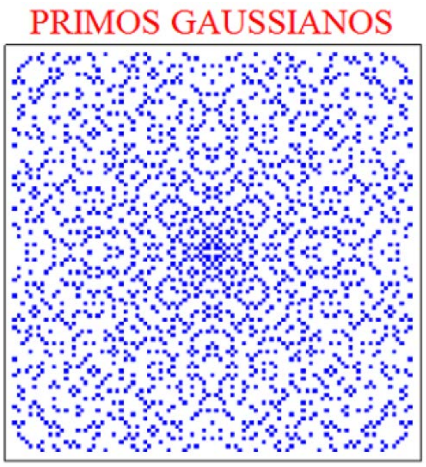
Primero probaremos por inducción la existencia de una factorización en primos. Asumiremos que cada Entero Gaussiano con norma más grande que 1 y menor que n tiene una factorización en primos. Un Entero Gaussiano con norma n es primo o compuesto. Si es primo, hemos encontrado una factorización en primos. Si es compuesto, entonces podemos factorizarlo en dos Enteros Gaussianos ambos con normas menores que n. Así, ambos de estos Enteros Gaussianos tendrá factorización en primos. Luego la factorización en primos de los Enteros Gaussianos en cuestión será el producto de dos factorizaciones en primos.

Ahora probaremos la unicidad de la factorización en primos. Supongamos que hay Enteros Gaussianos con múltiples factorizaciones en primos. Sea α un Entero Gaussiano con la norma más pequeña posible que tiene múltiples factorizaciones en primos. Sean las dos factorizaciones $\alpha = \pi_1 \cdots \pi_s$ y $\alpha = \gamma_1 \cdots \gamma_t$ donde todos los π_i y γ_i son primos y las dos factorizaciones no son iguales. Note que α no puede ser un primo porque un primo sólo tiene una factorización. Así $s, t \geq 2$. Note que $\pi_1 \big| \gamma_1 \cdots \gamma_t$. Luego $\pi_1 \big| \gamma_i$ para algún i. Sin pérdida de generalidad, asumamos que $\pi_1 \big| \gamma_1$. Sin embargo, π_1 y γ_1 son ambos primos, así que $\pi_1 = \gamma_1$. Por lo tanto, $\pi_2 \cdots \pi_s = \dfrac{\alpha}{\pi_1} = \gamma_2 \cdots \gamma_t$. Estas dos factorizaciones de $\dfrac{\alpha}{\pi_1}$ son diferentes. Sin embargo $N(\pi_1) > 1,\ N\left(\dfrac{\alpha}{\pi_1}\right) < N(\alpha)$. Pero nosotros asumimos que α tenía la norma más pequeña posible para un Entero Gaussiano con múltiples factorizaciones, lo que es una contradicción. Así la factorización en primos es única en el Conjunto de los Enteros Gaussianos $\left(\mathbb{Z}[i]\right)$.

Mediante la siguiente rutina desarrollada en *Mathematica 10*, se pueden graficar los primos gaussianos.

```
ArrayPlot[Table[If[PrimeQ[x+Iy,GaussianIntegers→True],1,0],{x,-50,50},{y,-50,50}],
ImageSize→{400,400},ColorRules→{0→White,1→Blue},PlotLabel→Style[Text["PRIMOS GAUSSIANOS"],Red,30]]
```

Veamos lo que produce esta interesante rutina:



2.11. Lema: Todo Primo en $\mathbb{Z}[i]$ divide un primo en $\mathbb{Z}$.

2.12. Definición: Llamaremos **inerte** a los primos en $\mathbb{Z}$ que son primos en $\mathbb{Z}[i]$.

2.13. Definición: Llamaremos **ramificados** a los primos en $\mathbb{Z}$ que se escriben como una unidad por un cuadrado.

