13. FACTORIZACIÓN GAUSSIANA Y CUERPOS CUADRÁTICOS

13.1 Teoría de los números algebraicos

1.1 Teoría de los números algebraicos.

La teoría algebraica de los números es la rama de la teoría de los números en la cual el concepto de número se expande a los números algebraicos, los cuales son las raíces de los polinomios con coeficiente racional.
Un campo de números algebraicos es una extensión finita, algebraica, del campo de los números racionales. El anillo de enteros de un campo de números algebraicos es la cerrazón de los enteros en dicho campo, es decir, el subconjunto del campo que consiste en los elementos que son raíces de polinomios con coeficientes enteros.
Se puede ver, y tratar, a un campo de números algebraicos como un análogo de los racionales, y a su anillo de enteros como análogo de sus enteros, ahora bien, la analogía no es perfecta: algunas de las propiedades familiares de los racionales y los enteros no se conservan, por ejemplo la factorización única.
Los campos de números algebraicos, así como los campos de funciones, son llamados campos globales. Gran parte de la teoría se puede desarrollar de manera paralela para ambos tipos de objetos. La localización consiste en el pasaje de un campo global a un campo local: en el caso de los campos de funciones, este procedimiento consiste simplemente en dirigir la mirada a un punto en particular de la superficie o variedad estudiada, y concentrarse en cómo las funciones se comportan en su vecindad inmediata.

1.2 Anillos y cuerpos.

Un anillo es una terna $(A,+,\cdot)$ en la que A es el conjunto y $+,\cdot$ son las leyes internas en A, de modo que se cumplan las siguientes propiedades:

1. $(a+b)+c=a+(b+c)$, para todos los a,b,c de A. Ley asociativa de la suma.
2. $a+b=b+a$, para todos los a,b de A. Ley conmutativa de la suma.
3. Existe un elemento 0 en A tal que $a+0=a$, para todo a de A. Es el elemento neutro o nulo del anillo.
4. Para todo a de A, existe un $-a$ en A tal que $a+(-a)=0$. Es el elemento simétrico u opuesto.
5. $(ab)c=a(bc)$, para todos los a,b,c de A. Ley asociativa de la multiplicación.
6. $a(b+c)=ab+ac$, $(a+b)c=ac+bc$, para todos los a,b,c de A. Leyes distributivas.

Un anillo es conmutativo si y sólo si $ab=ba$, para todos los elementos a,b de A.
Un anillo es unitario si existe un elemento 1 en A tal que $a\cdot 1=1\cdot a=a$, para todo elemento de a en A.
Un dominio es un anillo conmutativo y unitario en el que $1\neq 0$, luego $\mathbb{Z}$ es un dominio.
Un elemento a de un dominio A, es un divisor de cero si es no nulo y existe un b en A no nulo tal, que $ab=0$. Un dominio íntegro es un dominio sin divisores de cero.
Para dotar a $\mathbb{Z}$ x $\mathbb{Z}$ de estructura de dominio que no sea integro, planteamos lo siguiente:
Sea D y d números enteros con d no nulo. Entonces, existen unos únicos enteros c y r tales que $D=dc+r$ y $0\leqq r<|d|$, donde $|d|$ es igual a d si d es positivo y $a-d$ si es negativo.
Esta propiedad de los números enteros confiere propiedades muy importantes al anillo $\mathbb{Z}$ y es poseída por otros anillos de interés.

Un dominio euclídeo es un dominio íntegro A tal que existe una función $\phi: A \setminus \{0\} \to \mathbb{N}$ que cumpla lo siguiente:
Si a,b son elementos de $\phi(a) \leqq \phi(ab)$. A no nulos.
Si D,d son elementos de A con $d \neq 0$, entonces existen c y r en A de manera que $D = dc + r$ con $r = 0$ o bien $0 \leqq \phi(r) < \phi(d)$.
La función ϕ se llama norma euclidea.
Es obvio que $\mathbb{Z}$ es un dominio euclídeo con la norma ϕ dada por $\phi(a) = |a|$. Ahora bien, observemos que el cociente y el resto no son únicos. Por ejemplo, para dividir 8 entre 3 podemos hacer $8 = 3 \cdot 2 + 2$ o bien $8 = 3 \cdot 3 - 1$, en ambos casos, $|r| < |d|$.
Un elemento a de un dominio A es una unidad si existe un elemento b en A tal que $ab = 1$. Dicho elemento b está determinado por a, ya que si $ab = 1 = ac$, entonces $b = b1 = bac = ac = c1$. Este único elemento lo llamaremos inversos de a y lo representaremos por a^{-1}.
Obviamente 1 es una unidad y $1^{-1} = 1$. En cambio 0 no puede ser una unidad. Una unidad no puede ser divisor de cero, pues si a es una unidad y $ab = 0$, entonces $b = b1 = a^{-1}0 = 0$.
Las unidades de $\mathbb{Z}$ son exactamente 1 y -1. Un anillo de división es un anillo unitario con $1 \neq 0$ en el que todo elemento no nulo es una unidad.
Un cuerpo es un anillo de división conmutativo. En particular todo cuerpo es un dominio íntegro.
Observemos también que todo cuerpo K es un dominio euclídeo tomando como norma la aplicación constante 1, pues la división euclidea puede realizarse siempre con resto 0, es decir, $D = d(D/d) + 0$.
Las operaciones entre números enteros y los elementos de un anillo, pueden ser definidas de la siguiente forma:
Sea A un anillo unitario y a,b elementos de A. Sean m y n números enteros. Se cumple:

1. $m(a+b) = ma + mb$.
2. $(m+n)a = ma + na$.
3. $(-ma) = -(ma) = m(-a)$.
4. $m(na) = (mn)a$.
5. Si $ab = ba$, entonces $(ab)^m = a^m b^m$.
6. $a^{m+n} = a^m a^n$
7. $(a^m)^n = a^{mn}$.
8. $a^{-m} = (a-1)^m = (a^m)^{-1}$.

Además, si $A = \mathbb{Z}$, ma es lo mismo en el sentido de la definición anterior que en el sentido del producto usual en $\mathbb{Z}$.

1.3 Números algebraicos.

Un número algebraico es cualquier número real o complejo que es solución de una ecuación polinómica de la forma

$$a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \ldots + a_1 x + a_0 = 0$$

donde $n > 0 (a_n \neq 0)$, es el grado del polinomio y $a_i \in \mathbb{Z}$, son números enteros coeficientes del polinomio.

Todos los números racionales son algebraicos, porque toda fracción de la forma a/b es solución de $bx-a=0$.
Algunos números irracionales como $2^{1/2}$, raíz cuadrada de 2, y $3^{1/3}/2$, la mitad de la raíz cúbica de 3, también son algebraicos porque son soluciones de $x^2-2=0$ y $8x^3-3=0$, respectivamente.
No todos los números reales son algebraicos. Los casos más conocidos son π y e.
Si un número real o complejo no es algebraico, se dice que es un número trascendente.
Si un número algebraico es solución de una ecuación polinómica de grado n, pero no puede serlo de una ecuación polinómica de grado menor, entonces se dice que es un número algebraico del grado n. Teniendo en cuenta esta circunstancia, los números racionales no pueden ser números algebraicos de primer grado, pues no existe por ejemplo, una ecuación polinómica de grado uno con coeficientes enteros, cuya solución sea la raíz cuadrada de 2.
Las propiedades de la clausura podemos definirlas:

1. La suma, diferencia, producto o cociente de dos números algebraicos vuelve a ser algebraico, y por lo tanto los números algebraicos constituyen un cuerpo matemático.
2. Como consecuencia de lo anterior, todos los números que pueden escribirse a partir de los racionales empleando solamente las operaciones aritméticas $+,-,*,/$, potencias y raíces, son algebraicos. Sin embargo, existen números algebraicos que no pueden escribirse de esta forma, y son todos de grado >5. Ésta es una consecuencia de la Teoría de Galois.
3. Puede demostrarse que si los coeficientes a_i son números algebraicos cualesquiera, la solución de la ecuación volverá a ser número algebraico. En otras palabras, el campo de los números algebraicos es algebraicamente cerrado. De hecho, los números algebraicos son el campo algebraicamente cerrado más pequeño que contiene los racionales.

Un número algebraico que satisface una ecuación polinómica de grado n con $a_n=1$ se denomina entero algebraico. Algunos ejemplos de enteros algebraicos son: $3\cdot 2^{1/2}+5$ ó $6i-2$. La suma, diferencia y producto de enteros algebraicos vuelve a ser un entero algebraico, lo que significa que los enteros algebraicos forman un anillo. El nombre de entero algebraico proviene del hecho de que los únicos números racionales que son enteros algebraicos, son los enteros.

1.4 Números complejos.

El número complejo es un número de la forma $a+bi$, siendo a y b números reales e $i=\sqrt{-1}$ la unidad de los números imaginarios. En el número complejo $a+bi$, a recibe el nombre de parte real y bi el de la parte imaginaria. Si $a=0$, el número complejo se llama imaginario puro. Si $b=0$, el número complejo se reduce al número real a. Por consiguiente, en los números complejos están incluidos todos los números reales y todos los números imaginarios puros.
La condición necesaria y suficiente para que los números complejos $a+bi$ y $c+di$ sean iguales, es que $a=c$ y $b=d$. Así que $a+bi=0$ si y sólo si $a=0$ y $b=0$. Si $c+di=3$, se tendrá que $c=3$ y $d=0$.
El número complejo $a+bi$ es conjugado de $a-bi$, y recíprocamente. Por ejemplo, $5+2i$ es el conjugado de $5-2i$. Si efectuamos el producto, $(5+2i)(5-2i)=5^2+2^2=29$. En el anillo $\mathbb{Z}_{[i]}$ es una norma y genera los llamados enteros de Gauss.
El reciproco del número complejo $a+bi$ es el $b+ai$, y recíprocamente. Por ejemplo, $4-3i$ tiene como recíproco el $3-4i$.

Las operaciones algebraicas con números complejos son:

Suma: Para sumar dos números complejos se suman, por una parte las partes reales y, por otra, las imaginarias. Por ejemplo:

$$(a+bi)+(c+di)=(a+c)+(b+d)i$$
$$(5+4i)+(3+2i)=(5+3)+(4+2)i=8+6i$$

Resta: Para restar dos números complejos se restan, por una parte las parte reales y, por otra, las imaginarias. Por ejemplo:

$$(a+bi)-(c+di)=(a-c)+(b-d)i$$
$$(5+4i)-(3+2i)=(5-3)+(4-2)i=2+2i$$

Multiplicación: Para multiplicar dos números complejos, se realiza la multiplicación como si fueran dos binomios, y en el producto se sustituye i^2 por -1. Por ejemplo:

$$(a+bi)(c+di)=ac+adi+bci+bdi^2=ac+(ad+bc)i+bd(-1)=(ac-bd)+(ad+bc)i$$
$$(5+4i)(3+2i)=15+10i+12i+8i^2=15+22i+8(-1)=7+22i$$

Dividir: Para dividir dos números complejos, se multiplican el numerador y el denominador por el conjugado del denominador y se sustituye i^2 por -1. Por ejemplo:

$$\frac{a+bi}{c-di}=\frac{ac}{c^2+d^2}-\frac{bd}{c^2+d^2}+\left(\frac{ad}{c^2+d^2}+\frac{bc}{c^2+d^2}\right)i$$
$$\frac{2+i}{4-3i}=\frac{(2+i)(4+3i)}{(4-3i)(4+3i)}=\frac{8+6i+4i+3i^2}{16-9i^2}=\frac{5+10i}{25}=\frac{5(1+2i)}{25}=\frac{1}{5}+\frac{2i}{5}$$

Como $i=\sqrt{-1},$ tenemos:

$$i^2=-1$$
$$i^3=i^2\cdot i=(-1)i=-i$$
$$i^4=(i^2)^2=(-1)^2=1$$
$$i^5=i^4\cdot i=1\cdot i=i$$
$$i^6=i^4\cdot i^2=1(-1)=-1,$$

y así sucesivamente.
Una raíz n-ésima de la unidad es cualquiera de los números complejos z que satisfacen a la ecuación $z^n=1$. Las n raíces de la unidad son los números $e^{2\pi ik/n}$, donde k y n son coprimos y representan n a la raíz y k numerando las correspondientes soluciones para los enteros comprendidos entre $k=0$ y $k=n-1$. El número de raíces primitivas diferentes viene determinado por la función Euler, $\varphi(n)$. Por ejemplo, para $z^1=1$ sólo hay una raíz primera de la unidad, igual a 1. Para $z^2=1$ hay dos raíces: $z_1=e^{2\pi i1/2}=-1$ y $z_2=e^{2\pi i2/2}=1$. Para $z^3=1$ hay tres raíces: $z_1=e^{2\pi i3/3}=1,\ z_2=e^{2\pi i1/3}=\frac{-1+i\sqrt{3}}{2}$ y $z_3=e^{2\pi i2/3}=\frac{-1-i\sqrt{3}}{2}$.

Las raíces de la unidad de la ecuación cúbica corresponden a los llamados enteros de Eisenstein, en honor a Ferdinand Gotthold Eisenstein (1823-1852), y se representan como $\pm 1,\ \pm\omega,\ \pm\omega^2$.