2.14. Ejemplo: $2 = i^3(1+i)^2$.

2.15. Teorema: Un número $a+bi$ en $\mathbb{Z}[i]$ es un primo en $\mathbb{Z}[i]$ si y sólo si $a+bi$ es una unidad multiplicada por:

- $1+i$;
- un número primo $p \in \mathbb{Z}$, donde $p \equiv 3(mod\,4)$, ó
- $u+vi$, donde $u^2+v^2 = p$, y p es un primo en $\mathbb{Z}$ con $p \equiv 1(mod\,4)$.

3. Sistemas de clases residuales en los Enteros Gaussianos

3.1. Definición: Decimos que $a+bi \equiv c+di[mod(r+si)]$ si $(r+si)\big|[a-c+(b-d)i]$.

Si $a+bi$ es un primo, ¿cuántas clases residuales hay? Para el primo $1+i$ afirmamos que cada Entero Gaussiano es congruente con 0 ó 1 (mod $1+i$). En efecto, $a+bi \equiv 0$ ó $1[mod(1+i)]$ es cierto si

$$(1+i)\big|(a+bi-0) \text{ ó } (1+i)\big|(a+bi-1)$$

$$(1+i)\big|(a+bi) \text{ ó } (1+i)\big|[(a-1)+bi]$$

$$\frac{a+bi}{1+i}\cdot\frac{1-i}{1-i}=\frac{(a+bi)(1-i)}{1-i+i-i^2}=\frac{(a+bi)(1-i)}{1-i^2}=\frac{(a+bi)(1-i)}{1+1}=\frac{a-ai+bi-i^2b}{2}=\frac{(a+b)+(b-a)i}{2}=\frac{(a+b)}{2}+\frac{(b-a)}{2}i \quad (*)$$

$$\frac{[(a-1)+bi]}{1+i}\cdot\frac{1-i}{1-i}=\frac{a-1-i(a-1)+bi-i^2b}{2}=\frac{a-1-ai+i+bi+b}{2}=\frac{(a+b-1)}{2}+\frac{(b-a+1)i}{2} \quad (**)$$

Si $2\nmid(a+b)$ en (*), entonces $2\big|(a+b-1)$ en (**) y viceversa. Luego $\{0,1\}$ es un sistema completo de residuos módulo $1+i$.

El mismo truco trabaja para primos $c+di$ con norma $p\equiv 1(mod\,4)$: tomamos $i\equiv -\frac{c}{d}[mod(c+di)]$, por lo tanto $a+bi\equiv a-b\frac{c}{d}[mod(a+bi)]$. Así cada Entero Gaussiano es congruente con algún entero módulo $a+bi$. Ahora podemos reducir módulo p (esto es un múltiplo de $a+bi$) y encontramos que cada Entero Gaussiano es congruente con algún elemento $0,1,\ldots,p-1$ módulo $(a+bi)$. Más aún, estos elementos son incongruentes módulo $(a+bi)$: si $r\equiv s[mod(a+bi)]$ para $0\le r,\ s<p$, entonces $(a+bi)\big|(r-s)$; tomando normas dadas $p^2\big|(r-s)^2$, por lo tanto $p\big|(r-s)$ y finalmente $r=s$. Así $\{0,1,\ldots,p-1\}$ es un sistema completo de residuos módulo el primo $a+bi$ con norma p.

Finalmente, consideramos los primos inertes $q\equiv 3(mod\,4)$. Aquí afirmamos que

$$S=\{r+si: 0\le r,s<p\}$$

es un sistema completo de residuos modulo p (note que este conjunto contiene p^2 elementos). Es claro que cada $a+bi \equiv r+si(mod\ p)$ para algún $r+si \in S$: sólo reduce a y b módulo p. Sólo tenemos que mostrar que dos elementos que no están en S son congruentes módulo p. Asumamos por lo tanto que $r+si \equiv t+ui(mod\ p)$ para $0 \le r,\ st,\ u < p.$ Entonces $p \mid [r-t+(s-u)i],$ esto es, $\frac{r-t}{p}+\frac{s-u}{p}i \in \mathbb{Z}[i].$ Esto pasa si y sólo si $r \equiv t(mod\ p)$ y $s \equiv u(mod\ p),$ lo cual implica que $r=t$ y $s=u.$

Hemos probado que:

3.2. Proposición: El sistema completo de residuos módulo un Primo Gaussiano $a+bi$ tiene exactamente $N(a+bi)=a^2+b^2$ elementos.