Como los ceros del polinomio $p(z)=z^n-1$ son precisamente las raíces n-ésima de la unidad, cada uno con multiplicidad 1, el polinomio ciclotómico n-ésimo está definido por el hecho de que sus ceros son, precisamente, las raíces primitivas n-ésima de la unidad, cada una con multiplicidad 1.

13.2 Factores y divisores gaussianos

2.1 Factorizar el número 10.

La factorización canónica del número 10 es $10=2\cdot 5,$ dos factores primos.
La factorización gaussiana puede ser representada de alguna de las siguientes formas:

1. Como $10=2\cdot 5=(1+i)(1-i)(2+\mathrm{i})(2-\mathrm{i})$
2. Como $10=2\cdot 5=(1+i)(1+i)(2+i)(1+2i)(-1)=(1+i)^2(2+i)(1+2i)(-1)$
3. Como $10=2\cdot 5=(1-i)^2(2+i)(2-i)(i)$
4. Como $10=2\cdot 5=(1+i)^2(2+\mathrm{i})(2-\mathrm{i})(-\mathrm{i})$
5. Como $10=2\cdot 5=(3+i)(3-i)$
6. Como $10=2\cdot 5=(3+i)(1+3i)(-i)$

lo que nos demuestra la factorización no única de los enteros de Gauss, aunque con divisores finitos en el anillo $\mathbb{Z}[i]$. Efectivamente, los divisores de 10 vienen representados en el conjunto:

$$\{1,\ 1+i,\ 1+2i,\ 1+3i,\ 2,\ 2+i,\ 2+4i,\ 3+i,\ 4+2i,\ 5,\ 5+5i,\ 10\}$$

Veamos cómo se consigue todo esto.
Partimos de dos números algebraicos a los que llamaremos $z=1+i$ y $w=2+i$ cuyos conjugados son

$$z=(1+i)(1-i)=1^2+1^2=2 \text{ y } w=(2+i)(2-i)=2^2+1^2=5$$

en donde el producto de ambos resulta

$$zw=(1+i)(1-i)(2+i)(2-i)=3^2+1^2=2\cdot 5=10$$

Esto se conoce como factorización conjugada en el anillo $\mathbb{Z}[i]$.
Si

$$z=(1+i)(1+i)(-i)=(1+i)^2(-i)=1^2+1^2=2 \text{ ó } z=(1-i)(1-i)(i)=(1-i)^2(i)=1^2+1^2=2$$

y

$$w=(2+i)(1+2i)(-i)=2^2+1^2=5 \text{ ó } w=(2-i)(1-2i)(i)=2^2+1^2=5$$

entonces

$$zw=(1+i)(1+i)(2+i)(1+2i)(-1)=(1+i)^2(2+i)(1+2i)(-1)=3^2+1^2=10$$

o bien

$$zw=(1-i)(1-i)(2-i)(1-2i)(-1)=(1-i)^2(2-i)(1-2i)(-1)=3^2+1^2=10$$

Si se cambia el signo de los números algebraicos, también cambia el signo de la unidad.

$$zw=(1+i)^2(2-i)(1-2i)(1)=(1-i)^2(2+i)(1+2i)(1)=10$$

Esto se conoce como factorización opuesta o simétrica con unidad en el anillo $\mathbb{Z}[i]$.
Sea

$$(1+i)(2-i)=(3+i) \text{ y } (1-i)(2+i)=(3-i)$$

entonces

$$zw=(3+i)(3-i)=3^2+1^2=10$$

Es una factorización conjugada en el anillo $\mathbb{Z}[i]$.

Para $(1+i)(2+i)=(1+3i)$ y $(1+i)(2-i)=(3+i),$ tenemos

$$(1+3i)(3+i)(-i)=3^2+1^2=10$$

que es una factorización opuesta o simétrica con unidad en el anillo $\mathbb{Z}[i]$.
Sabemos que todo elemento irreducible del anillo $\mathbb{Z}[i]$ es de la forma $\pm p$ ó $\pm pi$ con p entero positivo primo de la forma $p=4k+3,$ o bien de la forma $p=4k+1=a^2+b^2$ donde $a^2+b^2=a+bi,$ primo con $\mathbb{Z}.$
En las siguientes tablas recogemos algunos de los primos a los que se hace referencia en este apartado:

	Enteros Gaussianos de la forma $4k+1$														
2	5	13	17	29	37	41	53	61	73	89	97	101	109	113	
137	149	157	173	181	193	197	229	233	241	257	269	277	281	293	
313	317	337	349	353	373	389	397	401	409	421	433	449	457	461	

	Primos Gaussianos de la forma $4k+3$														
3	7	11	19	23	31	43	47	59	67	71	79	83	103	107	
127	131	139	151	163	167	179	191	199	211	223	227	239	251	263	
271	283	307	311	331	347	359	367	379	383	419	431	439	443	463	

Para calcular los divisores gaussianos de 10, operamos del siguiente modo:

Por la exposición anterior el 10 es divisible por

$$\frac{10}{1+i}=5-5i=5(1-i),\ \ \frac{10}{2+i}=4-2i=2(2-i),\ \ \frac{10}{3+i}=3-i$$

Ahora establecemos los siguientes grupos de divisores, salvo asociados:

$1+i$	$1-i$	$2+i$
$2-i$	$(1+i)(1-i)=2$	$(1+i)(2+i)=1+3i$
$(1+i)(2-i)=3+i$	$(1-i)(2+i)=3-i$	$(1-i)(2-i)=1-3i$
$(2+i)(2-i)=5$	$2(2+i)=4+2i$	$2(2-i)=4-2i$
$5(1+i)=5+5i$	$5(1-i)=5-5i$	10
1		

En resumen, los divisores gaussianos de 10 son:

$$1,\ 1+i,\ 1+2i,\ 1+3i,\ 2,\ 2+i,\ 2+4i,\ 3+i,\ 4+2i,\ 5,\ 5+5i,\ 10$$

El anillo $\mathbb{Z}[i]=\{a+bi : a,b\in\mathbb{Z}\}$ es un dominio euclídeo con la aplicación $N(a+bi)=a^2+b^2$ definida para todo $a+bi\in\mathbb{Z}$. Aquí N es la norma o conjugado del número real o complejo.

2.2 Factorizar el número algebraico $z=19+5i$.

Supongamos que el número tiene factorización conjugada, entonces

$$z=(19+5i)(19-5i)=386=19^2+5^2$$

Cómo $386=2\cdot 193$ y $193=4k+1=4\cdot 48+1=12^2+7^2$, ambos números (2 y 193) son enteros de Gauss y, por tanto, pertenecen al anillo $\mathbb{Z}[i]$. Así que tenemos

$$(1+i)(1-i)=2 \text{ y } (12+7i)(12-7i)=193$$

con lo que

$$(1+i)(1-i)(12+7i)(12-7i)=386$$

Esto nos lleva a que, los divisores gaussianos de 386, son

1, 1+i, 2, 5+19i, 7+12i, 12+7i, 14+24i, 19+5i, 24+14i, 193, 193+193i, 386

Pero 386 es distinto a $z=19+5i$, por tanto no es esto lo que se nos pide.
Sabemos que $z=19+5i$ puede ser divisible por $(1+i)$ ó $(1-i)$. Veamos:

Si

$$\frac{19+5i}{1+i}=12-7i \text{ ó } \frac{19+5i}{1-i}=7+12i$$

entonces

$$\frac{19+5i}{12-7i}=1+i \text{ ó } \frac{19+5i}{12+7i}=\frac{263}{193}-\frac{73i}{193}$$

Pero en el segundo caso el resultado es distinto a $(1-i),$ por lo que $z=19+5i$ no es divisible por $12+7i,$ luego $(1+i)(7+12i)=19+5i$ o lo que es lo mismo

$$z=19+5i=(1+i)(7+12i)(-i)$$

y sus divisores

$$1,\ 1+i,\ 7+12i,\ 19+5i$$

2.3 Factorizar el número algebraico $z=3+4i.$

El número algebraico $z=3+4i$ es reducible en el anillo $\mathbb{Z}[i],$ ya que $N(3+4i)=25$ es compuesto en $\mathbb{Z}.$ Como $25=5^2$ y $5=(2+i)(2-i),$ tenemos que

$$(3+4i)(3-4i)=25=5^2=(2+i)(2-i)(2+i)(2-i)$$

por tanto, $(2+i)\ y\ (2-i)$ dividen a $(3+4i)(3-4i)$ y como $(2+i)\ y\ (2-i)$ son irreducibles en $\mathbb{Z}[i],$ alguno de ellos debe ser divisor de, al menos, uno de los factores de la izquierda de la igualdad anterior. En este caso

$$(3+4i)=(2+i)(2-i)$$

es la factorización gaussiana del número propuesto.
En cuanto a los divisores de $z=3+4i,$ resultan

$$1,\ 2+i,\ 3+4i$$

Hacemos notar que aquí N es la norma que se define como $N(a+bi)=a^2+b^2.$ Si $z=a+bi$ y $w=c+di$ se verifica que $N(zw)=N(z)N(w)$ ya que si $N(z)=a^2+b^2$ y $N(w)=c^2+d^2$ resulta para $zw=(ac-bd)+(ad+bc)i.$

2.4 Factorizar el número algebraico $z=-45+105i.$

Empecemos por calcular la norma o conjugado de $z=-45+105i.$

$$(-45+105i)(-45-105i)=13050=2\cdot 3^2\cdot 5^2\cdot 29$$

El número 3 es de la forma $3=4k+3=4\cdot 0+3,$ por tanto un primo irreducible de Gauss.
Si eliminamos el 3 y calculamos otra nueva norma, obtenemos

$$\frac{-45+105i}{3}=-15+35i$$

de donde

$$(-15+35i)(-15-35i)=1450=2\cdot 5^2\cdot 29$$

que son todos enteros de Gauss y, por tanto, alguno de ellos debe ser divisor de $-15+35i.$

Probamos con $(2\pm i)$:

$$(-15+35i)/(2+i)=1+17i \text{ y } (-15+35i)/(2-i)=-13+11i$$

Divisiones exactas lo que demuestran que $(2+i)$, $(1+17i)$ y $(-13+11i)$ son divisores de $-15+35i$.

Probamos con $(5\pm 2i)$ ya que $N(5\pm 2i)=5^2+2^2=29$:

$$(-15+35i)/(5+2i)=-\frac{5}{29}+\frac{205i}{29} \text{ y } (-15+35i)/(5-2i)=-5+5i$$

Aquí los divisores de $(-15+35i)$ son $(5+2i)$ y $(-5+5i)$. Este último es un asociado con factorización simétrica con unidad, por lo que los divisores serían $(2+5i)$ y $(5+5i)$.
Como el producto de los divisores conocidos es $3(1+i)(2+i)(2+5i)=-39+33i$ y el cociente con $(-45+105i)$ es $(-45+105i)/(-39+33i)=2-i$, la factorización de $z=-45+105i$ resulta

$$z=-45+105i=3(1+i)(2+i)(2+5i)(2-i)$$

En cuanto a los divisores gaussianos

$$1,\ 1+i,\ 1+2i,\ 1+3i,\ 1+17i,\ 2+i,\ 2+5i,\ 3,3+i,\ 3+3i,\ 3+6i,\ 3+9i,\ 3+51i,$$
$$5,\ 5+5i,\ 6+3i,\ 6+15i,\ 7+3i,\ 9+3i,\ 9+8i,\ 10+25i,\ 11+13i,\ 12+i,15,$$
$$15+15i,\ 21+9i,\ 27+24i,\ 30+75i,\ 33+39i,\ 35+15i,\ 36+3i,\ 105+45i$$

dejamos en sus manos la demostración de todos o algunos de ellos.