Consideremos para un primo $p=a^2+b^2 \equiv 1(mod\ 4),$ la función

$$\lambda : \mathbb{Z}/\ p\mathbb{Z} \to \mathbb{Z}[i]/\ (a+bi) : [r]_p \mapsto [r]_{a+bi}.$$

Esto es obviamente un homomorfismo porque $\lambda([r]_p)\lambda([s]_p)=[r]_{a+bi}[s]_{a+bi}=[rs]_{a+bi}=\lambda([rs]_p).$ De lo que hemos visto arriba, λ es suryectiva porque cada clase residual módulo $a+bi$ es representado por uno de los enteros $0,1,...,p-1.$ ¿Es λ inyectiva? Esto es el Kernel es $ker\lambda = \{[r]_p : [r]_{a+bi} = [0]_{a+bi}\}.$ Ahora $r \equiv 0[mod(a+bi)]$ implica que $p^2 \mid r^2,$ por lo tanto $p \mid r,$ así $[r]_p = [0]_p.$ Luego el $ker\lambda = \{[0]_p\},$ y λ es inyectiva.

Nosotros hemos visto que $\lambda : \mathbb{Z}/\ p\mathbb{Z} \to \mathbb{Z}[i]/(a+bi)$ es un isomorfismo: los dos sistemas de clases residuales tienen el mismo número de elementos, la misma estructura, en particular, ellos son ambos cuerpos con p elementos.

¿Qué podemos decir acerca de la clase residual del anillo $R = \mathbb{Z}[i]/(p)$ para primos $p \equiv 3(mod\,4)$? Verifiquemos que R es un dominio, esto es, que este no tiene divisores de cero. En efecto, asumamos que $(a+bi)(c+di) \equiv 0(mod\ p)$. Como p es un primo en $\mathbb{Z}[i]$, esto implica que $p \mid (a+bi)$ ó $p \mid (c+di)$, por lo tanto $[a+bi]_p = [0]_p$ ó $[c+di]_p = [0]_p$, y esto muestra que R es un dominio.

3.3. Proposición: Cualquier dominio R con finitamente muchos elementos es un cuerpo.

3.4. Proposición: Sea $p \equiv 3(mod\,4)$ un primo. Entonces $\mathbb{Z}[i]/(p)$ es un cuerpo con p^2 elementos.

También existen cuerpos finitos con p^2 elementos para primos $p \equiv 1(mod\,4)$, pero estos no pueden ser construidos como cuerpos de clases residuales en $\mathbb{Z}[i]$.

4. La Ley de Reciprocidad cuadrática en los Enteros Gaussianos

Ahora tomemos un primo $\pi = a+bi \equiv 1(mod\,2) \Rightarrow (a-1)+bi \equiv 0(mod\,2) \Rightarrow (a-1)$ y b son pares; note que esto significa que a es impar y b es par. Tenemos que:

4.1. Proposición (Primer Teorema de Fermat): Para cualquier elemento α coprimo con π tenemos que $\alpha^{N\pi-1} \equiv 1(mod\,\pi)$.

4.2. Ejemplo: Calculemos $(1+i)^{N\pi-1}(mod\,\pi)$ para $\pi = 1+2i$.

Note que $1+2i \equiv 1(mod\,2)$. Entonces $N\pi = 1^2 + 2^2 = 5$ y

$$\begin{aligned}(1+i)^{N\pi-1} &= (1+i)^4. \\ &= ((1+i)^2)^2. \\ &= (1+2i+i^2)^2. \\ &= (2i)^2. \\ &= 4i^2. \\ &= -4 \equiv 1(mod\,5).\end{aligned}$$