2.5 Factorizar el número 136.

La factorización canónica es $136=2^3\cdot 17$, dos factores primos principales que son enteros gaussianos, ya que $z=(1+i)(1-i)=1^2+1^2=2$ y $w=(4+i)(4-i)=4^2+1^2=17$, luego la factorización gaussiana de 136 vendrá determinada por

$$zw=\left((1+\mathrm{i})(1-\mathrm{i})\right)^3(4+\mathrm{i})(4-\mathrm{i})=10^2+6^2=136$$

Ahora bien, si tenemos en cuenta que

$$z=(1+i)(1+i)(-i)=(1+i)^2=1^2+1^2=2 \text{ y } w=(4+i)(1+4i)(-i)=4^2+1^2=17$$

es la factorización simétrica con unidad y que $(1+i)^2(4+i)(1+4i)(-1)=34$, para la factorización gaussiana del 136 resulta

$$zw=(1+i)^6(-i)(4+i)(1+4i)(i)=(1+i)^6(4+i)(1+4i)=136=10^2+6^2$$

Con un poco de paciencia se pueden encontrar los divisores gaussianos del número 136, que son

$1,\ 1+i,\ 1+4i,\ 2,\ 2+2i,\ 2+8i,\ 3+5i,\ 4,\ 4+i,\ 4+4i,\ 4+16i,$
$5+3i,\ 6+10i,\ 8,\ 8+2i,\ 8+32i,\ 10+6i,\ 12+20i,\ 16+4i,\ 17,$
$17+17i,\ 20+12i,\ 32+8i,\ 34,\ 34+34i,\ 68,\ 68+68i,\ 136$

2.6 Factorizar el número algebraico $z=-48+97i$.

El conjugado de $z=-48+97i$ es $(-48+97i)(-48-97i)=11713=13\cdot 17\cdot 53$. La estructura de cada uno de estos factores es la siguiente:

Para $13=4k+1=4\cdot 3+1=3^2+2^2=(3+2i)(3-2i)=(3+2i)(2+3i)(-i)$
Para $17=4k+1=4\cdot 4+1=4^2+1^2=(4+i)(4-i)=(4+i)(1+4i)(-i)$
Para $53=4k+1=4\cdot 13+1=7^2+2^2=(7+2i)(7-2i)=(7+2i)(2+7i)(-i)$

Todos los factores primos son enteros de Gauss, por lo que la factorización gaussiana resulta

$$(3+2i)(2+3i)(4+i)(1+4i)(7+2i)(2+7i)(i)=11713=97^2+48^2$$

Pero nosotros no buscamos esta factorización si no la de $z=\text{-}48+97i$. La presencia del asociado positivo (i) pone de manifiesto que algunos de los divisores de $z=\text{-}48+97i$ son simétricos luego, vamos a probar con $(1+4i)$ y con $(2+7i)$:

Para $(\text{-}48+97i)/(1+4i)=20+17i$ y para $(20+17i)/(2+7i)=3\text{-}2i$ donde el último es el conjugado de $(3+2i)$ y que es $(3-2i)(i)=3+2i$.
De acuerdo con lo expuesto, la factorización gaussiana es

$$z=(1+4i)(3\text{-}2i)(2+7i)=\text{-}48+97i$$

o bien

$$z=(1+4i)(2+3i)(2+7i)(\text{-}i)=\text{-}48+97i$$

Esta última como factorización simétrica con unidad o elemento asociado.
Los elementos $z=a+bi$ y $\overline{z}=a-bi$ son asociados en $\mathbb{Z}[i]$, si y sólo si, z es cualquiera de los cuatro elementos $\pm 1,\ \pm i$, donde $a,b\in\mathbb{Z},\ a\neq 0,\ b\neq 0$ y $z=a+bi$ irreducible en $\mathbb{Z}[i]$. Se pueden dar cuatro casos:

$z=\overline{z}$: es el caso en donde $b=0$. Por ejemplo, $z=(2+0i)(2-0i)=2^2+0^2=4$.
$z=-\overline{z}$: es el caso en donde $a=0$. Por ejemplo, $z=(0+3i)(0-3i)=0^2+3^2=9$.
$z=\overline{z}i$: es el caso en donde $a=b$ y por tanto $z=a+ai=a(1+i)$. Como z es irreducible y $(1+i)$ no es invertible en $\mathbb{Z}[i]$, $a=\pm 1$, y por tanto, los elementos $+1+i$ y $-1-i$.
$z=-\overline{z}i$: es el caso que produce $+1-i$ y $-1+i$.

Es fácil deducir los recíprocos a partir de las igualdades

$$i(1\text{-}i)=1+i,\ \ i(1+i)=\text{-}1+i,\ \ i(\text{-}1+i)=\text{-}1\text{-}i,\ \ i(\text{-}1\text{-}i)=1\text{-}i$$

En el número algebraico $z = -48 + 97i$ no existen factores primos, por lo que sus divisores son todos gaussianos, a saber

$$1,\ 1+4i,\ 2+3i,\ 2+7i,\ 11+10i,\ 15+26i,\ 20+17i,\ 97+48i$$

2.7 Factorizar el número algebraico $z = 84 + 63i$.

Observamos que el Máximo Común Divisor de 84 y 63 es $mcd(84,63) = 21,$ luego el número algebraico planteado tiene una primera representación como $z = 21(4+3i),$ un número asociado.
Cómo

$$(4+3i)(4-3i) = (4+3i)(3+4i)(-i) = 25$$

y el número 25 admite también como factorización gaussiana

$$25 = \left((2+i)(1+2i)\right)^2 (-1)$$

podemos establecer que

$$4+3i = (1+2i)^2(-i)$$

y, por tanto

$$z = 84+63i = 3\cdot 7\cdot (1+2i)^2(-i)$$

En cuando a los divisores de $z = 84+63i,$ tenemos

$$1,\ 1+2i,\ 3,\ 3+6i,\ 4+3i,\ 7,\ 7+14i,\ 12+9i,\ 21,\ 21+42i,\ 28+21i,\ 84+63i$$

Teniendo en cuenta lo comentado sobre los números asociados en el supuesto anterior, observen que entre los divisores de $z = 84+63i$ hayamos algunos, como por ejemplo

$$3+6i = 3(1+2i);\quad 7+14i = 7(1+2i);\quad 12+9i = 3(4+3i);\ \ldots$$

Localicen los que faltan.

13.3 Factorización gaussiana con elementos del anillo $\mathbb{Z}[i]$.

3.1 Sean $z = 4+6i$ y $w = 7-i$ dos números algebraicos. Calcular el $mcd(z,w) = d = zs + wt$.

Sean a y b dos números enteros o algebraicos tales que al menos uno de ellos sea distinto de cero. El Máximo Común Divisor de a y $b,$ que denotaremos como $mcd(a,b) = d,$ donde d es el único entero positivo que satisface a las dos condiciones siguientes:

1. $d \mid a$ y $d \mid b,$ es decir, d es divisor común de a y de $b.$
2. Si $c \mid a$ y $c \mid b,$ entonces $c \le d,$ es decir, d es el mayor de los divisores comunes.

A partir de este Algoritmo de Euclides, el Teorema de Bézout, descubierto por Etienne Bézout (1730-1783), asegura que existen otros dos enteros s y t tales que el $mcd(a,b)=d=as+bt$. Este teorema o identidad nos proporciona una forma lineal dentro del anillo.

La factorización de los números algebraico es la siguiente:

Para $z=4+6i:\ z=(1+i)^2(2+3i)(-i)=4+6i$
Para $w=7-i:\ w=(1+i)(1+2i)^2(-1)=7-i$

El máximo divisor que divide a ambos números es el $(1+i)$, por tanto

$$mcd(4+6i,7-i)=1+i$$

Sabemos que $N(4+6i)=(4+6i)(4-6i)=52$ y que $N(7-i)=(7-i)(7+i)=50$. El Máximo Común Divisor de ambos números es $mcd(52,50)=2$. Cómo $N(1+i)=(1+i)(1-i)=2$, obtenemos el mismo resultado que con la factorización gaussiana.
La forma lineal de $z=4+6i$ y $w=7-i$ resulta

$$mcd(52,50)=2=52(1)+50(-1)$$

para números enteros, donde $s=1$ y $t=-1$

$$mcd(4+6i,7-i)=1+i=(4+6i)(-2)+(7-i)(1+2i)$$

para los números algebraicos, donde $s=-2$ y $t=1+2i$.

3.2 Sean $z=10+11i$ y $w=8+i$ dos números algebraicos. Calcular $mcd(z,w)=d=zs+wt$.

Empecemos por factorizar los dos números algebraicos. A saber

Para $z=10+11i:\ z=(3+2i)(4+i)=10+11i$
Para $w=8+i:\ w=(1+2i)(3+2i)(-i)=8+i$

Claramente podemos observar que el número que divide a ambos algebraicos es el $(3+2i)$. Comprobamos:

$$\frac{10+11i}{3+2i}=4+i\ \rightarrow\ 10+11i=(3+2i)(4+i)$$
$$\frac{8+i}{3+2i}=2-i\ \rightarrow\ 8+i=(3+2i)(2-i)$$

luego, el Máximo Común Divisor de ambos números es

$$mcd(10+11i,8+i)=3+2i$$

En cuanto a la forma lineal, si $s=1$ y $t=-1-i$, tenemos

$$mcd(10+11i,8+i)=3+2i=(10+11i)(1)+(8+i)(-1-i)$$

Si los números algebraicos los transformamos en números enteros, tenemos

$$N(10+11i)=221 \text{ y } N(8+i)=65$$

entonces

$$mcd(221,65)=13=221(-2)+65(7)$$

3.3 Sean $z=3+2i$ **y** $w=1-i$ **dos elementos de** $\mathbb{Z}[i]$. **Encontrar** $c,r\in\mathbb{Z}[i]$ **tales que** $z=cw+r$ **con** $r=0$ *ó* $N(r)<N(w)$.

Un dominio de integridad conmutativo y con unidad D es un dominio euclídeo si existe una aplicación N definida $D^*=D-\{0\}$ con valores en los enteros no negativos tal que

I. $N(r)\le N(rs)$ para todo $r,s\in D^*$.
II. Para todo $t,s\in D,\ s\neq 0,$ existen $c,r\in D$ tales que $t=cs+r,$ con $r=0$ ó $N(r)<N(s)$.

Sean $z=a+bi$ y $w=c+di$ dos elementos de $\mathbb{Z}[i],$ con $w\neq 0$. El cociente $z/w=r+si,$ será un punto del plano complejo de $\mathbb{Z}[i]$ tal que $|r-m|\le 1/2$ y $|s-n|\le 1/2$.
Si anotamos

$$z=(z/w)w=cw+[(r-m)+(s-n)i]w$$

de tal forma que

$$[(r-m)+(s-n)i]w=z-cw\in\mathbb{Z}[i]$$

entonces

$$N([(r-m)+(s-n)i]w)=N((r-m)+(s-n)i)N(w)\le[(1/4)+(1/4)]N(w)<N(w)$$

Esto se conoce como división euclidea de polinomios en el anillo $\mathbb{Z}[i]$.
Aplicado a nuestro caso, tenemos

$$(3+2i)/(1-i)=(1/2)+(5/2)i$$

Si $c=2i,$ resulta para

$$z=(2i)w+[(1/2)+(1/2)i]w=(2i)w+1$$

de donde

$$N(1)=1<2=N(w)$$

Como $z=(2i)(1-i)+1=3+2i$ y $N(1)<N(1-i)=1<2,$ la solución se ajusta la división euclidea de polinomios.

Observen que la descomposición no es única:

$$z=(3i)w+\left[(1/2)-(1/2)i\right]w=(3i)w-i$$

donde $z=(3i)(1-i)+(-i)=3+2i$ y $N(-i)<N(1-i)=1<2.$

3.4 Sean $z=7-5i,\ w=3+4i$ dos números algebraicos. Calcular la división euclidea tal que $z/w=r+si$.

Empecemos por dividir los polinomios:

$$\frac{z}{w}=\frac{(7-5i)(3-4i)}{(3+4i)(3-4i)}=\frac{1-43i}{25}=(1/25)+(-2+7/25)i$$

Tomemos para $c=-2i,$ entonces

$$(7-5i)-(3+4i)(-2i)=-1+i$$

de donde

$$z=(3+4i)(-2i)+(-1+i)=7-5i$$

por lo que

$$N(-1+i)<N(3+4i)=2<25.$$

No es la única factorización de esta división euclidea, por ejemplo:

$$z=(3+4i)(-i)+(3+2i)=7-5i \text{ y } N(-i)<N(3+4i)=1<25.$$

3.5 Sean $z=20+17i,\ w=4+5i$ dos números algebraicos. Calcular la división euclidea tal que $z/w=r+si$.

Empecemos por dividir los polinomios:

$$\frac{z}{w}=\frac{20+17i}{4+5i}==(165/41)+(32/41)i$$

Tomemos para $c=4-i,$ entonces

$$(20+17i)-(4+5i)(4-i)=-1+i$$

de donde

$$z=(4+5i)(4-i)+(-1+i)=20+17i$$

por lo que

$$N(-1+i) < N(4+5i) = 2 < 41.$$

Observen que las factorizaciones de z y w son

$$z = 20+17i = (2+3i)(2+7i)(-i) = (20+17i)(17+20i)(-i) = 689$$
$$w = (4+5i)(5+4i)(-i) = 41$$

El primer polinomio admite más de una factorización, luego es reducible. El segundo polinomio sólo admite la factorización de la norma, luego es un primo irreducible. Efectivamente, el Máximo Común Divisor y la forma lineal de estos polinomios son

$$\text{El } mcd(20+17i, 4+5i) = 1 = (20+17i)(4) + (4+5i)(-16+3i)$$

que nos demuestra la presencia de un número primo en su estructura.