Así, $(1+i)^{N\pi-1} \equiv 1(mod\,5)$. Como $5 = (1+2i)(1-2i)$, entonces

$$(1+i)^{N\pi-1} \equiv 1(mod[(1+2i)(1-2i)]).$$

Luego

$$(1+i)^{N\pi-1} \equiv 1[mod\,(1+2i)].$$

$$(1+i)^{N\pi-1} \equiv 1(mod\,\pi).$$

Como $\pi = 1+2i \equiv 1(mod\,2)$, encontramos que

$$\begin{aligned}1+2i &\equiv 1(mod\,2). \\ (1+2i)(1-2i) &\equiv 1-2i(mod\,2). \\ 5 &\equiv 1-2i(mod\,2). \\ 5 &\equiv 1(mod\,4).\end{aligned}$$

O sea que

$$N\pi = a^2 + b^2 = 1+4 \equiv 1(mod\,4)$$

lo que implica que

$$N\pi - 1 \equiv 0(mod\,4).$$

Como $\alpha^{N\pi-1} - 1 \equiv 0(mod\,\pi)$ y $\alpha^{N\pi-1} - 1 = \left(\alpha^{\frac{N\pi-1}{2}} - 1\right)\left(\alpha^{\frac{N\pi-1}{2}} + 1\right)$ tenemos que

$$\left(\alpha^{\frac{N\pi-1}{2}} - 1\right)\left(\alpha^{\frac{N\pi-1}{2}} + 1\right) \equiv 0(mod\,\pi).$$

Luego

$$\alpha^{\frac{N\pi-1}{2}}-1\equiv 0(mod\,\pi)$$
$$\alpha^{\frac{N\pi-1}{2}}+1\equiv 0(mod\,\pi)$$

ya que π es primo. O sea

$$\alpha^{\frac{N\pi-1}{2}}\equiv \pm 1(mod\,\pi).$$

Ahora definamos el Símbolo Cuadrático de Legendre $\left[\frac{\alpha}{\pi}\right]=\pm 1$ en $\mathbb{Z}[i]$ por:

$$\left[\frac{\alpha}{\pi}\right]\equiv \alpha^{\frac{N\pi-1}{2}}(mod\,\pi).$$

4.3. Ejemplo: *Calcular* $\left[\frac{1+i}{1+2i}\right]$.

Mediante una rutina desarrollada en *Mathematica 10*, se puede calcular el Símbolo de Legendre.

```
c1=Input[“Escriba el Entero Gaussiano (recuerde que la i se escribe en mayúscula):”]
c2=Input[“Escriba el Módulo (recuerde que debe ser un Primo Gaussiano congruente con
          1 módulo 2 y que la i se escribe en mayúscula):”]
If[PrimeQ[c2,GaussianIntegers→True],
  If[EvenQ[Re[c2]],
    Print[“La Parte Real del módulo (“,c2,”) debe ser impar.”],
    If[OddQ[Im[c2]], Print [“La Parte Imaginaria del módulo (“,c2,”) debe ser par.”],
     If[CoprimeQ[c1,c2],
      nor:=Abs[c2]^2;
      exp:=(nor-1)/2;
      pot:=(c1)^exp;
      leg:=Mod[pot,c2];
      Print[“El Símbolo de Legendre es: “,leg,”.”],
      Print[c1,” no es coprimo con “, c2, “.”]]]],
Print[c2” no es un Primo Gaussiano.”]]
1+i
1+2i
El Símbolo de Legendre es: -1.
```

Con esta rutina se calculó que $\left[\frac{1+i}{1+2i}\right]=-1.$

Veamos algunas propiedades simples de estos símbolos en $\mathbb{Z}[i]$.

4.4. Proposición: Para elementos $\alpha,\ \beta,\ \pi\in\mathbb{Z}[i]$ con $\pi\equiv 1(mod\,2)$ primo tenemos que:

1. $\left[\frac{\alpha}{\beta}\right]=\left[\frac{\beta}{\pi}\right]\ si\ \ \alpha\equiv\beta(mod\,\pi);$
2. $\left[\frac{\alpha\beta}{\pi}\right]=\left[\frac{\alpha}{\pi}\right]\left[\frac{\beta}{\pi}\right];$
3. $\left[\frac{\alpha}{\pi}\right]=+1\ \ si\ \ \alpha\equiv\xi^2(mod\,\pi).$

Demostración:

1. Si $\alpha=\beta(mod\,\pi)$, entonces $\alpha^{\frac{N\pi-1}{2}}\equiv\beta^{\frac{N\pi-1}{2}}(mod\,\pi)$ y por lo tanto, $\left[\frac{\alpha}{\beta}\right]=\left[\frac{\beta}{\pi}\right].$
2. $\left[\frac{\alpha\beta}{\pi}\right]\equiv(\alpha\beta)^{\frac{N\pi-1}{2}}(mod\,\pi)\equiv\alpha^{\frac{N\pi-1}{2}}\beta^{\frac{N\pi-1}{2}}(mod\,\pi)=\left[\frac{\alpha}{\pi}\right]\left[\frac{\beta}{\pi}\right].$ *Así* $\left[\frac{\alpha\beta}{\pi}\right]=\left[\frac{\alpha}{\pi}\right]\left[\frac{\beta}{\pi}\right].$
3. Si $\alpha\equiv\xi^2(mod\,\pi);$ entonces $\alpha^{\frac{N\pi-1}{2}}\equiv\xi^{2(\frac{N\pi-1}{2})}(mod\,\pi).$ Luego, $\alpha^{\frac{N\pi-1}{2}}\equiv\xi^{N\pi-1}(mod\,\pi).$

   Como, $\xi^{N\pi-1}\equiv 1(mod\,\pi)$ (por el Primer Teorema de Fermat), tenemos que

   $$\alpha^{\frac{N\pi-1}{2}}\equiv 1(mod\,\pi).$$

   Luego, por definición, $\left[\frac{\alpha}{\pi}\right]=+1.$

También usaremos algunos resultados sobre el carácter cuadrático de ciertos enteros.

4.5. Proposición: Sea $p = a^2 + b^2$ un primo impar, y supongamos que a es impar. Entonces:

- $\left(\frac{a}{p}\right) = 1.$
- $\left(\frac{b}{p}\right) = \left(\frac{2}{p}\right).$
- $\left(\frac{a+b}{p}\right) = \left(\frac{2}{a+b}\right).$

Demostración: Como $p = a^2 + b^2$ es un primo impar entonces, $p \equiv 1(mod\, 4)$. Luego, $\left(\frac{a}{p}\right) = 1,$ porque a es un entero cuadrático $mod\, p,$ $\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right).$

Como $(a+b)^2 = a^2 + b^2 + 2ab = p + 2ab,$ entonces

$$(a+b)^2 \equiv 2ab(mod\, p)$$
$$(a+b)^2 \equiv a(2b)(mod\, p)$$

y por lo tanto $\left(\frac{a}{p}\right) = \left(\frac{2b}{p}\right).$

$$Como\ \ 2p = 2(a^2 + b^2).$$
$$= 2a^2 + 2b^2.$$
$$= (a+b)^2 + (a-b)^2.$$

Entonces $\left(\frac{a+b}{p}\right) = \left(\frac{p}{a+b}\right) = \left(\frac{2}{a+b}\right).$

Observación:

Para la Ley de Reciprocidad Cuadrática en $\mathbb{Z}[i]$, escribimos $\pi = a+bi$, $\lambda = c+di$; entonces $\pi \equiv \lambda \equiv 1(mod\,2)$ implica que $a \equiv c \equiv 1(mod\,2)$ y $b \equiv d \equiv 0(mod\,2)$. Si $\pi = p \in \mathbb{Z}$ ó $\lambda = \ell \in \mathbb{Z}$, resulta que

$$\left[\frac{p}{\lambda}\right] = \left(\frac{p}{N\lambda}\right) \text{ y } \left[\frac{\pi}{\ell}\right] = \left(\frac{N\pi}{\ell}\right).$$

4.6. Proposición: Para primos $\pi \in \mathbb{Z}[i]$ y elementos $a \in \mathbb{Z}$ coprimos con π tenemos que $\left[\frac{a}{\pi}\right] = \left(\frac{a}{N\pi}\right)$.