3.6 Sean $z = 44+5i,\ w = 33-13i$ dos números algebraicos. Calcular la división euclidea tal que $z/w = r+si$.

Excepto asociados, empecemos por factorizar los dos números algebraicos:

$$z = (1+6i)(7+2i)(-i) = 44+5i \text{ y } w = (1+i)(4+i)(6+i)(-i) = 33-13i$$

No existe ningún factor común, por tanto el Máximo Común Divisor resulta:

$$mcd(44+5i,\ 33-13i) = 1$$

En cuanto a la forma lineal, a partir de la función Identidad de Euler, tenemos

$$d = z(\pm s) + w(\pm t) = (44+5i)(4-13i) + (33-13i)(-12+12i) = 1$$

Si comparamos estos resultados con números enteros:

$$z = N(44+5i) = 1961 = 37 \cdot 53 = (6^2+1^2)(7^2+2^2)$$
$$w = N(33-13i) = 1258 = 2 \cdot 17 \cdot 37 = (1^2+1^2)(4^2+1^2)(6^2+1^2)$$

de donde

$$mcd(1961,1258) = 37 \text{ y } d = 37 = 1961(9) + 1258(-14)$$

Observemos que, mientras 1961 y 1258 no son coprimos, pues ambos son divisibles por 37, $z = 44+5i$ y $w = 33-13i$ sí son coprimos. El culpable de este desencuentro lo tiene el número $37 = 6^2+1^2 = (6+i)(6-i)$. Efectivamente, si

$$(44+5i)/(6-i) = 7+2i \ \rightarrow\ z = (6-i)(7+2i) = 44+5i$$
$$(33-13i)/(6+i) = 5-3i \ \rightarrow\ w = (6+i)(5-3i) = 33-13i$$

el primero admite como factor gaussiano a $(6-i)$ y el segundo como $(6+i)$, números distintos pero que ambos generan el conjugado 37.
La división gaussiana viene determinada como

$$\frac{z}{w}=\frac{44+5i}{33-13i}==(1387/1258)+(737/1258)i=\frac{(1+6i)(7+2i)}{(1+i)(4+i)(6+i)}$$

Para $c=1+i$, tenemos

$$(44+5i)-(33-13i)(1+i)=-2-15i$$

Como

$$N(-2-15i)<N(33-13i)=229<1258$$

resulta una descomposición euclidea de

$$z=(33-13i)(1+i)+(-2-15i)=(1+6i)(7+2i)(-i)=44+5i$$

3.7 Sean $z=86-24i,\ w=5+2i$ dos números algebraicos. Calcular la división euclidea tal que $z/w=r+si$.

La factorización de $z=86-24i$ es $z=(1+i)^2\ (12+43i)(-1)=86-24i$. En cuanto a $w=5+2i$, es un entero de Gauss, ya que $w=(5+2i)(2+5i)(-i)=29=5^2+2^2$.
En cuanto a la forma lineal

$$mcd(86-24i,5+2i)=1=(86-24i)(1)+(5+2i)(-13+10i)$$

son dos números gaussianos primos entre sí.
La división euclidea resulta

$$\frac{z}{w}=\frac{86-24i}{5+2i}==(282/29)+(292/29)i=-\frac{(1+i)^2(12+43i)}{5+2i}$$

Para $c=13-10i$, tenemos

$$z=(86-24i)-(5+2i)(13-10i)=1$$

Como

$$N(1)<N(5+2i)=1<29$$

resulta una descomposición euclidea de

$$z=(5+2i)(13-10i)+1=(1+i)^2\ (12+43i)(-1)=86-24i$$

Para $c=13-11i$, tenemos

Como

$$N(-1+5i) < N(5+2i) = 26 < 29$$

resulta una factorización euclidea de

$$z = (5+2i)(13-11i) + (-1+5i) = (1+i)^2\ (12+43i)(-1) = 86-24i$$

con lo que se demuestra que los números algebraicos propuestos no tienen un factorización única.

3.8 Sean $z = 50+13i,\ w = 4+3i$ dos números algebraicos. Calcular la división euclidea tal que $z/w = r+si$.

Tenemos que

$$\frac{z}{w} = \frac{50+13i}{4+3i} == (239/25) + (98/25)i = \frac{(1+4i)(11+6i)}{(1+2i)^2}$$

Si $c = 9-4i,\ r = 2+2i$

$$z = (4+3i)(10-4i) + (2+2i) = (1+4i)(11+6i)(-i) = 50+13i$$

con

$$N(2+2i) < N(4+3i) = 8 < 25$$

Si $c = 10-4i,\ r = -2-i$

$$z = (4+3i)(10-4i) + (-2-i) = (1+4i)(11+6i)(-i) = 50+13i$$

con

$$N(-2-i) < N(4+3i) = 5 < 25$$

Si $c = 10-4i,\ r = 2+2i$

$$z = (4+3i)(10-4i) + (2+2i) = (1+4i)(11+6i)(-i) = 50+13i$$

con

$$N(2+2i) < N(4+3i) = 8 < 25$$

13.4 Factorización euclidea con elementos del anillo $\mathbb{Q}\sqrt{D}$.

4.1 **Sean** $z=N(2+\sqrt{19}i)$ **y** $w=2+i$ **dos elementos de** $\mathbb{Q}\sqrt{D}$. **Encontrar** $c,r\in\mathbb{Z}[i]$. **tales que** $z=cw+r$ **con** $r=0$ *ó* $N(r)<N(w)$.

Sea D un número negativo libre de cuadrados. El anillo de los enteros de $\mathbb{Q}\sqrt{D}$ es un dominio euclídeo si y sólo si $D<0$ y toma los valores de

$$D=-1,-2,-3,-7,-11,-19,-43,-67,-163$$

que son cuerpos cuadráticos imaginarios con factorización única.
Si $D>0,$ serán un dominio euclídeo para valores de

$$D=2,3,5,6,7,11,13,14,17,19,21,22,23,29,31,33,37,38,41,$$
$$43,46,47,53,57,59,61,62,67,69,71,73,77,83,86,89,93,94,97$$

En estos casos, la norma euclidea es $\phi(z)=N(z)$.

Los enteros algebraicos $z=a+b\sqrt{D}$ con $a,b\in Z$ del cuerpo $\mathbb{Q}\sqrt{D}$ son de la forma

$$\begin{cases} a+b\sqrt{D} & si\ \ D\equiv 2,3(mód.4) \\ a+b\dfrac{(1+\sqrt{D})}{2} & \text{si}\ \ \mathrm{D}\equiv 1(mód.4) \end{cases}$$

con $a,b\in\mathbb{Z}$.
El entero algebraico es raíz del polinomio $x^2+bx+c\in\mathbb{Z}[x]$.
El valor de la norma es $z=N(2+\sqrt{19}i)=(2+\sqrt{19}i)(2-\sqrt{19}i)=23.$ Ahora procedemos a la división euclidea.

$$\frac{z}{w}=\frac{23}{2+i}=(46/5-23/5i)\simeq(9,2-4,6i)$$

Para $c=9-4i$

$$23-(2+i)(9-4i)=1-i$$

Como $N(1-i)<N(2+i)=2<5,$ entonces

$$z=(2+i)(9-4i)+(1-i)=23=N(2+\sqrt{19}i)$$

Para $c=9-6i$

$$z=(2+i)(9-6i)+(-1+3i)=23=N(2+\sqrt{19}i)$$

Pero $N(-1+3i)>N(2+i)=10>5,$ luego $r=-1+3i$ no es un elemento del anillo euclídeo.

Para $c=9-5i$

$$23-(2+i)(9-5i)=i$$

Como $N(i)<N(2+i)=1<5,$ entonces

$$z=(2+i)(9-5i)+(i)=23=N(2+\sqrt{19}i)$$

Lo que demuestra la factorización no única en el anillo euclídeo.

4.2 **Sean** $z=N(6-\sqrt{7}i)$ **y** $w=2-3i$ **dos elementos de** $\mathbb{Q}\sqrt{D}$. **Encontrar** $c,r\in\mathbb{Z}[i].$ **tales que** $z=cw+r$ **con** $r=0$ *ó* $N(r)<N(w).$

La norma tiene como valor $N(6-\sqrt{7}i)=(6-\sqrt{-7})(6+\sqrt{-7})=43$ y el polinomio que la genera es x^2 -$12x+43=0.$
La factorización de este polinomio resulta

$$x^2\text{-}12x+43=x(-12)x+43=(x-6)^2+7$$

por lo que la solución es

$$x=6\pm\sqrt{7}i$$

Para la división euclidea, tenemos

$$\frac{z}{w}=\frac{43}{2-3i}=(86/13+129/13i)\simeq(6,61+9,92i)$$

Si damos a $c=6+10i,$ obtenemos para r

$$r=43-(2-3i)(6+10i)=1-2i$$

por lo que el valor de w queda desglosado en

$$w=(2-3i)(6+10i)+(1-2i)=43=N(6-\sqrt{7}i)$$

ya que $N(1-2i)<N(2-3i)=5<13.$
Pero, sabemos que

$$w=N(6-\sqrt{7}i)=x^2-12+43$$

o lo que es lo mismo

$$w=(2-3i)(6+10i)+(1-2i)=x^2-12x+43=43$$

Si hacemos operaciones

$$\begin{aligned} 43 &= x^2 - 12x + 43 \\ &= (x-12)x + 43 \end{aligned}$$

de donde

$$12x - x^2 = 0 = 36 - (x-6)^2$$

por lo que

$$x = 0,12$$

son las soluciones enteras de $w = N(6-\sqrt{7}i) = x^2 - 12 + 43.$

4.3 **Sean** $z = N(9-2\sqrt{11})$ **y** $w = 4-3i$ **dos elementos de** $\mathbb{Q}\sqrt{D}$. **Encontrar** $c, r \in \mathbb{Z}[i]$. **tales que** $z = cw + r$ **con** $r = 0$ *ó* $N(r) < N(w).$

El valor de la norma es $z = N(9+2\sqrt{11}) = 37$ que es generada por el polinomio x^2 -$18x + 37 = 0.$ La factorización de este polinomio es

$$x^2 - 18x + 37 = (x-18)x + 37 = (x-9)^2 - 44$$

de donde, sus raíces resultan $x = 9 \pm 2\sqrt{11}.$
Para la división euclidea

$$\frac{z}{w} = \frac{37}{4-2i} = \frac{(6+i)(1+6i)(-i)}{(1+i)^2(1+2i)(-1)} = (37/5 + 37/10i) \simeq (7,4 + 3,7i)$$

Si tomamos para $c = 7+4i,$ obtenemos para r

$$r = 37 - (4-2i)(7+4i) = 1-2i$$

de donde

$$z = (4-2i)(7+4i) + (1-2i) = 37 = N(9-2\sqrt{11}) = x^2 - 18x + 37$$

ya que $N(1-2i) < N(4-2i) = 5 < 20.$
Como

$$(4-2i)(7+4i) + (1-2i) = x^2 - 18x + 37$$

haciendo operaciones, tenemos

$$\begin{aligned} 37 &= x^2 - 18x + 37 = (x-18)x + 37 \\ 81 - (x-9)^2 &= 0 = 18x - x^2 \end{aligned}$$

por lo que $x = 0{,}18$.
Observar que en esta comparación entre el polinomio y su descomposición en división euclidea, las raíces son 0 y b.

4.4 **Sean** $z = N(15 - 2\sqrt{29})$ **y** $w = 7 + 3i$ **dos elementos de** $\mathbb{Q}\sqrt{D}$. **Encontrar** $c, r \in \mathbb{Z}[i]$. **tales que** $z = cw + r$ **con** $r = 0$ *ó* $N(r) < N(w)$.

La norma genera 109 como número entero y un polinomio de $x^2 - 30x + 109 = 0$ que tiene como raíces $x = 15 \pm 2\sqrt{29}$, un conjugado real.
Para la división euclidea, tenemos

$$\frac{z}{w} = \frac{109}{7+3i} = \frac{(10+3i)(3+10i)(-i)}{(1+i)(2+5i)(-i)} = (763/58 - 327/58i) \simeq (13{,}16 - 5{,}64i)$$

Para $c = 13 - 5i$ *ó* $13 - 6i$ genera para $r = 3 - 4i$ *ó* $3i$.

$$z = (7+3i)(13-5i) + (3-4i) = 109 = x^2 - 30x + 109$$
$$z = (7+3i)(13-6i) + (3i) = 109 = x^2 - 30x + 109$$

ya que

$$N(3-4i) < N(7+3i) = 25 < 58$$
$$N(3i) < N(7+3i) = 3 < 58$$

Se pueden encontrar otras representaciones, dado el margen existente de las normas.

4.5 **Sean** $z = N\left(\frac{7 + \sqrt{195}i}{2}\right)$ **y** $w = 5 - 4i$ **dos elementos de** $\mathbb{Q}\sqrt{D}$. **Encontrar** $c, r \in \mathbb{Z}[i]$. **tales que** $z = cw + r$ **con** $r = 0$ *ó* $N(r) < N(w)$.

El valor de la norma es $z = N\left(\frac{7 + \sqrt{195}i}{2}\right) = \left(\frac{7 + \sqrt{195}i}{2}\right)\left(\frac{7 - \sqrt{195}i}{2}\right) = 61$ y la ecuación que la genera es $x^2 - 7x + 61 = 0$, que tiene como raíces $x = \frac{7 \pm \sqrt{195}i}{2}$.
La división euclidea resulta

$$\frac{z}{w} = \frac{61}{5-4i} = \frac{(6+5i)(5+6i)(-i)}{(4+5i)(-i)} = (305/41 - 244/41i) \simeq (7{,}44 + 5{,}95i)$$

Para $c = 7 + 6i$ y $r = 2 - 2i = -(1+i)^3$, obtenemos

$$z = (5-4i)(7+6i) + (2-2i) = 61 = x^2 - 7x + 61$$

Como $61 = x^2 - 7x + 61$, operando

$$\frac{49}{4}-\left(x-\frac{7}{2}\right)^2=0=7x-x^2$$

de donde $x=0,7.$

4.6 Sean $z=N\left(\frac{10-4\sqrt{18}i}{2}\right)$ **y** $w=2-8i$ **dos elementos de** $\mathbb{Q}\sqrt{D}.$ **Encontrar** $c,r\in\mathbb{Z}[i].$ **tales que** $z=cw+r$ **con** $r=0$ *ó* $N(r)<N(w).$

El valor de esta norma es $z=N\left(\frac{10-4\sqrt{18}i}{2}\right)=\left(\frac{10+4\sqrt{18}i}{2}\right)\left(\frac{10-4\sqrt{18}i}{2}\right)=97$ y el polinomio generado es $x^2-10x+97=0$ con solución $x=5\pm 6\sqrt{2}i.$
Observen que el discriminante se ha modificado. Ha pasado de -18 a $-2.$ También ha cambiado el denominador $2.$ Todo esto es debido a que 10 y 4 son divisibles por 2 y, por tanto $z=N(5+2\sqrt{-18})=(5+2\sqrt{18}i)(5-2\sqrt{18}i)=97$ generando el mismo polinomio con la misma solución. Pero el discriminante se modifica por no ser libre de cuadrados, a saber

$$D=b^2-4ac=10^2-4\cdot 97=-288=-2^2\cdot 72\ \rightarrow\ \Delta=-2$$

Esto ha sido debido a que 10 y 4 son números asociados.
Procedemos a la división euclidea.

$$\frac{z}{w}=\frac{97}{2-8i}=\frac{(9+4i)(4+9i)(-i)}{(1+i)^2(4+i)(-1)}=(97/34-194/17i)\simeq(2{,}85+11{,}41i)$$

Para $c=3+11i,\ r=3+2i.$ Con $N(3+2i)<N(2-8i)=13<68.$
El valor de z resulta

$$z=(2-8i)(3+11i)+(3+2i)=97=N\left(\frac{10-4\sqrt{18}i}{2}\right)=x^2-10x+97$$

Los ceros de este polinomio se determinan para $x=0,10.$

13.5 Factorización única en los cuerpos cuadráticos $K=\mathbb{Q}(\sqrt{D}).$

5.1 Definición de los cuerpos cuadráticos.

Sea $K=Q(\alpha)$ un cuerpo cuadrático donde α es un entero algebraico y raíz de un polinomio $x^2+bx+c\in Z[x].$ Sea $\alpha=\frac{-b\pm\sqrt{b^2-4ac}}{2}$ y $K=Q\sqrt{b^2-4c}.$ Podemos establecer que $b^2-4ac=m^2d,$ donde d es libre de cuadrados, y así $K=Q\left(m\sqrt{d}\right)=Q\left(\sqrt{d}\right).$ Tenemos pues que todo cuerpo cuadrático es de la forma $K=Q\left(\sqrt{d}\right)=\left\{a+b\sqrt{d}:\ a,b\in\mathbb{Q}\right\}$ donde d es un

entero libre de cuadrados, $d \neq 1$. Si $\mathcal{O} = \left\{ x = a + b\sqrt{d} \,:\, x^2 - sx + p = 0,\ s, p \in \mathbb{Z} \right\}$. Si $x \in \mathcal{O}$ y $\mathcal{O}k = \mathbb{Z}[\omega]$ es el anillo de $K = \mathbb{Q}\sqrt{D}$, entonces

$$\omega = \sqrt{D} \ si\ D \not\equiv 1(mód.4) \text{ y } \omega = \frac{D + \sqrt{D}}{2} \ si\ D \equiv 1(mód.4)$$

Como $\frac{D + \sqrt{D}}{2} \in \mathcal{O}k$ es raíz del polinomio $x^2 - Dx + \frac{D(D-1)}{4} \in \mathbb{Z}[x]$, se satisface que

$$\mathcal{O}k = \mathbb{Z}\left[\frac{D + \sqrt{D}}{2} \right]$$

Como en el polinomio mínimo $\left(\sqrt{d}, Q\right) = x^2 - d = \left(x + \sqrt{d}\right)\left(x - \sqrt{d}\right)$ resulta que los elementos de K son de la forma $a + b\sqrt{d}$, donde $a, b \in Q$, la extensión K/Q es una extensión de Galois y sus automorfismos son la identidad y el determinado por $\sigma\left(\sqrt{d}\right) = -\sqrt{d}$. A este automorfismo le llamaremos simplemente conjugado de K, y lo representaremos como una norma, donde

$N\left(a + b\sqrt{-D}\right) = a^2 + Db^2$, si es un cuerpo cuadrático imaginario ó
$N\left(a + b\sqrt{D}\right) = a^2 - Db^2$, si es un cuerpo cuadrático real

Así, la diferencia entre un cuerpo cuadrático imaginario o complejo y un cuerpo cuadrático real es que, el discriminante del primero es negativo y el del segundo positivo. Cuando $D < 0$ hay una cantidad finita de valores de a y b, si $D > 0$, los valores de a y b son infinitos.
La suma y diferencia de los dos números algebraicos se obtienen como

$\left(a + b\sqrt{\pm D}\right) + \left(a - b\sqrt{\pm D}\right) = 2a$, como suma de los dos números algebraicos.
$\left((a + b\sqrt{\pm D}) - (a - b\sqrt{\pm D})\right) \Big/ (\sqrt{\pm D})$ como diferencia de los dos números algebraicos.

5.2 Demostrar la relación existente entre $x^2 - 6x + 29$ y $N(a + b\sqrt{5}i) = 29.$

La factorización del polinomio es

$$x^2 - 6x + 29 = (x - 6)x + 29 = (x - 3)^2 + 20$$

con una solución conjugada de $x = 3 \pm 2\sqrt{5}i.$
Sea $N(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = x^2 + 5y^2 = 29.$ Sea $(a + b\sqrt{-5}) + (a - b\sqrt{-5}) = 2a.$
Por la factorización del polinomio sabemos que $b = 2$ y $6 = 2a = 2 \cdot 3$, por tanto

$$N(3 + 2\sqrt{-5}) = (3 + 2\sqrt{-5})(3 - 2\sqrt{-5}) = 3^2 + 5^2 = 29$$

La demostración de que esto es cierto es que

$$D = b^2 - 4ac = 6^2 - 4 \cdot 29 = -80 = -5 \cdot 4^2 \ \rightarrow \ \Delta = -5$$

y, por tanto

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{6 \pm \sqrt{6^2 - 4 \cdot 29}}{2} = \frac{6 \pm \sqrt{-80}}{2} = \frac{6 \pm 4\sqrt{-5}}{2} = 3 \pm 2\sqrt{5}i$$

5.3 Factorizar $z = N(a + b\sqrt{\pm 5}) = 6$ y generar el polinomio mínimo.

Los factores $2\ y\ 3$ son irreducibles en $z = a + bi$ con $z \in \mathbb{Z}[i]$ y $a, b \in \mathbb{Q}$ ya que, como $-5 \not\equiv 1(mód.4)$, el anillo de enteros de $\mathbb{Q}\sqrt{-5}$ es $\mathbb{Z}\left[\sqrt{-5}\right]$.

Supongamos que $1 + \sqrt{-5} = (a + b\sqrt{-5})(c - d\sqrt{-5})$, para $a, b, c, d \in \mathbb{Z}$, entonces

$$6 = (a^2 + 5b^2) = (c^2 + 5d^2)$$

Si $a^2 + 5b^2$ es un número no negativo, $a^2 + 5b^2 = 1, 2, 3\ ó\ 6.$

Para $N(1 + \sqrt{-5}) = 1^2 + 5 \cdot 1^2$. Como $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$ y $(1 + \sqrt{-5}) + (1 - \sqrt{-5}) = 2$, la ecuación generada es $x^2 - 2x + 6 = 0$, con solución $x = 1 \pm \sqrt{5}i$. Podemos probarlo mediante

$$D = b^2 - 4ac = 2^2 - 4 \cdot 1 \cdot 6 = -20 = -2^2 5 \ \rightarrow \ \Delta = -5$$

donde D es libre de cuadrados.

Para $N(2 + \sqrt{-2}) = 2^2 + 2 \cdot 1^2$. Como $(2 + \sqrt{-2})(2 - \sqrt{-2}) = 6$ y $(2 + \sqrt{-2}) + (2 - 2\sqrt{-2}) = 4$, la ecuación generada es $x^2 - 4x + 6 = 0$, con solución $x = 2 \pm \sqrt{2}i$. Podemos probarlo mediante

$$D = b^2 - 4ac = 4^2 - 4 \cdot 1 \cdot 6 = -8 = -2^2 2 \ \rightarrow \ \Delta = -2$$

donde D es libre de cuadrados.

Para $N(3 + \sqrt{3}) = 3^2 - 3 \cdot 1^2$. Como $(3 + \sqrt{3})(3 - \sqrt{3}) = 6$ y $(3 + \sqrt{3}) + (3 - \sqrt{3}) = 6$, la ecuación generada es $x^2 - 6x + 6 = 0$, con solución $x = 3 \pm \sqrt{3}$. Podemos probarlo mediante

$$D = b^2 - 4ac = 6^2 - 4 \cdot 1 \cdot 6 = 12 = 2^2 3 \ \rightarrow \ \Delta = 3$$

donde D es libre de cuadrados.

Para $N(5 + \sqrt{19}) = 5^2 - 19 \cdot 1^2$. Como $(5 + \sqrt{19})(5 - \sqrt{19}) = 6$ y $(5 + \sqrt{19}) + (5 - \sqrt{19}) = 10$, la ecuación generada es $x^2 - 10x + 6 = 0$, con solución $x = 5 \pm \sqrt{19}$. Podemos probarlo mediante

$$D = b^2 - 4ac = 10^2 - 4 \cdot 1 \cdot 6 = 76 = 2^2 19 \ \rightarrow \ \Delta = 19$$

donde D es libre de cuadrados.

Hemos demostrado las representaciones cuadráticas limitadas de 6 en el campo complejo e ilimitadas en el campo real.

Ahora, supongamos que

$$N(3+\sqrt{6}) = (3+\sqrt{6})(3-\sqrt{6}) = 3$$
$$N(2+\sqrt{6}) = -(2+\sqrt{6})(2-\sqrt{6}) = 2$$
$$N(3-\sqrt{6}) = (3-\sqrt{6})(2+\sqrt{6}) = \sqrt{6}$$

Si

$$(2+\sqrt{6})/(3-\sqrt{6}) = (5+2\sqrt{6}) = p_1$$
$$(2+\sqrt{6})/(2-\sqrt{6}) = (-5-2\sqrt{6}) = p_2$$

entonces

$$3 = (3-\sqrt{6})^2 p_1 = (3-\sqrt{6})^2(5+2\sqrt{6})$$
$$2 = -(2-\sqrt{6})^2 p_2 = -(2-\sqrt{6})^2(-5-2\sqrt{6})$$
$$\sqrt{6} = (3-\sqrt{6})(2-\sqrt{6})\,p_2 = (3-\sqrt{6})(2-\sqrt{6})(-5-2\sqrt{6}$$

de donde

$$6 = (3+\sqrt{6})(3-\sqrt{6})(2+\sqrt{6})(2-\sqrt{6})(-1)$$

Otra factorización la encontramos en

$$(\sqrt{6})^2 \cdot 3 \cdot (1+i)^2(-i) = 1^2 + 1^2 + 2^2 = 6 = 2 \cdot 3$$

5.4 **Factorizar** $N(a+b\sqrt{3}) = 2,\ N(a+b\sqrt{3}) = 11,\ N(a+b\sqrt{3}) = 22\ y\ N(a+b\sqrt{3}) = 33,$ teniendo en cuenta que $\mathbb{Q}\sqrt{3}.$

Si p, q son dos números primos, entonces para $\mathbb{Q}\left(\sqrt{-pq}\right),\ -pq = \sqrt{-pq}\sqrt{-pq} = -(p)(q)$ que representa la factorización irreducible de dos números algebraicos. En el mismo caso se encuentra para $\mathbb{Q}\left(\sqrt{pq}\right)$, donde $pq = \sqrt{pq}\sqrt{pq} = -(p)(q).$

Para $N(a+b\sqrt{3}) = 2,$ admite como solución $2 = (1+\sqrt{3})(1-\sqrt{3})(-1).$ Teniendo en cuenta que $\sqrt{2}\sqrt{2} = 2,$ resulta que $2 = (1+\sqrt{3})(1-\sqrt{3})(-1) = \sqrt{2}\sqrt{2}.$

Para $N(a+b\sqrt{3}) = 11,$ admite como solución $11 = (4+3\sqrt{3})(4-3\sqrt{3})(-1).$ Si tenemos en cuenta que $\sqrt{11}\sqrt{11} = 11,$ tenemos que $11 = (4+3\sqrt{3})(4-3\sqrt{3})(-1) = \sqrt{11}\sqrt{11}.$

Para $N(a+b\sqrt{3}) = 22,$ admite como solución $22 = (7+3\sqrt{3})(7-3\sqrt{3}).$ Si tenemos en cuenta que $\sqrt{2\cdot 11}\sqrt{2\cdot 11} = 22,$ obtenemos $22 = (7+3\sqrt{3})(7-3\sqrt{3}) = \sqrt{2\cdot 11}\sqrt{2\cdot 11}.$

Para $N(a+b\sqrt{3}) = 33,$ admite como solución $33 = (6+\sqrt{3})(6-\sqrt{3}).$ Si tenemos en cuenta que $\sqrt{3\cdot 11}\sqrt{3\cdot 11} = 33,$ obtenemos $33 = (6+\sqrt{3})(6-\sqrt{3}) = \sqrt{3\cdot 11}\sqrt{3\cdot 11}.$