Demostración:

Como $\left[\frac{a}{\pi}\right] \equiv a^{\frac{N\pi-1}{2}}(mod\,\pi)$ y $\left(\frac{a}{N\pi}\right) \equiv a^{\frac{N\pi-1}{2}}(mod\,N\pi)$. Por lo tanto, $\left[\frac{a}{\pi}\right] \equiv a^{\frac{N\pi-1}{2}}(mod\,\pi)$ y $\left(\frac{a}{N\pi}\right) \equiv a^{\frac{N\pi-1}{2}}(mod\,\pi)$, lo que implica que $\left[\frac{a}{\pi}\right] \equiv \left(\frac{a}{N\pi}\right)(mod\,\pi)$. Si los símbolos fueran diferentes, entonces sería

$1 \equiv -1(mod\,\pi)$.

$2 \equiv 0(mod\,\pi)$.

Entonces π debe dividir a 2, y por lo tanto $N\pi$ debe dividir a 4, y esto no tiene sentido ya que π tiene norma impar mayor que 1.

Así, podemos asumir que $p = N\pi$ y $\ell = N\lambda$ son primos. Encontramos inmediatamente que

$$ai \equiv b(mod\,\pi) \text{ y } ci \equiv d(mod\,\lambda).$$
$$ai \equiv b[mod(a+bi)] \text{ y } ci \equiv d[mod(c+di)].$$
$$ai - b \equiv 0[mod(a+bi)] \text{ y } ci - d \equiv 0[mod(c+di)].$$

Note que:

$$\frac{ai-b}{a+bi}=i \text{ y } \frac{ci-d}{c+di}=i.$$

Luego obtenemos que:

$$\left[\frac{\pi}{\lambda}\right]=\left[\frac{c}{\lambda}\right]\left[\frac{ac+bci}{\lambda}\right]=\left[\frac{c}{\lambda}\right]\left[\frac{ac+bd}{\lambda}\right].$$

Como $c\in\mathbb{Z}$ y $ac+bd\in\mathbb{Z},$ tenemos:

$$\left[\frac{c}{\lambda}\right]=\left(\frac{c}{\lambda}\right) \quad \text{y} \quad \left[\frac{ac+bd}{\lambda}\right]=\left(\frac{ac+bd}{\lambda}\right).$$

Usando Proposición 4.5, tenemos que:

$$\left[\frac{\pi}{\ell}\right]=\left(\frac{ac+bd}{\ell}\right). \qquad (1)$$

Pero ahora $p\ell=(a^2+b^2)(c^2+d^2)=(ac+bd)^2+(ad-bc)^2\equiv(ad-bc)^2[mod(ac+bd)]$ lo cual implica que $\left(\frac{\ell}{ac+bd}\right)=\left(\frac{p}{ac+bd}\right),$ y aplicando la Ley de Reciprocidad Cuadrática en $\mathbb{Z}$ dos veces tenemos que:

$$\left(\frac{ac+bd}{\ell}\right)=\left(\frac{\ell}{ac+bd}\right)=\left(\frac{p}{ac+bd}\right)=\left(\frac{ac+bd}{p}\right).$$

La Ley de Reciprocidad Cuadrática en $\mathbb{Z}[i]$ se sigue por simetría:

$$\left[\frac{\pi}{\lambda}\right]=\left(\frac{ac+bd}{\ell}\right)=\left(\frac{ac+bd}{p}\right)=\left[\frac{\lambda}{\pi}\right].$$

Las leyes suplementarias se siguen inmediatamente de (1), poniendo $a=0, b=1$ ó $a=b=1,$ y usando reciprocidad cuadrática.