5.5 Sean $z=1+2\sqrt{-5}$ y $w=2+\sqrt{-5}$ dos números algebraicos. Demostrar que no tienen factorización única.

Los valores de las normas de los dos algebraicos son

$$z=N(1+2\sqrt{-5})=21 \text{ y } w=N(2+\sqrt{-5})=9$$

Sea

$$\frac{z^2}{w}=(1+2\sqrt{-5})^2/(2+\sqrt{-5})=-2+3\sqrt{-5} \text{ y } \frac{9}{w}=9/(2+\sqrt{-5})=2-\sqrt{-5}$$

Los números algebraicos generados pertenecen al anillo $\mathbb{Q}\sqrt{-5},$ mientras que $\sqrt{z}\in\mathbb{Z}.$
Como $\sqrt{w}=\sqrt{2+\sqrt{-5}}$

$$\sqrt{w}=\left(-\frac{2\left(1+2\sqrt{-5}\right)}{\sqrt{\left(2+\sqrt{-5}\right)}}\right)\left(1+2\sqrt{-5}\right)-\left(\frac{12-3\sqrt{-5}}{\sqrt{\left(2+\sqrt{-5}\right)}}\right)3=\sqrt{2+\sqrt{-5}}$$

Similarmente para $7,$ obtenemos $\sqrt{k}$ donde $k=2+3\sqrt{-5}.$
Con simples operaciones encontramos
Como $N(2+3\sqrt{-5})=49$ y $N(2+\sqrt{-5})=9,$ obtenemos

$$3=\sqrt{-w}\sqrt{-w'}=\sqrt{2+\sqrt{-5}}\sqrt{2-\sqrt{-5}}$$
$$7=\sqrt{-k}\sqrt{-k'}=\sqrt{2+3\sqrt{-5}}\sqrt{2-3\sqrt{-5}}$$

de donde

$$21=\sqrt{-w}\sqrt{-w'}\sqrt{-k}\sqrt{-k'}=\sqrt{2+\sqrt{-5}}\sqrt{2-\sqrt{-5}}\sqrt{2+3\sqrt{-5}}\sqrt{2-3\sqrt{-5}}=3\cdot 7$$

Ya sabemos que $21=(1+2\sqrt{-5})(1-2\sqrt{-5}).$ Consideremos ahora el campo $\mathbb{Q}[\omega]$ donde $\omega=\frac{-1+\sqrt{-3}}{2}$ es una raíz del polinomio $P_{(x)}=x^2+x+1,$ entonces $[\mathbb{Q}(\omega):\mathbb{Q}]=2.$ El determinante de la siguiente matriz nos revela que

$$\Delta(1,\omega)=\begin{vmatrix} 1 & 1 \\ \frac{(-1+\sqrt{-3})}{2} & \frac{(-1-\sqrt{-3})}{2} \end{vmatrix}^2=(-i\sqrt{-3})^2=3$$

lo que nos lleva a que si $(1+\sqrt{-6})(1\sqrt{-6})=7,$ obtenemos otra factorización de 21

$$21=(-i\sqrt{-3})^2(1+\sqrt{-6})(1-\sqrt{-6})=3\cdot 7$$

5.6 Factorizar $z = N(a+b\sqrt{-D}) = 21$ y generar los polinomios mínimos correspondientes.

Los cuerpos cuadráticos correspondientes a $\mathbb{Q}\sqrt{-D} = 2,3,5,6,7,13,17,21,29,\ldots$ son dominios euclídeos con el valor absoluto de la norma, esto es $\phi(a) = N(a)$. Como se trata de cuerpos cuadráticos imaginarios, los valores de D deben ser $D \le \sqrt{21},$ esto es

$$21-1^2 = 20 = 2^2 5;\ \ 21-2^2 = 17;\ \ 21-3^2 = 12 = 2^2 3;\ \ 21-4^2 = 5$$

Para $N(1+2\sqrt{-5}) = 1^2 + 5\cdot 2^2 = 21.$

Si $p = (1+2\sqrt{-5})(1-2\sqrt{-5}) = 21$ y $s = (1+2\sqrt{-5}) + (1-2\sqrt{-5}) = 2,$ el polinomio mínimo $f(x) = x^2 - sx + p$ resulta $x^2 - 2x + 21 = 0,$ con $x = 1 \pm 2\sqrt{5}i.$

Para $N(1+2\sqrt{-5}) = 1^2 + 5\cdot 2^2 = 21.$

Si $p = (2+\sqrt{-17})(2-\sqrt{-17}) = 21$ y $s = (2+\sqrt{-17}) + (2-\sqrt{-17}) = 4,$ el polinomio mínimo $f(x) = x^2 - sx + p$ resulta $x^2 - 4x + 21 = 0,$ con $x = 2 \pm \sqrt{17}i.$

Si $p = (3+2\sqrt{-3})(3-2\sqrt{-3}) = 21$ y $s = (3+2\sqrt{-3}) + (3-2\sqrt{-3}) = 6,$ el polinomio mínimo $f(x) = x^2 - sx + p$ resulta $x^2 - 6x + 21 = 0,$ con $x = 3 \pm 2\sqrt{3}i.$

Si $p = (4+\sqrt{-5})(4-\sqrt{-5}) = 21$ y $s = (4+\sqrt{-5}) + (4-\sqrt{-5}) = 8,$ el polinomio mínimo $f(x) = x^2 - sx + p$ resulta $x^2 - 8x + 21 = 0,$ con $x = 4 \pm \sqrt{5}i.$

5.7 Factorizar $z = N(a+b\sqrt{D}) = a^2 - Db^2 = 2^3$ y generar los polinomios mínimos correspondientes.

Sea $N(5+\sqrt{17}) = 5^2 - 17\cdot 1^2 = 8,$ donde $a+b = (5+\sqrt{17}) + (5-\sqrt{17}) = 10$ y $ab = 8.$ La ecuación generada es $x^2 - 10x + 8 = 0,$ con $x = 5 \pm \sqrt{17}.$ Podemos comprobar que

$$D = b^2 - 4ac = 10^2 - 4\cdot 8 = 68 = 2^2 \cdot 17,\ \text{con}\ \Delta = 17,$$

libre de cuadrados.

Sea $N(1+\sqrt{-7}) = 1^2 + 7\cdot 1^2 = 8,$ donde $a+b = (1+\sqrt{-7}) + (1-\sqrt{-7}) = 2$ y $ab = 8.$ La ecuación generada es $x^2 - 2x + 8 = 0,$ con $x = 1 \pm \sqrt{7}i.$ Podemos comprobar que

$$D = b^2 - 4ac = 2^2 - 4\cdot 8 = -28 = -2^2 \cdot 7,\ \text{con}\ \Delta = -7,$$

libre de cuadrados.

Sea $N(4+2\sqrt{2}) = 4^2 - 2\cdot 2^2 = 8,$ donde $a+b = (4+2\sqrt{2}) + (4-2\sqrt{2}) = 8$ y $ab = 8.$ Ahora bien, el $mcd(4,2) = 2,$ entonces $(2+\sqrt{2})(2-\sqrt{2}) = 2,$ y por tanto

$$\left[(2+\sqrt{2})(2-\sqrt{2})\right]^3=8$$

esto nos lleva a un polinomio mínimo de $x^2-x+2=0,$ con $x=\dfrac{1\pm\sqrt{7}i}{2}$ y una norma de

$$N\left(\frac{1+\sqrt{-7}}{2}\right)=2$$

Sea $N(10+2\sqrt{23})=10^2-23\cdot 2^2=8,$ donde $a+b=(10+2+\sqrt{23})+(10-2\sqrt{23})=20$ y $ab=8.$
Pero, el $mcd(10,2)=2,$ entonces $(5+\sqrt{23})(5-\sqrt{23})=2$ y el polinomio mínimo generado es $x^2-10x+2=0,$ con $x=5\pm\sqrt{23}.$
Como $(5+\sqrt{23})(5-\sqrt{23})=2$ y $\left[(5+\sqrt{23})(5-\sqrt{23})\right]^3=8,$ tenemos como factorización de 8

$$8=\left[(2+\sqrt{2})(2-\sqrt{2})\right]^3=\left[(5+\sqrt{23})(5-\sqrt{23})\right]^3=2^3$$

En la obra de los profesores Alaca y Willians, Introductory Algebraic Number Theory, encontramos la siguiente solución:

Sea $\alpha=(5+\sqrt{17})^{1/3}+(5-\sqrt{17})^{1/3}\in\mathbb{R},$ entonces

$$\begin{aligned}\alpha^3&=(5+\sqrt{17})+3(5+\sqrt{17})^{2/3}(5-\sqrt{17})^{1/3}+3(5+\sqrt{17})^{1/3}(5-\sqrt{17})^{2/3}+(5-\sqrt{17})\\&=10+3(5+\sqrt{17})^{1/3}(5-\sqrt{17})^{1/3}((5-\sqrt{17})^{1/3})+(5-\sqrt{17})^{1/3}\\&=10+3((5+\sqrt{17})(5-\sqrt{17}))^{1/3}\alpha\\&=10+8^{1/3}\alpha\\&=10+6\alpha\end{aligned}$$

por lo que α es una raíz del polinomio mónico $x^3-6x-10\in\mathbb{Z}[x].$ Por lo tanto α es un número entero algebraico.
La solución algebraica de la ecuación es

$$x_1=\frac{2\left(\dfrac{\sqrt{3}\,i}{2}-\dfrac{1}{2}\right)}{\left(\sqrt{17}+5\right)^{\frac{1}{3}}}+\left(\sqrt{17}+5\right)^{\frac{1}{3}}\left(-\frac{\sqrt{3}\,i}{2}-\frac{1}{2}\right),$$

$$x_2=\left(\sqrt{17}+5\right)^{\frac{1}{3}}\left(\frac{\sqrt{3}\,i}{2}-\frac{1}{2}\right)+\frac{2\left(-\dfrac{\sqrt{3}\,i}{2}-\dfrac{1}{2}\right)}{\left(\sqrt{17}+5\right)^{\frac{1}{3}}},\quad x_3=\left(\sqrt{17}+5\right)^{\frac{1}{3}}+\frac{2}{\left(\sqrt{17}+5\right)^{\frac{1}{3}}}$$

Como $\left[(5+\sqrt{17})(5-\sqrt{17})\right]^{1/3}=2,$ la factorización de 8 es

$$(5+\sqrt{17})(5-\sqrt{17})=8$$

Solución que es coincidente con la forma cuadrática.

13.6 Factorización polinomio ciclotómico.

6.1 Polinomio ciclotómico: definición

Se llama polinomio ciclotómico de índice n a $\Phi_n(z)=(z-p_1)(z-p_2)\cdot\ldots\cdot(z-p_k)$, donde $p_1, p_2, \ldots, p_k$ son las k raíces primitivas *n-ésimas* de la unidad en el cuerpo de los números complejos, siendo $k=\varphi(n)$ la función de Euler. Los polinomios Φ_n tienen sus coeficientes en $\mathbb{Z}$, son irreductibles sobre $\mathbb{Q}$ y verifican que $z^n-1=\prod_{d/n}\Phi_n(z)$. Estos polinomios deben su nombre al problema de la división del círculo en n partes iguales que equivale a la resolución de la ecuación $\Phi_n(z)=0$. Las fórmulas siguientes representan la factorización del polinomio z^n-1 en sus factores irreducibles

$$z^1-1=z-1$$
$$z^2-1=(z-1)(z+1)$$
$$z^3-1=(z-1)(z^2+z+1)$$
$$z^4-1=(z-1)(z+1)(z^2+1)$$
$$z^5-1=(z-1)(z^4+z^3+z+1)$$
$$z^6-1=(z-1)(z+1)(z^2+z+1)(z^2-z+1)$$
$$z^7-1=(z-1)(z^6+z^5+z^4+z^3+z^2+z+1)$$
$$z^8-1=(z-1)(z+1)(z^2+1)(z^4+1)$$
$$z^9-1=(z-1)(z^2+z+1)(z^6+z^3+1)$$
$$z^{10}-1=(z-1)(z+1)(z^4-z^3+z^2-z+1)(z^4+z^3+z^2+z+1)$$

Mediante la inversión de la función de Möbius podemos obtener los polinomios ciclotómicos mediante la fórmula

$$\Phi_n(z)=\prod_{d|n}(z^{n/d}-1)^{\mu(d)}$$

donde μ es la función de Möbius definida como

$$\mu(d)=\begin{cases}0 & \text{si d es divisible por } p^2 \text{ para algun primo p}\\ (-1)^r & \text{si d es producto de r primos distintos}\\ 1 & \text{si d =1}\end{cases}$$

Así, los primeros polinomios ciclotómicos son

$$\Phi_1(z) = z - 1$$
$$\Phi_2(z) = (z^2 - 1)(z-1)^{-1} = z + 1$$
$$\Phi_3(z) = (z^3 - 1)(z-1)^{-1} = z^2 + z + 1$$
$$\Phi_4(z) = (z^4 - z)(z^2 - 1)^{-1} = z^2 + 1$$
$$\Phi_5(z) = (z^5 - 1)(z-1)^{-1} = z^4 + z^3 + z^2 + z + 1$$
$$\Phi_6(z) = (z^6 - 1)(z^3 - 1)^{-1}(z^2 - 1)^{-1}(z-1) = z^2 - z + 1$$
$$\Phi_7(z) = (z^7 - 1)((z-1)^{-1} = z^6 + z^5 + z^4 + z^3 + z^2 + z + 1$$
$$\Phi_8(z) = (z^8 - 1)(z^4 - 1)^{-1} = z^4 + 1$$
$$\Phi_9(z) = (z^9 - 1)(z^3 - 1)^{-1} = z^6 + z^3 + 1$$
$$\Phi_{10}(z) = z^{10} - 1)(z^5 - 1)^{-1}(z+1)^{-1} = z^4 - z^3 + z^2 - z + 1$$

En las siguientes tablas se recogen valores para las funciones de Euler y Möbius:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0	-1	1	1	0	-1	0	-1	0

El cuerpo ciclotómico de índice n es un cuerpo de dislocación del polinomio ciclotómico Φ_n. Se le denota Q_n ó $Q(\omega_n)$ con ω_n raíz primitiva *n-ésima* de 1 en $\mathbb{C}$, siendo $[Q_n : Q] = \varphi(n)$.
Si $z^n = 1,$ con $(n = 1,2,3,...),$ son las raíces n-ésimas de la unidad, la solución compleja viene determinada por $e^{2\pi ik/n}$, con $(k = 0,1,2,...,n-1),$ dónde k y n son coprimos. El número de raíces primitivas diferentes viene determinado por la función de Euler $\varphi(n)$. Si n es primo, entonces todas las raíces n-ésimas de la unidad son, excepto 1, son primitivas, y tenemos

$$\Phi n(z) = \frac{z^n - 1}{z - 1} = \sum_{k=0}^{n-1} z^k$$

De hecho, por el teorema de Moivre, para la ecuación $z^n - 1 = 0,$ las raíces n-ésimas de la unidad son

$$1,\ e^{2\pi i/n},\ e^{4\pi i/n},\ e^{6\pi i/n},\ ...,\ e^{2(n-1)\pi i/n}$$

cuya suma resulta

$$1 + e^{2\pi i/n} + e^{4\pi i/n} + e^{6\pi i/n} + ... + e^{2(n-1)\pi i/n} = 0$$

6.2 Factorizar los polinomios z^{2n} -1 *con* $n \le 8$ *y* $z^{3n} - 1$ *con* $n \le 5.$

A partir de la fórmula $\Phi_n(z) = \prod_{d|n} (z^{n/d} - 1)^{\mu(d)}$ vamos a factorizar alguno de los polinomios propuestos.

Para $\Phi_6(z)=\prod_{d|n}(z^{6/d}-1)^{\mu(d)}$, tenemos

$$\begin{aligned}\Phi_6(z)&=(z^6-1)^{\mu(1)}(z^3-1)^{\mu(2)}(z^2-1)^{\mu(3)}(z^1-1)^{\mu(6)}\\&=(z^6-1)^1(z^3-1)^{-1}(z^2-1)^1=z^2-z+1\end{aligned}$$

o bien

$$z^6-1=\frac{(z^6-1)(z-1)}{(z^3-1)(z^2-1)}=\frac{(z^6-1)}{(z-1)(z+1)(z^2+z+1)}=z^2-z+1$$

Para $\Phi_{12}(z)=\prod_{d|n}(z^{12/d}-1)^{\mu(d)}$, tenemos

$$\Phi_{12}(z)=\frac{z^{12}-1}{(\varphi_1\varphi_2\varphi_3\varphi_6)\varphi_4}=\frac{z^{12}-1}{(z^6-1)(z^2+1)}=\frac{z^6+1}{z^2+1}=z^4-z^2+1$$

o bien

$$z^{12}-1=\frac{(z^{12}-1)}{(z^6-1)(z^2+1)}=\frac{z^6+1}{z^2+1}=z^4-z^2+1$$

Para $\Phi_{14}(z)=\prod_{d|n}(z^{14/d}-1)^{\mu(d)}$, tenemos

$$\Phi_{14}(z)=\frac{z^{12}-1}{(\varphi_1\varphi_7)\varphi_2}=\frac{z^{14}-1}{(z^7-1)(z+1)}=\frac{z^7+1}{z+1}=z^6-z^5+z^4-z^3+z^2-z+1$$

o bien

$$z^{14}-1=\frac{z^{14}-1}{\left(z^7-1\right)(z+1)}=\frac{z^7+1}{z+1}=z^6-z^5+z^4-z^3+z^2-z+1$$

Para $\Phi_{15}(z)=\prod_{d|n}(z^{15/d}-1)^{\mu(d)}$, tenemos

$$\Phi_{15}(z)=\frac{z^{15}-1}{(\varphi_1\varphi_5)\varphi_3}=\frac{z^{15}-1}{(z^5-1)(z^2+z+1)}=\frac{z^{10}+z^5+1}{z^2+z+1}=z^8-z^7+z^5-z^4+z^3-z+1$$

o bien

$$z^{15}-1=\frac{(z^{15}-1)}{(z^5-1)(z^2+z+1)}=\frac{z^{10}+z^5+1}{z^2+z+1}=z^8-z^7+z^5-z^4+z^3-z+1$$

Para $\Phi_{16}(z)=\prod_{d|n}(z^{16/d}-1)^{\mu(d)}$, tenemos

$$\Phi_{16}(z)=\frac{z^{16}-1}{\varphi_1\varphi_2\varphi_4\varphi_8}=z^8+1$$

o bien

$$z^{16}-1=\frac{(z^{16}-1)}{(z^8-1)}=\frac{(z^{16}-1)}{(z-1)(z+1)(z^2+1)(z^4+1)}=z^8+1$$

El resto de polinomios los dejamos como ejercicios de prácticas.

6.3 Calcular algunas de las raíces de la unidad de los polinomios ciclotómicos indicados.

La ecuación $z^n=1$, donde las soluciones $\omega=e^{2\pi ik/n}$ son las raíces de la unidad, a veces llamadas números de Moivre en honor a Abraham de Moivre (1667-1754). Gauss demostró que la ecuación ciclotómica se puede reducir a la solución de una serie de ecuaciones de segundo grado cada vez que es un primo de Fermat. En 1836 el matemático francés Pierre Wantzel (1814-1848) demostró que esta condición no es sólo suficiente, sino también necesaria. Una "irreductible" ecuación ciclotómica es una expresión de la forma

$$\frac{z^p-1}{z-1}=z^{p-1}+z^{p-2}+\ldots+1=0$$

donde p es primo. Sus raíces z_i satisfacen a $|z_i|=1$.
A continuación calculamos las raíces de la unidad de alguno de los polinomios ciclotómicos siguientes:

Para $\Phi_3(z)=z^2+z+1$, las raíces de la unidad son

$$\left\{\left\{z=-\sqrt[3]{-1}\right\},\left\{z=(-1)^{2/3}\right\}\right\}$$

Como $\sqrt{-1}=i$, probamos que las raíces de la unidad se verifican

$$\left(-\sqrt[3]{(-1)}\right)^3=1 \text{ y } \left((-1)^{2/3}\right)^3=\left(-\sqrt[3]{(-i)^2}\right)^3=1$$

Para $\Phi_4(z)=z^2+1$, las raíces de la unidad son

$$\{\{z=-i\},\{z=i\}\}$$

Para $\Phi_5(z)=z^4+z^3+z^2+z+1$, las raíces de la unidad son

$$\left\{\left\{z=-\sqrt[5]{-1}\right\},\left\{z=(-1)^{2/5}\right\},\left\{z=-(-1)^{3/5}\right\},\left\{z=(-1)^{4/5}\right\}\right\}$$

Probamos que las raíces de la unidad se verifican como

$$\left(-\sqrt[5]{(-i)^1}\right)^5=(i)^5=-i,\ \left(-\sqrt[5]{(-i)^2}\right)^5=-(-1)^5=1,\ \left(-\sqrt[5]{(-i)^3}\right)^5=(-i)^5=-i,$$
$$\left(-\sqrt[5]{(-i)^4}\right)^5=(-1)^5=-1.$$

Para $\Phi_6(z)=z^2-z+1,$ las raíces de la unidad son

$$\{\{z=\sqrt[3]{-1}\},\{z=-(-1)^{2/3}\}\}$$

Las raíces complejas de esta ecuación son

$$\left(e^{2\pi i4/6}\right)=-\frac{1}{2}+\frac{\sqrt{3}i}{2}\ \acute{o}\ -\left(e^{2\pi i4/6}\right)=\frac{1}{2}-\frac{\sqrt{3}i}{2}$$

donde comprobamos que

$$\left(z-\frac{1+\sqrt{3}i}{2}\right)\left(z-\frac{1-\sqrt{3}i}{2}\right)=z^2-z+1 \text{ y } \left(\frac{1+\sqrt{3}i}{2}\right)\left(\frac{1-\sqrt{3}i}{2}\right)=1$$

Para $\Phi_7(z)=z^6+z^5+z^4+z^3+z^2+z+1,$ las raíces de la unidad son

$$\left\{\left\{z=-\sqrt[7]{-1}\right\},\left\{z=(-1)^{2/7}\right\},\left\{z=-(-1)^{3/7}\right\},\left\{z=(-1)^{4/7}\right\},\left\{z=-(-1)^{5/7}\right\},\left\{z=(-1)^{6/7}\right\}\right\}$$

Para $\Phi_8(z)=z^4+1,$ las raíces de la unidad son

$$\left\{\left\{z=-\sqrt[4]{-1}\right\},\left\{z=\sqrt[4]{-1}\right\},\left\{z=-(-1)^{3/4}\right\},\left\{z=(-1)^{3/4}\right\}\right\}$$

Para $\Phi_9(z)=z^6+z^3+1,$ las raíces de la unidad son

$$\left\{\left\{z=-\sqrt[9]{-1}\right\},\left\{z=(-1)^{2/9}\right\},\left\{z=(-1)^{4/9}\right\},\left\{z=-(-1)^{5/9}\right\},\left\{z=-(-1)^{7/9}\right\},\left\{z=(-1)^{8/9}\right\}\right\}$$

Para $\Phi_{10}(z)=z^4-z^3+z^2-z+1,$ las raíces de la unidad son

$$\left\{\left\{z=\sqrt[5]{-1}\right\},\left\{z=-(-1)^{2/5}\right\},\left\{z=(-1)^{3/5}\right\},\left\{z=-(-1)^{4/5}\right\}\right\}$$

Para $\Phi_{12}(z)=z^4-z^2+1,$ las raíces de la unidad son

$$\left\{\left\{z=-\sqrt[6]{-1}\right\},\left\{z=\sqrt[6]{-1}\right\},\left\{z=-(-1)^{5/6}\right\},\left\{z=(-1)^{5/6}\right\}\right\}$$

Las soluciones a la ecuación $z^4-z^2+1,$ son $z=\pm\frac{\sqrt{1+\sqrt{3}i}}{\sqrt{2}}$, $z=\pm\frac{\sqrt{1-\sqrt{3}i}}{\sqrt{2}}$ que comprobamos

$$\left(z-\left(\frac{\sqrt{1+\sqrt{3}i}}{\sqrt{2}}\right)\right)\left(z-\left(-\frac{\sqrt{1+\sqrt{3}i}}{\sqrt{2}}\right)\right)=z^2-\frac{\sqrt{3}i}{2}-\frac{1}{2}$$

$$\left(z-\left(\frac{\sqrt{1-\sqrt{3}i}}{\sqrt{2}}\right)\right)\left(z-\left(-\frac{\sqrt{1-\sqrt{3}i}}{\sqrt{2}}\right)\right)=z^2+\frac{\sqrt{3}i}{2}-\frac{1}{2}$$

$$\left(z^2-\frac{\sqrt{3}i}{2}-\frac{1}{2}\right)\left(z^2+\frac{\sqrt{3}i}{2}-\frac{1}{2}\right)=z^4-z^2+1$$

$$\left(\frac{i\left(i+\sqrt{3}\right)}{2}\right)\left(\frac{i\left(i-\sqrt{3}\right)}{2}\right)=1$$

Para $\Phi_{18}(z)=z^6-z^3+1,$ las raíces de la unidad son

$$\left\{\left\{z=\sqrt[9]{-1}\right\},\left\{z=-(-1)^{2/9}\right\},\left\{z=-(-1)^{4/9}\right\},\left\{z=(-1)^{5/9}\right\},\left\{z=(-1)^{7/9}\right\},\left\{z=-(-1)^{8/9}\right\}\right\}$$

13.7 Factorización única en los anillos $\mathbb{Z}p$.

7.1 Demostrar la equivalencia de $7x^2-2x+1\equiv 7(x+2)(x+4)(mód.11)$ y calcular sus soluciones si las hubiera $\in \mathbb{Z}$.

El inverso de 7 respecto a 11 es $8,$ por lo que

$$8(7x^2-2x+1)\equiv 8(7(x+2)(x+4)(mód.11)=x^2+6x+8$$

ambas ecuaciones son equivalentes respecto al anillo $\mathbb{Z}_{11},$ ya que el desarrollo de la segunda equivalencia es $(x+2)(x+4)=x^2+6x+8.$

En cuanto a las soluciones modulares, tenemos

$$7x^2-2x+1\equiv x^2+6x+8\equiv 0(mód.11)\ \rightarrow\ x\equiv 7,9(mód.11)\ \in\ \mathbb{Z}$$

7.2 Demostrar la equivalencia de $8x^2-8x+3\equiv 8(x+7)(x+33)(mód.41)$ y calcular sus soluciones si las hubiera $\in \mathbb{Z}$.