5. La Ley de Reciprocidad Cuártica en los Enteros Gaussianos

Consideremos un primo $\pi = a + bi \equiv 1(mod\, 2),$ para cualquier elemento α coprimo con $\pi,$ tenemos que $\alpha^{N\pi-1} - 1 \equiv 0(mod\, \pi)$ (Primer Teorema de Fermat).

Como, $\alpha^{N\pi-1} - 1 = \left(\alpha^{\frac{N\pi-1}{2}} - 1\right)\left(\alpha^{\frac{N\pi-1}{2}} + 1\right)$ $\left[ya\ que\ N\pi - 1 \equiv 0(mod\, 2)\right]$ y

$$\left(\alpha^{\frac{N\pi-1}{2}} - 1\right)\left(\alpha^{\frac{N\pi-1}{2}} + 1\right) = \left(\alpha^{\frac{N\pi-1}{4}} - 1\right)\left(\alpha^{\frac{N\pi-1}{4}} + 1\right)\left(\alpha^{\frac{N\pi-1}{4}} - i\right)\left(\alpha^{\frac{N\pi-1}{4}} + i\right).$$

$\left[Ya\ que\ N\pi - 1 \equiv 0(mod\, 4)\right]$ Tenemos que:

$$\left(\alpha^{\frac{N\pi-1}{4}} - 1\right)\left(\alpha^{\frac{N\pi-1}{4}} + 1\right)\left(\alpha^{\frac{N\pi-1}{4}} - i\right)\left(\alpha^{\frac{N\pi-1}{4}} + i\right) \equiv 0(mod\, \pi).$$

Por lo tanto, podemos definir el símbolo de residuo bicuadrático o cuártico $\left[\frac{\alpha}{\pi}\right]_4 \in \{1, -1, i, -i\}$ tal que:

$$\left[\frac{\alpha}{\pi}\right]_4 \equiv \alpha^{\frac{N\pi-1}{4}} (mod\, \pi) \text{ se satisfaga.}$$

La Ley de Reciprocidad Cuártica: Sean $\pi, \lambda \in \mathbb{Z}[i]$ primos distintos tal que $\pi \equiv \lambda \equiv 1[mod\,(2+2i)];$ entonces

$$\left[\frac{\pi}{\lambda}\right]_4 = (-1)^{\frac{N\pi-1}{4}\cdot\frac{N\lambda-1}{4}} \left[\frac{\lambda}{\pi}\right]_4.$$

5.1. Ejemplo: *Calcule los símbolos cuárticos* $\left[\frac{1+2i}{1+4i}\right]_4$ *y* $\left[\frac{1+4i}{1+2i}\right]_4$, *y verifique si la Ley de Reciprocidad Cuártica se satisface para estos elementos.*

Calculemos $\left[\frac{1+2i}{1+4i}\right]_4$

$$\left[\frac{1+2i}{1+4i}\right]_4 \equiv (1+2i)^{\frac{N(1+4i)-1}{4}}[mod(1+4i)].$$

Utilizando *Mathematica 10* tenemos que:

$$Mod\left[(1+2i)^{\frac{N(1+4i)-1}{4}},1+4i\right]=-1. \qquad (*)$$

Ahora, calculamos $\left[\frac{1+4i}{1+2i}\right]_4$

$$\left[\frac{1+4i}{1+2i}\right]_4 \equiv (1+4i)^{\frac{N(1+2i)-1}{4}}[mod(1+2i)].$$

Utilizando *Mathematica 10* tenemos que:

$$Mod\left[(1+4i)^{\frac{N(1+2i)-1}{4}},1+2i\right]=-1. \qquad (**)$$

De (*) y (**) concluimos que $\left[\frac{1+2i}{1+4i}\right]_4 = \left[\frac{1+4i}{1+2i}\right]_4$.