Empecemos por eliminar el coeficiente independiente 8. Para ello calculamos la forma lineal entre 8 y 41, a saber $mcd(8,41)=1=8(-5)+41(1).$ Si ahora multiplicamos la equivalencia planteada, tenemos

$$-5(8x^2-8x+3)\equiv -5(8(x+7)(x+33))(mód.41)=x^2+40x+26$$

donde ambas ecuaciones son equivalentes respecto al anillo $\mathbb{Z}_{41},$ ya que el desarrollo de la segunda equivalencia es $(x+7)(x+33)=x^2+40x+231$ y respecto al módulo 41, $x^2+40x+26.$

En cuanto a las soluciones modulares, tenemos

$$8x^2-8x+3\equiv x^2+40x+26\equiv 0(mód.41)\ \rightarrow\ x\equiv 8,34(mód.41)\ \in\ \mathbb{Z}$$

7.3 Demostrar la equivalencia de $x^3-4x^2-7x+5\equiv(x+4)(x^2+11x+6)(mód.19)$ **y calcular sus soluciones si las hubiera** $\in\mathbb{Z}$.

La factorización de la primera equivalencia respecto al módulo 19, es

$$x^3-4x^2-7x+5\equiv x^3+15x^2+12x+5(mód.19)$$

El desarrollo de la segunda equivalencia respecto al módulo 19, es

$$(x+4)(x^2+11x+6)\equiv x^3+15x^2+12x+5(mód.19)$$

por lo que ambas equivalencias son iguales.

Para las soluciones modulares, obtenemos

$$x^3-4x^2-7x+5\equiv x^3+15x^2+12x+5\equiv 0(mód.19)\ \rightarrow\ x\equiv 15(mód.19)\ \in\ \mathbb{Z}$$

7.4 Demostrar la equivalencia de $x^4-3x-4\equiv(x+1)(x+7)(x^2+5x+5)(mód.13)$ **y calcular sus soluciones si las hubiera** $\in\mathbb{Z}$.

Comprobamos que $x^4-3x-4\equiv x^4+10x+9\equiv(x+1)(x+7)(x^2+5x+5)$.
La solución a la ecuación común, es

$$x^4-3x-4\equiv x^4+10x+9\equiv 0(mód.13)\ \rightarrow\ x\equiv 6,12(mód.13)\ \in\ \mathbb{Z}$$

Vamos a comprobar a partir de la primera ecuación si este resultado es cierto. Para ello utilizaremos la Regla de Ruffini.

	1	0	0	-3	-4
6		6	36	216	1278
	1	6	36	213	1274

$\mapsto\ \boxed{x^3+6x^2+10x+5\equiv 0(mód.13)}$

Ecuación generada $x^3+6x^2+36x+213\equiv x^3+6x^2+10x+5(mód.13)$.

	1	6	10	5
12		12	216	2712
	1	18	226	2717

$\mapsto\ \boxed{x^2+5x+5\not\equiv 0(mód.13)}$

Ecuación generada $x^2+18x+226\not\equiv x^2+5x+5(mód.13)$. Efectivamente, la ecuación no tiene soluciones en $\mathbb{Z}$, ya que $x=\dfrac{5\pm\sqrt{5}}{2}\ \in\ \mathbb{Q}$.
Queda demostrado que las únicas soluciones que admite la ecuación son 6 y 12.

7.5 Demostrar la equivalencia de $z^6-1\equiv(z-1)(z+1)(z^2-z+1)(z^2+z+1)(mód.11)$ y calcular la solución ciclotómica si las hubiera $\in\mathbb{Z}$.

Empecemos por simplificar el segundo miembro de la ecuación.

$$(z+1)(z\text{-}1)=z^2\text{-}1 \text{ y } (z^2+z+1)(z^2-z+1)=z^4+z^2+1$$
$$(z^2-1)(z^4+z^2+1)=z^6-1$$

luego, ambos miembros son equivalentes.
Para z^6-1 respecto a 11, como el $mcd(6,11)=1=6(2)+11(-1),$ obtenemos

$$z^{6\cdot 2}-11\equiv z^6+10(mód.11)$$

que tiene como soluciones $z\equiv 1,10(mód.11)$.
Las raíces n primitivas de 1 son aquellas raíces enésimas, y sólo aquellas $\rho,\rho^2,\rho^3,...,\rho^n$ de 1 cuyos exponentes son primos relativos con $n,$ siendo ρ

$$\rho=\cos(2\pi/n)+\text{sen}\,(2\pi/n)i$$

Para $z^6=1,$ tenemos

$$\rho=\cos(\pi/3)+\text{sen}\,(2\pi/3)i=\frac{1}{2}i+\frac{\sqrt{3}i}{2},\ \ \rho^2=\cos(2\pi/3)+\text{sen}\,(2\pi/3)i=-\frac{1}{2}i+\frac{\sqrt{3}i}{2}$$
$$\rho^3=\cos(\pi)+sen(\pi)i=-1,\ \ \rho^4=\cos(4\pi/3)+\text{sen}\,(4\pi/3)i=-\frac{1}{2}-\frac{\sqrt{3}i}{2}$$
$$\rho^5=\cos(5\pi/3)+\text{sen}\,(5\pi/3)i=\frac{1}{2}-\frac{\sqrt{3}i}{2},\ \ \rho^6=\cos(\pi)+sen(\pi)i=1$$

De éstas, $\rho^3=-1\ y\ \rho^6=1$ son raíces cuadradas de 1 y $\rho^2=-\frac{1}{2}+\frac{\sqrt{3}i}{2},\rho^4=-\frac{1}{2}-\frac{\sqrt{3}i}{2}\ y\ \rho^6=1$ son raíces cúbicas de 1.

7.6 Demostrar la equivalencia de $z^{10}-1\equiv(z^2-1)(z^8+z^6+z^4+z^2+1)(mód.43)$ y calcular la solución ciclotómica si la hubiera $\in\mathbb{Z}$.

El $mcd(10,43)=1=10(13)+43(\text{-}3),$ por lo que $z^{10}-1\equiv z^{10}+42\equiv 0(mód.43)$ y tiene como soluciones $z\equiv 1,42(mód.43)$.
Las raíces enésimas de la unidad vienen determinadas por $Cos(2t\pi/10)+Sen(2t\pi/10)i$

$$z_1=\frac{1}{4}\left(1+\sqrt{5}\right)+i\sqrt{\frac{5}{8}-\frac{\sqrt{5}}{8}},\ \ z^2=\frac{1}{4}\left(\sqrt{5}-1\right)+i\sqrt{\frac{5}{8}+\frac{\sqrt{5}}{8}},\ \ z_3=\frac{1}{4}\left(1-\sqrt{5}\right)+i\sqrt{\frac{5}{8}+\frac{\sqrt{5}}{8}}$$
$$z_4=\frac{1}{4}\left(-1-\sqrt{5}\right)+i\sqrt{\frac{5}{8}-\frac{\sqrt{5}}{8}},\ \ z_5=-1,\ z_6=\frac{1}{4}\left(-1-\sqrt{5}\right)-i\sqrt{\frac{5}{8}-\frac{\sqrt{5}}{8}},$$
$$z_7=\frac{1}{4}\left(1-\sqrt{5}\right)-i\sqrt{\frac{5}{8}+\frac{\sqrt{5}}{8}},\ z_8=\frac{1}{4}\left(\sqrt{5}-1\right)-i\sqrt{\frac{5}{8}+\frac{\sqrt{5}}{8}},\ z_9=\frac{1}{4}\left(1+\sqrt{5}\right)-i\sqrt{\frac{5}{8}-\frac{\sqrt{5}}{8}},\ z_{10}=1$$

o por $e^{\frac{ki\pi}{5}}$

$$z_1 = e^{\frac{i\pi}{5}},\ z_2 = e^{\frac{2i\pi}{5}},\ z_3 = e^{\frac{3i\pi}{5}},\ z_4 = e^{\frac{4i\pi}{5}},\ z_5 = -1,$$
$$z_6 = e^{-\frac{4i\pi}{5}},\ z_7 = e^{-\frac{3i\pi}{5}},\ z_8 = e^{-\frac{2i\pi}{5}},\ z_9 = e^{-\frac{i\pi}{5}},\ z_{10} = 1$$

En ambos casos las raíces de la unidad son la 5ª y la 10ª.

7.7 Demostrar la equivalencia de $z^{14} - 1 \equiv (z^2 - 1)(z^{12} + z^{10} + z^8 + z^6 + z^4 + z^2 + 1)(mód.31)$ y calcular la solución ciclotómica si la hubiera $\in \mathbb{Z}$.

El $mcd(14,31) = 1 = 14(-11) + 31(5),$ de donde la ecuación que determinada como

$$z^{14} - 1 \equiv z^{14} + 30 \equiv 0(mód.31)$$

que tiene como soluciones $z \equiv 1,30(mód.31).$
Aplicando métodos anteriores, las raíces primitivas y de unidad son

$$z = e^{\frac{i\pi}{7}},\ z = e^{\frac{2i\pi}{7}},\ z = e^{\frac{3i\pi}{7}},\ z = e^{\frac{4i\pi}{7}},\ z = e^{\frac{5i\pi}{7}},\ z = e^{\frac{6i\pi}{7}},\ z = -1,$$
$$z = e^{-\frac{6i\pi}{7}},\ z = e^{-\frac{5i\pi}{7}},\ z = e^{-\frac{4i\pi}{7}},\ z = e^{-\frac{3i\pi}{7}},\ z = e^{-\frac{2i\pi}{7}},\ z = e^{-\frac{i\pi}{7}},\ z = 1$$

7.8 Demostrar que $(z+1)^2(z^2-1)(z^2+z-1) \equiv (z-1)(z+1)^3(z^2+z-1)(mód.19)$ no es una equivalencia ciclotómica.

Los desarrollos de ambos miembros de la ecuación son

$$(z+1)^2(z^2-1)(z^2+z-1) = z^6 + 3z^5 + z^4 - 4z^3 - 3z^2 + z + 1$$
$$(z-1)(z+1)^3(z^2+z-1) = z^6 + 3z^5 + z^4 - 4z^3 - 3z^2 + z + 1$$

En ambos casos obtenemos una ecuación idéntica, por tanto, queda demostrada la equivalencia algebraica, cuya solución es

$$z = \frac{-1 \pm \sqrt{5}}{2},\ z = \pm 1$$

y no es una ecuación ciclotómica, ya que no es de la forma $z^n = 1,$ o de la forma

$$\frac{z^n - 1}{z - 1} = z^{n-1} + z^{n-2} + ,...,+1 = 0$$

En cuanto a la solución modular, respecto al módulo 19, es equivalente a

$$z^6 + 3z^5 + z^4 + 15z^3 + 16z^2 + z + 1 \equiv 0(mód.19)$$

que tiene como soluciones $z \equiv 1,4,14,18(mód.19).$

BIBLIOGRAFÍA

ALACA and KENNETH, Introductory Algebraic Number Theory, ISBN: 0-521-54011-9
ALEGRE ESPADA, Miguel y otros, Problemas sobre Funciones de Variable Compleja, ISBN: 84-89607-30-3
ALLENBY, R.B.J.T., Rings, Fields and Groups An Introduction to Abstract Algebra, ISBN: 0-340-54440-6
AYRES, Frank Jr., Álgebra Moderna, ISBN: 968-422-917-8
BIRKOHFF y MAC LANE, Álgebra Moderna, ISBN: 84-316-1226-6
COHN, Harvey, Advanced Number Theory, ISBN: 0-486-64023-X
DICKSON, Leonard, Algebraic Theories, ISBN: 0-489-49573-6
DORRONSORO y HERNÁNDEZ, Números, Grupos y Anillos, ISBN: 84-7829-009-5
IVORRA CASTILLO, Carlos, Matemáticas, Apuntes en PDF, libres de descarga en Internet
IVORRA CASTILLO, Carlos, Teoría de Números, Apuntes en PDF, libres de descarga en Internet
KRASNOV, KISELIOV y MAKÁRENKO, Funciones de Variable Compleja, ISBN: 5-354-01102-7
POLLARD, Harry, The Theory of Algebraic Numbers, ISBN: 0-88385-000-1
SHIDLOVSKI,A.B., Aproximaciones Diofánticas y Números Transcendentes, ISBN: 84-7585-156-8
SPIEGEL, Murray R., Variable Compleja, ISBN: 968-422-883-X
VERA LÓPEZ, Antonio, Problemas y Ejercicios de Matemática Discreta, ISBN: 84-605-4351-X

APOYO INTERNET

http://en.wikipedia.org/wiki/Algebraic_number
http://en.wikipedia.org/wiki/Gaussian_integer
http://en.wikipedia.org/wiki/Quadratic_integer
http://en.wikipedia.org/wiki/Table_of_Gaussian_integer_factorizations
http://wims.unice.fr/wims/ (Calculadora en línea)
http://www.alpertron.com.ar/GAUSIANO.HTM (Calculadora en línea)
http://es.wikipedia.org/wiki/Cuerpo_ciclot%C3%B3mico
http://es.wikipedia.org/wiki/Ra%C3%ADz_de_la_unidad
http://es.wikipedia.org/wiki/Polinomio_ciclot%C3%B3mico
http://www.youtube.com/watch?v=1LCiuis7rZE&feature=related (Video sobre multiplicación y división de complejos)
http://mathworld.wolfram.com/deMoivreNumber.html