Verifiquemos si la Ley de Reciprocidad Cuártica se satisface:

Note que $1+2i \equiv -1\left[mod(2+2i)\right]$ *y por lo tanto no verifica la hipótesis.*

5.2. Ejemplo: *Calcule los símbolos cuárticos* $\left[\frac{17-12i}{3+2i}\right]_4$ *y* $\left[\frac{3+2i}{17-12i}\right]_4$, *y verifique si la Ley de Reciprocidad Cuártica se satisface para estos elementos.*

Calculemos $\left[\frac{17-12i}{3+2i}\right]_4$

$$\left[\frac{17-12i}{3+2i}\right]_4 \equiv (17-12i)^{\frac{N(3+2i)-1}{4}}[mod(3+2i)].$$

Utilizando *Mathematica 10* tenemos que:

$$Mod\left[(17-12i)^{\frac{N(3+2i)-1}{4}}, 3+2i\right] = 1. \quad (*)$$

Ahora, calculamos $\left[\frac{3+2i}{17-12i}\right]_4$

$$\left[\frac{3+2i}{17-12i}\right]_4 \equiv (3+2i)^{\frac{N(17-12i)-1}{4}}[mod(17-12i)].$$

Utilizando *Mathematica 10* tenemos que:

$$Mod\left[(3+2i)^{\frac{N(17-12i)-1}{4}}, 17-12i\right] = 1. \quad (**)$$

De (*) y (**) concluimos que $\left[\frac{17-12i}{3+2i}\right]_4 = \left[\frac{3+2i}{17-12i}\right]_4$.

Note que:

$$1 = \left[\frac{17-12i}{3+2i}\right]_4 = (-1)^{\frac{N(17-12i)-1}{4}\cdot\frac{N(3+2i)-1}{4}}\left[\frac{3+2i}{17-12i}\right] = (-1)^{324} = 1.$$

Por lo tanto se verifica la ley.

Mediante la siguiente rutina desarrollada en *Mathematica 10*, se puede calcular el símbolo de residuo cuártico:

```
c1=Input["ESCRIBA EL NÚMERO PRIMO GAUSSIANO"]
c2=Input["ESCRIBA EL MÓDULO"]
If[PrimeQ[c1,GaussianIntegers→True],
 If[PrimeQ[c2,GaussianIntegers→True],If[c1..c2,Print["LOS PRIMOS GAUSSIANOS TIENEN QUE SER
          DISTINTOS."],
   If[Mod[c1,2+2I]=1,If[Mod[c2,2+2I]=1,nor:=Abs[c2]^2;
      exp:=(nor-1)/4;
      pot:=(c1)^exp;
      leg:=Mod[pot,c2];
      Print["EL SÍMBOLO DE RESIDUO CUÁRTICO ES: ",leg,"."], Print["EL NÚMERO ",c2," TIENE
            QUE SER CONGRUENTE CON 1 MÓDULO 2+2I"]], Print["EL NÚMERO ",c1," TIENE QUE SER

            CONGRUENTE CON 1 MÓDULO 2+2I"]]],Print["EL MÓDULO TIENE QUE SER PRIMO
            GAUSSIANO."]],Print["EL NÚMERO TIENE QUE SER PRIMO GAUSSIANO."]]
  17-12i
  3+2i
EL SÍMBOLO DE RESIDUO CUÁRTICO ES: 1.
```

Con esta rutina se calculó que $\left[\frac{17-12i}{3+2i}\right]_4 = 1.$

Referencias bibliográficas

Lemmermeyer, F. (2000). *Reciprocity Laws: From Euler to Eisenstein*. New York, USA: Springer.

Koshy, T. (2007). *Elementary Number Theory with Applications*. California, USA: Elsevier Inc.

Burton, D. M. (1980). *Elementary number theory*. Boston, USA: Allyn and Bacon, Inc.

Hardy, G. H. (1979). *Wright, E.M.: An introduction to the theory of numbers*. New York, USA: Oxford Science Public.

Rosen, K.H. (1988). *Elementary number theory*. USA: Addison-Wesley.